CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CYBER SECURITY COOPERATIVE RESEARCH CENTRE SUMBMISSION:
Privacy Act Review

Edith Cowan University
270 Joondlaup Drive,
Joondalup WA 6027
PO BOX 4155, Kingston ACT 2604

cybersecuritycrc.org.au

Dear Sir/Madam

Submission: Privacy Act Review

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) submission to the Attorney-General's Department's Privacy Act Review. Undoubtedly, the provisions and frameworks established under the *Privacy Act 1988 (Cth)* (the Act) impact the lives of all Australians and this review is both timely and pertinent. The rapid evolution of technology, namely the interconnectedness brought by the internet, has impacted the world profoundly since the Act was established. This has had serious ramifications for the privacy of individuals and protection of their personal data, the integrity of which, is of the highest priority. Therefore, The CSCRC commends the Federal Government for undertaking a consultative review of this significant Act, which affects us all.

About the Cyber Security Cooperative Research Centre

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding, and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 24 Participants including seven Research Providers, seven State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding the review.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre

Executive Summary

The online and offline worlds are inextricably linked and, over a relatively short period of time, this has had serious implications for the privacy of all Australians. While the provisions and frameworks established under the *Privacy Act 1988 (Cth)* (the Act) provide specific safeguards for the privacy of individuals, these protections are not absolute. Hence, this review is both pertinent and timely, providing an opportunity to bring the Act further into line with the realities of contemporary society.

While it is imperative that the personal data of Australians be adequately protected by laws that are fit-for-purpose and proportionate, the CSCRC recognises this is a tough balancing act and is multifaceted. It involves the hardening of provisions that protect personal data while also considering the needs of government and business, by not overregulating what is already a complex area.

Therefore, while the CSCRC supports this review and its aims, caution is advised in regard to overregulation, which has the to potential to result in compliance paralysis and overly onerous reporting requirements for Australian Privacy Principle (APP) entities.

Furthermore, the CSCRC recognises that privacy protections are not only the responsibility of APP entities – individuals must also, to the best of their ability, take responsibility for securing their personal data. To this end, greater education regarding the value and personal information is required across the entire community, especially in an increasingly digitised world. This is well within the remit of the Office of the Australian Information Commissioner (OAIC).

Key recommendations:

- Explicit recognition of the remit of the OAIC to enforce the provisions of the Act be included in section 2A.
- The definition of 'personal information' be amended to align with the GDPR definition.
- While it is appropriate for the electoral roll to be provided to political representatives or registered political party, individuals on the Do Not Call Register should not be contacted.
- Definitions of 'journalism' and 'media organisation' should be revised to reflect the vastly altered media landscape that has evolved since the Act was established.

- APP entities should be required to provide notices for all collections of personal information, with limited exemptions, to help build consumer confidence and awareness.
- Standardised icons and phrases should be implemented to assist consumers decipher quickly and easily the meaning of data handling information they receive.
- Consent requirements should be strengthened to increase transparency of information processing and reduce the power imbalance between consumers and APP entities.
- Individuals should have the right to be comprehensively informed of the data an APP entity holds about them and the 'right to erasure'.
- The Government publish and maintain a list of international privacy protection laws and binding schemes to provide APP entities with certainty regarding exceptions to disclosure.
- Australia's Information and Privacy Commissioner take a more public role in discussing the OAIC's work and breaches of the Notifiable Data Breach scheme.
- The introduction of a direct right for individuals to bring actions and class actions under the Act, to would operate alongside existing methods of recourse.
- The introduction of a Commonwealth tort to deal with serious invasions of privacy.
- The development of clear and prescriptive guidelines and resources for APP entities so, in the event of a data breach, they can respond in a timely and effective fashion.

Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

The CSCRC submits the objects outlined in section 2A of the Act remain relevant and fit-for-purpose and are sufficiently broad to capture technological developments that have occurred since the Act's inception. Importantly, care has been taken to recognise that the protections and privacy of individuals must be considered in conjunction and balanced with the interests of entities in carrying out their functions or activities[1]. This is vital.

