ACS Response to the Privacy Act Review Report

March 2023

Australian Computer Society Inc. (ACT)
ARBN 160 325 931
National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Attorney General of Australia

ACS response
Privacy Act Review Report

30 March 2023

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical issue.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology sector. We represent over 35,000 members working in all sectors and across the nation.

The ACS works to grow the technology sector while making sure IT professionals act ethically, responsibly, and in keeping with the best interests of not only their employers, but the wider community.

We're extremely happy to see the Australian Government, led by the Attorney General's Department, undertaking this critical work. We've seen the importance of privacy laws writ large in recent breaches that have affected the lives of millions of Australians, where excessive data hoarding and poor custodial practices have led to outcomes much worse than they might have been.

More than that, there are critical principles in play, highlighted by rapidly evolving AI, data analytics and IoT. Privacy is a fundamental right, and Australians deserve to know that those rights are being respected and protected in law even as technology evolves.

Yours sincerely

Troy Steer
Director of Policy, Advocacy and Communications
Australian Computer Society

General notes

ACS very much supports the work being done by the Attorney General's (AG) Department, and believes in both the need for the reforms and the consultative approach that the AG's Department is taking.

We find ourselves in agreement with the majority of changes recommended by the AG's Department, and are very happy to see that this brings us more in line with modern privacy statutes like the GDPR.

A clear statement of intent, as outlined in Section 3 (the Objects), is also very welcome. In the absence of a Bill of Rights, this is the kind of clarity we need around privacy in Australia.

We do have ongoing concerns about the capacity of the Office of the Australian Information Commissioner (OAIC). As the Privacy Commissioner's recent evidence before Senate Estimates made clear, the OAIC is already struggling under the weight of freedom of information review requests and consultations about notifiable data breaches, and these proposed changes will likely place more responsibility on the office. Further consideration needs to be given to better funding the OAIC to enable it to be an appropriately resourced regulator.

For the sake of brevity, we will detail here only the areas where we think the review needs a little more consideration. In particular, there are clarifying points around de-identification, enforcement and company obligations that could be inserted into an Act that arises out of this review.

Section 4: Personal information, de-identification and sensitive information

Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.

We agree with this change, and note that any such definition should include technical (for example, IP addresses), inferred or generated information (marketing and personality profiles, for instance). Any information that that has a 1:1 correlation with an individual, or can be made to be 1:1 with publicly available information (for example, mobile phone number or first name, job title, postcode) must be addressed by the definition.

There are additional points of clarity that could be addressed here as well. We would argue that information should be considered personal information if it enables a person to be singled out from a crowd (individuated). That is, if an individual can be

singled out and acted upon, regardless of whether their actual identity is known, that should be enough to trigger the provisions of the Act. Existing OAIC decisions incorporate this concept.

We believe that the Act needs clarity around this concept: whether individuation (singling out) should be clearly expressed to be sufficient to bring matter within the Act. As things are, entities will still be making judgment calls and constantly having to ask themselves whether a person is 'identifiable'.

Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.

We are concerned that some of the language in this section leaves the issue of de-identification too open to interpretation and misuse.

The language and application of the law around de-identification is critical. De-identification is a technique that will let Australia enjoy the best of both worlds, where individual privacy is protected but aggregate data can still be used and shared productively. Regulation in these areas needs to be carefully designed to ensure that APP entities have appropriate incentives to properly de-identify information and use only de-identified information wherever practicable.

There are objective and repeatable models for determining identifiability that provide a measure of the PII (personally identifiable information) data in a dataset or datasets. These can provide 'hard lines' or threshold measures for de-identification based around identifiable cohort sizes.[1]

We would recommend focussed research on a standardised way to measure degrees of de-identification and the application of those in practice, and to use that research as a guide for APP entities. There are already tools available that can be applied, such as the CSIRO's PIF (Personal Information Factor) tool, which was used for COVID data.[2]

The language in the Report would seem to leave measurements and interpretations of de-identification entirely in the hands of the APP entity, offering them an easy 'out' in cases where they have failed to meet their obligations as data custodians.

[1] See for example "Data Sharing Frameworks", Australian Computer Society, December 2017 https://www.acs.org.au/insightsandpublications/reports-publications/data-sharing-frameworks.html

[2] See https://www.csiro.au/en/news/news-releases/2021/new-data-privacy-tool-ensures-anonymous-covid-19-data-remains-secure-and-private

In particular, we would disagree with the explanatory text the paper that says: "Further defining when the reasonableness threshold would be met would not be useful. The range of circumstances in which entities deal with information is broad. Each entity will need to conduct the assessment in their own context and address the reasonableness of identification in that context."

For the law to have any meaning, there must be thresholds defined within it, or at least guidance provided by the relevant agency. Otherwise, 'reasonable' will become anything the entity in question says it is.

