Australian Banking Association

ABA submission to Legal and Constitutional Affairs Legislation Committee: Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Overview

The Australian Banking Association (ABA) welcomes the opportunity to provide a submission to the Committee's inquiry into the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Bill). ABA advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. The ABA promotes and encourages policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

ABA agrees the *Privacy Act 1988* (Privacy Act) should provide robust protections for citizens' personal information and sensitive information and significant penalties play an important role in focusing entities on their responsibilities to have strong and effective data protection measures in place. The quantum of the maximum penalties in the proposed Bill – which have no dollar value cap – is significant. It will be critical for legislation to clearly specify when a civil penalty can be sought, thresholds for finding a serious or repeated breach, and any safe harbour or defences.

Businesses – as well as Government – operate in an increasingly complex cybersecurity environment as detailed in the latest Annual Cyber Threat Report published by the Australian Cyber Security Centre. Increasingly, data breaches can be the result of a cybersecurity attack and may raise complex questions for the entity about how to respond. ABA members cooperate with relevant Government agencies and with the Council of Financial Regulators (CFR) on responses to data breaches and cyber security matters and we look forward to strengthening those partnerships.

In this environment, ABA calls for a privacy regime that also supports Australia's national security and cybersecurity strategy by encouraging entities to cooperate with Government and continually build up their cybersecurity defences. ABA also calls for a national framework for responding to data breaches and protecting the customers whose information was compromised in the breach, not just impose penalties on the entity that was the subject of a data breach.

Key ABA recommendations

- If the Government proceeds with the proposed amendments to increase maximum civil penalties, legislation to provide a safe harbour or defences which expressly address when an entity has made reasonable efforts to 'do the right thing' by complying with standards for data security and protection.
- Legislation to also clarify key concepts and terms in legislation, including 'turnover', 'relevant time period', and clarify the thresholds for 'serious' or 'repeated' interference with privacy.
- Government to review the existing legal requirements to retain personal information under a range of federal and state regulatory regimes to provide clear and consistent retention requirements.
- Government to complete its work on a framework enabling organisations to respond to a large data breach, including expressly enabling disclosure of personal information to prevent further harm to affected consumers subject to clear and robust safeguards, and identifying and using infrastructure for the secure disclosure and use of data for a protective purpose.

Australian Banking Association

- Government review and reconcile areas of potential conflict or inconsistency between the Privacy Act regime and cybersecurity regimes.
- Seek alignment between federal and state and territory privacy legislation.

Size of maximum penalty

The Bill would make a number of amendments to the Privacy Act, including to increase the maximum penalty to the greater of $50 million, or 3 times the value of the benefit (if it can be determined), or 30% of "adjusted turnover" for the "breach turnover period" (if the benefit cannot be determined).

There is no caselaw on the application of the current civil penalty provision in the Privacy Act. In the current Facebook matter, the Office of the Australian Information Commissioner (OAIC) has taken a broad interpretation of how civil penalties should be applied for serious and repeated privacy breaches and the penalty sought would far exceed $50 million.

The maximum penalty in the Bill differs from the maximum penalties in other jurisdictions with similar economy-wide privacy legislation. For a large organisation in Australia, increasing the penalty to 30% of adjusted turnover during a breach turnover period of 3 years, for example, would equate to practically the entire group turnover in a year and go to billions of dollars (noting under the Regulatory Powers 2014, the OAIC can bring civil penalties within 6 years of the alleged breach of the Privacy Act). By comparison:

- The penalty regime under the GDPR, which is a global benchmark, has maximum penalties of up to 20 million euros or from 2-4% of an entity's global turnover of the preceding fiscal year whichever is higher, for severe violations.
- In Japan, a corporate body violating an order of the PPC carries fines of up to 100 million yen (equivalent to approximately A$1.1 million).

Proposals relating to the imposition of penalties

If the Government proceeds with the proposed amendments to increase maximum penalties, ABA requests the Government provide clarity and certainty within the legislation about when a civil penalty may be sought, what factors are used to determine a 'serious' breach and what are mitigating factors that may reduce the size of the penalty. A lack of clarity can dampen innovation, and create an environment that hinders consumers and organisations making lawful and ethical use of data.

Safe harbour or defence: when data breaches happen despite entities doing the right thing

In our current cybersecurity environment, entities (and even Government) can be and have been victims of sophisticated and targeted actions by large scale organised criminals or state actors, even though the entity has taken all reasonable steps to comply with the Australian Privacy Principles (APP) including by adhering to relevant security standards in designing, building, monitoring and maintaining its cybersecurity defences..

These cyber criminals are a threat to our national interest, and are constantly evolving to seek out new weaknesses. The Government has recognised that safeguarding our nation against cyber attacks relies on partnerships and timely information-sharing between Government, businesses and the community. Cybersecurity attacks can also raise difficult questions for an organisation's Board, often under extreme time pressure. For example, an organisation may seek technical support from the Australian Cyber Security Centre and follow the Government's recommendation not to pay ransom, but that decision could have flow-on consequences.