The CSCRC understands why the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry – Final Report* (DPI Report) questioned this consideration and its potential impact on the ability of consumers to make informed decisions.[2] However, the CSCRC submits that any change to this objective would be particularly onerous on business, adding extra regulatory burden in what is a challenging time. It should not solely be the remit of business to ensure consumers and their privacy are adequately protected – consumers should be encouraged to ask questions and satisfy themselves their personal data is being adequately secured. This is touched upon later in the submission.

If the objects were to be expanded, the CSCRC recommends explicit recognition of the remit of the Office of the Australian Information Commissioner (OAIC) to enforce the provisions of the Act be included.

The definition of 'personal information'

The Act defines 'personal information'[3] as:

"Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not."

While applications of the definition in practice have been established in case law, notably in the matter of the *Privacy Commission v Telstra (2017),* in which the Federal Court of Australia concluded that "even if a single piece of information is not 'about the individual' it

[1] https://www.legislation.gov.au/Details/C2020C00025
[2] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, 477

[3] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

may be about the individual when combined with other information",[4] greater clarity is needed.

The CSCRC submits that the definition should be refined and updated and supports the recommendation of the DPI Report that it be aligned with the European Union's General Data Protections Regulation (GDPR) definition of personal information.[5] Under this definition, 'personal data' is: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[6]

Adopting such a definition would effectively expand the constitution of 'personal information' and help allay concerns related to privacy risks arising from new forms of 'personal information' like IP addresses and social media profiles. Harmonisation with the GDPR's definition would also better align Australia with what is widely recognised as international best practice.

Australian Privacy Principles

The framework of the Act, which is guided by the 13 Australian Privacy Principles (APPs), sets clear and easy-to-understand guidelines that entities subject to the Act can follow. They remain relevant, fit-for purpose and sufficiently broad so as to provide flexibility for a wide range of entities, acts and practices.

Exemptions

The CSCRC submits exemptions for small businesses under the Act are appropriate in their current form. Extending the reach of the Act as it relates to small business would be onerous, especially in the current economic climate, imposing unnecessary compliance costs. When it comes to providing personal information to small businesses not covered by the Act, while there is certainly onus on these businesses not to over-collect, individuals must take a level of personal responsibility and question why such information would be

[4] https://www.oaic.gov.au/updates/news-and-media/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision/
[5] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 460
[6] https://gdpr-info.eu/art-4-gdpr/

required. Unfortunately, many individuals fail to recognise the value of their personal information and do not consider the potential implications of providing it without question. Ultimately, the panacea to this problem is education, specifically, to help Australians understand the value of their personal information and in what circumstances they are required to provide it.

While political exemptions should remain in place, the CSCRC recommends these exemptions should be removed in regard to the *Do Not Call Register Act 2006.* Likewise, political exemptions should not apply in regard to spam and telemarketing rules. The CSCRC submits that while it is appropriate for the electoral roll to be provided to a political representative or registered political party, individuals on the roll who are on the Do Not Call Register should not be contacted and their explicit desire for privacy respected.

Press freedom is fundamental to the Australian way of life and exemptions for journalists and media organisations acting 'in the course of journalism'[7] should remain in place. However, consideration should be given to refining and narrowing the definitions of 'journalism' and 'media organisation', given the proliferation of citizen journalism and social media that has occurred since the Act was established. The current wording, which is overly broad, could result in serious unintended consequences.

Notice of collection of personal information

It is appropriate and necessary that under the Act and the APPs regulated entities must take 'reasonable steps' to notify individuals of the collection of their personal information, as individuals can only provide informed consent if this is the mandated practice. However, it is pertinent to note that since the Act's establishment the definition of 'reasonable steps' has undoubtedly evolved as a result of rapid technological developments. While amendments should be made to better define 'reasonable steps' in a bid to ensure the wording is fit-for-purpose, a key advantage of the proliferation of communication technologies ultimately means that notification of collection is easier to achieve than ever before.

[7] https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/42-journalism-exemption/retaining-an-exemption-for-journalistic-acts-and-practices/#:~:text=42.3%20Under%20s%207B(4,standards%20that%20deal%20with%20privacy.

The CSCRC supports the recommendations of the DPI Report regarding measures to strengthen notification requirements by APP entities.[8] As noted in the report, the recommendation that APP entities be required to provide a notice for all collections of personal information, with limited exemptions, would help build consumer confidence and awareness of when personal information is being collected. Furthermore, it is common sense that such notices should be conveyed in clear, easily understood language, with details of how the information is collected, used and disclosed. The CSCRC submits that it would also be useful to consumers to know the jurisdiction within which their data was being held. It would also be appropriate to 'layer' notices of collection, for example, follow up the initial notice with an electronic or telephonic notification.

In circumstances where personal information is collected by a third party, the CSCRC agrees with the ACCC's assertion that an individual should always be provided with notice when their personal information is collected, whether such collection is direct or indirect. It is for this reason the ACCC commenced proceedings against Google on July 27 2020, " alleging Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising".[9]

Finally, the CSCRC accepts that in an increasingly digitised world consumers are subject to 'information overload'. This presents a significant challenge because, given the volume of information they receive, consumers can become complacent as to the personal privacy implications of 'ticking and flicking', for example, an updated privacy policy. Hence, the CSCRC agrees with the ACCC's suggestion of standardised icons and phrases to assist consumers decipher quickly and easily the meaning of data handling information received.[10] While such a solution is a not a silver bullet it would help establish clear signposts for consumers in this space.

Consent to collection and use and disclosure of personal information

As it stands, and as noted in the issues paper, consent is dependent on the type of personal data that is being collected and the context in which this occurs. The Act also provides for exceptions for consent, where public interest overrides the right of privacy, for example, in

[8] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp35
[9] https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data
[10] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 403

the event of an emergency declaration or in relation to law enforcement activities.[11] Such exemptions are essential and must remain in place.

However, the CSCRC agrees with the recommendation of the DPI Report that consent requirements should be strengthened to increase the transparency of information processing and reduce the bargaining power imbalance between consumers and the APP entities.[12] In particular, the CSCRC supports the principle that: "Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled".[13] The CSCRC strongly supports the inclusion of 'off' default settings for information that is not required for the provision of products or services because changing such settings would be more illustrative of meaningful consent. The CSCRC also submits that language used within privacy policies should be regularly reviewed to ensure it is intelligible and fit-for-purpose.

Finally, as previously noted, while there is a clear responsibility for APP entities to ensure reasonably necessary steps have been taken in terms of gaining informed consent, consumers must also play a key role.

Control and security of personal information

Personal information is valuable and must be vigorously protected to ensure the privacy of individuals is not compromised. The proliferation of digitised data collection by APP entities has added significant complexity in ensuring the protection of personal information and, while it has undoubtedly streamlined organisational functions, it has increased the risks associated with data breaches. This has ramifications for both individuals and APP entities. For individuals, it means they must remain vigilant to whom they are providing their personal information to and how that information is being used. For APP entities it means ensuring their security measures – especially in relation to cyber security – are adequate

[11] https://www.legislation.gov.au/Details/C2020C00025
[12] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 465.

[13] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 35

and up to date. This is especially pertinent given 60 per cent of the 964 eligible breaches reported between 1 April 2018 and 31 March 2019 were malicious or criminal attacks.[14]

The CSCRC submits that individuals should have the right to be comprehensively informed of the data an APP entity holds about them. Furthermore, they should have the ability to require the deletion of unnecessary personal information that is being stored. To this end, the CSCRC supports the DPI Report's recommendation that a 'right to erasure' be established under the Act "unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason".[15] Such a right must also include exemptions and be counterbalanced with matters of public interest including freedom of speech, freedom of the media, public health and safety, and national security.

While the Act and APPs set out obligations that apply when it is no longer appropriate for an entity to retain personal information, including the destruction and deidentification of personal information, the CSCRC submits these obligations should be hardened. The CSCRC notes the DPI Report did not support the introduction of a mandatory deletion obligation once data is obsolete, as it could prove a significant regulatory burden, especially for small businesses.[16] The CSCRC disagrees with this assessment and submits that while small businesses should be exempt, large entities have the capacity to fulfil the obligations associated with mandatory deletion. This is especially relevant given the increasing commoditisation and stockpiling of personal data, which is valuable for commercial and criminal enterprise alike.

Overseas data flows and third-party certification

As noted in the issues paper, there is no single global standard that governs international data flows. Indeed, international harmonisation of such a standard would be virtually impossible to implement. The paper also clearly highlights the current distinction in the APPs between the 'disclosure' of personal information to an overseas recipient, which is required under law, as opposed to the 'transfer' or 'use' of the data by the APP entity, which may be routed through overseas servers and does not require disclosure.