ABA proposes the Privacy Act treatment of notifiable data breaches and the associated penalties regime recognise and align with these additional policy considerations by explicitly providing a safe harbour where, notwithstanding a data security breach incident, entities have taken reasonable steps to comply with recognised standards for data security and protection. Alternatively, at a minimum, the

Australian Banking Association

Privacy Act should expressly provide that the courts should consider the following factors in determining whether a penalty should be applied and the quantum of the penalty:

- whether the entity has taken reasonable steps to comply with the Privacy Act for a notifiable data breach, including by complying with recognised standards for security and had robust privacy frameworks in place;
- whether an entity disclosed a breach in a timely way; and
- whether an entity worked in good faith with the OAIC and relevant authorities to remediate the breach.

More legal certainty on key concepts

ABA asks for legislation to provide more certainty and clarity about meaning of key concepts that will go to the imposition and quantum of penalties, prior to the increased maximum penalties coming into effect.

ABA strongly proposes the legislation more clearly define these terms, prior to the revised penalties coming into effect:

- Provide further guidance and information on the interpretation of '30 per cent of a company's adjusted turnover in the relevant period', particularly how this will apply if there are different interferences with privacy that are the subject of the civil penalty orders.
- Provide further guidance on what constitutes the "breach turnover period" for the contravention and/or otherwise provide clarity about how this definition and the penalty operate in situations where a contravention persists for a number of years (which can occur where a data breach is not discovered until years after).

ABA strongly proposes legislation defining or otherwise clarify the meaning of 'serious' or 'repeated' interference with privacy, prior to the revised penalties coming into effect:

- 'Serious' or 'repeated' interference with privacy: these concepts are not defined in the Privacy Act; no caselaw is available. ABA also notes the OAIC's Guide to Privacy Regulatory Action (the Guide) provides a limited number of factors that are taken into consideration by the OAIC to establish whether an interference with privacy amounts to a 'serious' or 'repeated' that do not address the cyber security considerations outlined above.
- While the revised penalties appear to be modelled on the penalties for unfair contract terms under Australian Consumer Law (ACL), there are critical differences between the regimes. The Privacy Act heavily relies on interpretation and application of the APPs, for which there is no counterpart in consumer law. For example, establishing a 'serious' or 'repeated' interference with privacy under section 13G of the Privacy Act requires establishing a contravention of the APP (or another section of the Privacy Act), however, it can be highly uncertain whether an organisation has failed to taken 'reasonable steps' to protect information under APP 11.1.

Implications for the OAIC

The above sections highlight that increasing the maximum penalty will have further implications for the OAIC and how it operates. For example, the OAIC has a number of other regulatory powers available that involve supporting entities or instructing entities to improve their security and retention capabilities. Effective use of these tools would do as much, or more, to promote improved awareness of and compliance with Privacy Act obligations.

These powers and tools could be extended to include:

Australian Banking Association

- The OAIC being able to conduct privacy assessments of an entity's acts and practices, and providing recommendations as to how an entity might reduce risks or address areas of non-compliance.
- After completing an investigation of a complaint or Commissioner Initiated Investigation (CII), the Commissioner making a Determination requiring the entity take particular steps. Determinations not only serves as public precedent but is also educational in providing a current interpretation of the Privacy Act from the Commissioner.

These functions can go further towards the investment into best privacy practices of APP entities in the security of personal information held, rather than the impact of civil penalties alone.

ABA recommendation: if the Government proceeds with the proposed amendments relating to increased maximum penalties, ABA strongly recommends the Government also include legislative amendments to:

- provide a safe harbour or defences which expressly address when an entity is considered to have made reasonable efforts to 'do the right thing' by complying with standards for data security and protection.
- clarify key concepts and terms in legislation, including 'turnover', 'relevant time period', and clarify the thresholds for 'serious' or 'repeated' interference with privacy to align with the Government's cybersecurity policy. Legislative amendments may be supported by guidance or case studies from OAIC.

Address the root cause of data breaches

The penalties amendments do not address the source of many data breaches including high profile recent data breaches, being cyber hacks and the lack of a regime that enables government and private sector protect victims of breaches and helps the affected organisation to build back. The amendments in this Bill may also need to be reviewed in context of the broader Privacy Act review. We draw the Committee's attention to the following issues.

Data retention and record keeping requirements

In light of recent high profile data breaches, consumers and industry stakeholders have identified the case for reducing the amount of personal information that organisations hold about customers.

However, there are legislative barriers to organisations seeking to reduce the amounts of personal information they hold. Several Australian laws require that companies collect and maintain certain types of information to demonstrate compliance with the requirements of these regimes on an ongoing basis, for example, Know Your Customer (KYC) regimes or for taxation purposes. Financial sector entities hold information such as customer or transaction records for a number of regulatory purposes.

The consequence of this is often complex and overlapping retention requirements that result in companies needing to maintain data longer than is perhaps necessary to manage the actual risk the law is intended to deal with. Addressing these complexities is a key part of Australia's holistic response to data breaches.