[14] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf, p 4
[15] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 470
[16] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 473

The CSCRC notes there are also exceptions for disclosure requirements if an APP entity 'reasonably believes' the jurisdiction within which the recipient is operating is subject to legal or binding obligations regarding protection of personal information.[17] The CSCRC submits such exemptions are overly subjective and require refinement. To this end, the CSCRC supports the Australian Law Reform Commission's (ALRC) recommendation that a list of international laws and binding schemes be published and maintained by the government, a move that would provide APP entities with certainty regarding exceptions to disclosure.[18]

Enforcement powers under Privacy Act and role of the OAIC

The Australian Information and Privacy Commissioner (the Commissioner) has significant powers under law, including the ability to:

- accept an enforceable undertaking and bring proceedings to enforce an enforceable undertaking;
- make a determination and bring proceedings to enforce a determination;
- seek an injunction to prevent ongoing activity or a recurrence;
- apply to court for a civil penalty order for a breach of a civil penalty provision, which includes a serious or repeated interference with privacy.[19]

The CSCRC notes the Commissioner has used these powers extensively in relation to enforceable undertakings and enforcement of determinations and has awarded victims small monetary sums as compensation in multiple cases. However, the Commissioner's powers to seek civil pecuniary penalties that were established in 2014, were not applied until March 2020, when proceedings were launched against Facebook for numerous alleged breaches that occurred from 2014-15.[20] Under the Act, such pecuniary penalties can equate to significant fines (many millions of dollars). The case, which remains before the Federal Court of Australia, will set a significant precedent moving forward.

The CSCRC submits that the Commissioner's powers and their enforcement, especially in relation to civil pecuniary penalties, could serve as a powerful deterrent to organisations failing to fulfil their requirements under the Notifiable Data Breach (NDB) scheme. If faced

[17] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 83
[18] https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol2.pdf
[19] https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#australian-information-commissioners-role-in-the-ndb-scheme
[20] https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2020/2020fca0531

with the risk of large fines, it makes sense entities shirking their duties could move towards more effective implementation. If this were to occur it would ultimately serve to enhance the privacy protections of all Australians. Furthermore, while the CSCRC notes rulings regarding enforceable undertakings and decisions are available on the OAIC's website, wider publication would help heighten public understanding of the Commissioner's good work, role and powers, as well as their own rights under the Act. This too would enhance the privacy of Australians and encourage APP entities to fulfil their duties under the NDB Scheme.

The CSCRC commends the Commissioner for recognising the harm caused by data breaches in decisions. A good example is the recent case of *ST and Chief Executive Officer of Services Australia (Privacy)*[21], in which the Commissioner exercised her powers to 'award compensation for any loss or damage suffered by reason of the interference with privacy'. The decision states: "I accept the evidence provided by the complainant's consultant psychiatrist stating that the disclosure caused her 'considerable distress'".

Finally, the CSCRC supports proposed reforms that would provide the Commissioner with new infringement notice powers for failure to cooperate with efforts to resolve minor breaches. Providing the option to pay a fine in full as an alternative to prosecution for an offence or litigation of a civil matter in court would help mitigate against a backlog of cases and assist the Commissioner in utilising the resources of the OAIC more effectively.

Direct right of action

The CSCRC notes that under the Act individuals are limited in their ability to take legal action related to a breach of their privacy, with current options for recourse limited to making a complaint to the Commissioner or applying directly to the Federal Court or Federal Circuit Court for an injunction. Such a process is potentially onerous and complex and puts undue onus on the individual alleging their privacy was breached.

Hence, the CSCRC supports the recommendation of the DPI Report, which calls for the introduction of a direct right for individuals to bring actions and class actions under the Act,[22] which would operate in addition to existing methods of recourse. Ultimately, this would provide consumers with greater control over their personal information by way of direct legal redress that forgoes reliance on the OAIC. It would also provide greater

[21] http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2020/30.html
[22] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 473

incentive for APP entities to comply with their requirements under the Act and the APPs, with the cost impost of litigation a key mitigating factor.

However, the introduction of direct right of action would have to established with clear perimeters, including a threshold limit regarding the seriousness of a complaint. The CSCRC submits that such action should only be permitted in the event of serious breaches of the Act or APPs with a cap for damages imposed.

Statutory tort

A Commonwealth tort that deals specifically with digital privacy breaches would help provide clarity in what remains a grey area because in Australia there is no charter of rights or specific constitutional or tortious right to privacy. While the Act does provide limited protections, the law and its interpretation are murky despite the fact cyber harms resulting from data breaches are real, tangible and damaging. Given the rapid proliferation of personal information being shared digitally with APP entities, it is a logical inference that they could also become increasingly common. Therefore, the law needs to be sufficiently prepared to deal with such harms.

In 2014 ALRC released its *Serious Invasions of Privacy in the Digital Era* report,[23] which recommended the establishment of a new Commonwealth tort to address cyber harms resulting from digital invasions of privacy. It found such a tort should provide that a plaintiff proves invasion of privacy by either intrusion upon seclusion or misuse of private information. The report also noted the tort should be actionable only where a person would have had a reasonable expectation of privacy and confined to intentional or reckless invasions of privacy, not negligence. Further, it should provide that action is allowed only where the invasion of privacy is 'serious', with a court able to award damages, including for emotional distress.

The need for a tort to deal with serious invasions of privacy was mirrored in the DPI Report, which stated it would provide "protection for individuals against serious invasions of privacy that may not be captured within the scope of the Privacy Act … (and) increase the accountability of businesses for their data practices and give consumers greater control over their personal information".[24] The DPI Report also stated that: "Doing this would lessen the bargaining power imbalance between consumers and digital platforms by

[23] https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/
[24] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 493

providing Australian consumers with an additional way of seeking redress for poor data practices by digital platforms and other businesses that collect Australians' personal information".[25]

The CSCRC supports the recommendations of both the ALRC and, more recently, the ACCC through the Digital Platforms Inquiry, for a new tort to deal with serious invasions of privacy. Such a tort would provide a clear mechanism through which individuals could seek to protect their privacy, which extends beyond the protections offered in the Act. The CSCRC also supports the view that such a tort must support and not impinge on freedom of speech and include a public interest consideration for media, political communication and artistic expression.

The Notifiable Data Breach (NDB) scheme – impact and effectiveness

Since coming in to force in 2018, the NBD Scheme, under the remit of the OAIC, has proven to be an effective mechanism through which organisations covered by the Act can report potential data breaches. As noted in the DPI Report, data from the OAIC indicates reporting of data breaches increased by 712 per cent following the introduction of the NDB Scheme.[26] The sectors with the highest reporting rates are health, finance and legal service providers.[27] This is significant and illustrates that implementation of the scheme is being adopted by organisations. It is also important to note that 60 per cent of the 964 eligible breaches reported between 1 April 2018 and 31 March 2019 were malicious or criminal attacks.[28]

However, the CSCRC notes the scheme does have limitations, with a key factor being reliance on organisations to self-report and requirement that only breaches 'likely to result in serious harm' be reported.[29] The CSCRC agrees with the ACCC's assertion that as a result, data breaches that consumers could consider to be a breach of privacy are not captured in the reporting.[30] The scheme is also limited in that there is no requirement to provide consumers who have suffered a breach with details of what data was stolen or lost. The

[25] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf; pp 493
[26] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 444
[27] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 450
[28] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf, p 4
[29] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-July-December-2019.pdf, pp 4
[30] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, pp 445

CSCRC submits that consumers would have greater trust in the scheme if more detailed information was provided, as there is little point in notification for notification's sake.

The CSCRC also submits that some organisations captured by the NDB Scheme could find themselves in breach of the Act and APPs because of poor cyber hygiene. It is vital that clear and prescriptive guidelines and educational resources be provided to APP entities so, in the event of a data breach, they can respond in a timely and effective fashion. This means such entities must clearly understand how and where their data is stored, who has access to the data and who is protecting the data. If this does not occur, it is difficult for APP entities to meet their mandated obligations. To this end, the CSCRC supports the OAIC's sentiment that "organisations must ultimately move beyond a purely compliance mindset"[31] and take steps to ensure that in practice the are responsible custodians of valuable personal data.

[31] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/