A longer term national response to data breaches should also consider:

- Government and industry identify ways to use technology innovation to minimise the need for data retention. A future state should include the use of digital identity which can promote more privacy-preserving ways of verifying customers' identity.
- Government review legislative and regulatory regimes relating to the sharing and use of data (between government entities and with the private sector) to reconcile the priorities of sharing and using data to support innovation and realise economic and consumer benefit, and the protection of personal information.

Australian Banking Association

ABA recommendation: ABA asks the Government to review the existing legal requirements to retain personal information under a range of federal and state regulatory regimes to provide clear and consistent retention requirements. Also consider whether these requirements remain fit for purpose, and compatible with both APP 11.2 and current community expectations.

A framework for responding to data breaches

Increased civil penalties under the Privacy Act does not meet the need for a national framework to respond to large data breaches affecting millions of Australians. Australia needs a comprehensive set of actions, with cooperation between government, industry and communities, to enhance the nation's resilience to cyber attacks and to have an effective framework to respond to and remediate data breaches (going beyond the scope of the Cyber Incident Management Arrangements).

Responding to a data breach to prevent further harm to affected customers – including identity theft, fraud and scams – may often require assistance from State or federal authorities and private sector entities.

Customers need clear, consistent and actionable information about what steps they should take to protect themselves. As such, a national response should support the entity affected by a data breach to advise and support their affected customers.

While there are data sharing arrangements between many government and regulatory authorities, a private sector response can be impeded by strict confidentiality or non-disclosure requirements in industry regulatory regimes and concerns about the sharing of customer information for the limited specific purpose of protecting these customers from further harm.

ABA also notes the Business Council of Australia's call for a single advisor and coordinator to manage the Government's response to these incidents.

ABA recommendation: ABA urges the Government complete its work on a framework enabling organisations to respond to a large data breach. Specifically:

- Expressly enabling disclosure of personal information as part of a response to a data breach for a protective purpose (for example, to detect and prevent a cyber attack, fraud, scams or identity theft), subject to clear and robust safeguards.
- More generally, consider amending the Privacy Act to allow disclosure of personal information for a range of protective purposes such as to safeguard financial wellbeing, subject to clear and robust safeguards.
- Identifying and use data and reporting infrastructure that can support the secure disclosure and use of data for a protective purpose. The Australian Financial Crimes Exchange is an existing example of such an infrastructure, developed with Government endorsement, in the financial sector.

Alignment, or avoid inconsistency, between privacy and cyber security regimes

While different legislation and areas of government policy apply to privacy (and notifiable data breaches) and cyber security and data security, these two areas will often apply to the same incident. Given the importance of each policy area and the speed with which entities may need to respond to cyber attacks causing data breaches, it is critical for the applicable regulatory regimes to align, provide clarity to assist entities responding to these incidents, and avoid creating conflicting incentives and requirements that can impede these responses.

Key issues of potential conflict are:

- Whether a refusal to pay a ransom demand adds to the seriousness of the interference with the privacy of an individual. If yes, how can the broader community interest in not paying ransoms be recognised and what discounting of the penalty is appropriate?

Australian Banking Association

- For notifiable data breaches that result from a cyber attack, whether an entity that has complied with relevant cyber technical standards (ie, APRA CPS 234, obligations under the *Security of Critical Infrastructure Act 2018*, ACSC guidance or applicable industry standards) can still be penalised for a breach of the Privacy Act because of the fact of the data breach. If so, the Privacy Act will effectively set a new and undefined cybersecurity standard carrying significant financial and reputational liability.
- The Government's critical infrastructure regulatory regime make the disclosure of the statutory incident report to the ACSC a criminal offence – the Information Commissioner's powers to disclose information about a data breach should not be able to override those requirements in the interests of national security.

Further issues where ABA seeks consistency between privacy and cybersecurity policy are:

- Before the Information Commissioner publicly discloses information about an actual or suspected breach, the Information Commissioner should be required 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.
- Consider whether the Information Commissioner's proposed new powers to gather information in response to an actual or suspected notifiable data breach should be bounded by some form of time based requirement (for example, after the 30 day assessment period). In context of cyber security, Government policy has recognised that duplicative information requests when an entity is actively responding to an attack or data breach may be a distraction or divert critical resources from the main objective of securing the breach and protecting data subjects.

ABA recommendation: the Government review and reconcile areas of potential conflict or inconsistency between the Privacy Act regime and cybersecurity regimes.

Application to Government including State Government

Cyber security capability enhancement should be a priority for Government as well as private sector, noting that State and Territory government agencies are not subject to the Privacy Act.

The Privacy Act is a federal law which does not cover local, state or territory government agencies. Most Australian states and territories have equivalent legislation which covers their public sector agencies, though some state authorities are bound by the Privacy Act.

ABA recommendation: alignment between federal and state and territory legislation to ensure any reform of the Privacy Act is also reflected in the equivalent state and territory legislation.

Lack of time for consultation

ABA strongly recommends ensuring adequate time to allow for community and industry consultation. The short period of time for consultation leaves little time for stakeholders to conduct an adequate review of the proposed amendments to determine impact and provide useful feedback. This short time for consultation also limits the opportunity for industry identify questions about the implications for the OAIC, including how the amended provisions will be applied.