Proposal 4.7 Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.

and

Proposal 4.8 Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where:

- the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way.
- the re-identification is conducted by a processor with the authority of an APP entity controller of the information.

A clear understanding of 'malicious' may be warranted here. A company that re-identifies data for, say, marketing purposes, may not be acting 'maliciously', but would not be acting the best interests of the people whose data was de-identified.

Broadly, we would be against deliberate attempts to re-identify data that has been de-identified, with the exception of those who achieve re-identification accidentally when combining data sets, where it is necessary through (court-approved) law-enforcement action, or in 'whistleblower' or 'white hat' activities where researchers are demonstrating the vulnerability of a system.

Those who do achieve re-identification accidentally or as part a research/vulnerability testing should also be required to take new measures to de-identify the data again.

With respect to 4.7 and 4.8, we wonder why a far simpler model of banning all deliberate re-identification activities, with a list of exceptions, is not appropriate? Once data is de-identified, the goal should be to keep it that way.

Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.

We broadly agree with this position. However, we would ask why it is not being included as part of a broader proposal around sensitive information?

We would also note that, contra to the explanatory notes, we believe this *should* cover the temporal logging of network addresses, cell towers and Wi-Fi networks, since while they are not 'precise', they do provide information on the location and movements of an individual.

An APP entity that wishes to provide localised services based on that data can do so (an IP address, for example, is fundamental to the process of communication and cannot be hidden from the service provider), but that data should not be logged or retained without explicit consent.

Section 8: Political exemption

Proposal 8.1 Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.

ACS can see no convincing reason, on the grounds of public good, for political parties or politicians to enjoy any exemption at all.

This proposal also does not address many criticisms that have been made on opaque and arguably intrusive practices of collection and handling of personal information by politicians and political parties.

Proposal 8.5 The political exemption should be subject to a requirement that political entities must:

(a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure

(b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and

(c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.

We would add that any use of this data (for example, through SMS messages) should include identification of which political party or operative is doing the direct marketing, so that people know who to contact to opt-out.

Section 10: Privacy policies and collection notices

Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.

Privacy notices that are clear and human-readable is certainly a positive step, but even then, it's still likely that consumers will not read them or simply agree to them, especially when given no other choice ("agree to this or don't get the product").

Companies should, by default, only gather and store information that is strictly necessary to deliver the product.

We would argue that 'direct marketing profiles' (eg. purchase histories, ad tracking cookies) would generally not be considered a necessary part of a service offering. If there is a desire for additional information gathering, then that should be explicitly opt-in.

Mobile applications can serve as a model here. When Apple changed the permissions for the use of Apple Advertising ID tracking, Facebook and other app providers were forced to make changes. When given the option, people almost invariably choose not to be tracked.

They are also a model of simplicity. They clearly enumerate all the data fields that are linked.

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

Again, mobile application permissions can serve as something of a model, and the OAIC can enumerate a list of the most commonly stored data fields. A simple list of data gathered and held would be useful.

For example, "We gather and store data on:

- Date of birth
- Email address
- Address
- Credit card information
- Purchase history
- Product preferences"

Consumers could then be given the option to individually opt out of these items.

Section 11: Consent and privacy default settings

Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

and

Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

We agree with the sentiment of these changes, with the caveat that clicking through a privacy agreement (no matter how simply worded) does not meet that standard.

Specific unbundled prompts would meet the standard. For example: "do you agree to allow us to use your purchase history to customise your search options?" would meet the standard of voluntary and informed.

Proposal 11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

While we strongly agree with this, consideration needs to be given to how it interacts with other data retention laws. There are some regulations that require organisations to keep information for six years or even beyond, and compliance with such may conflict with 11.3.

Proposal 11.4 Online privacy settings should reflect the privacy by default framework of the Act. APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.

The wording around this proposal could use adjustment, with 'privacy by default' being somewhat unclear in its intent and application in practice. Default opt-in and default opt-out are clearer and better understood.

We would also argue that it be a requirement that organisations that gather data also ensure they have systems in place for customers/clients to update and revoke privacy settings. Those systems should have short, measurable response times.

For example, a company's privacy settings should be directly accessible from the front page of the website, and not require human intervention to implement, which often results in people giving up on making changes due to time-consuming support calls or slow email responses.

Section 14: Research

Proposal 14.2 Consult further on broadening the scope of research permitted without consent for both agencies and organisations.

We would note additionally to this that adequately de-identified data should obviate the need for consent.

We suggest that there should also be additional clarity with respect to the use of data for AI training or the development of other decision models (for example, the use of such data for analytics applications). Does this fall under the definition of 'research' in this model?

Section 15: Organisational Accountability

Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.

The person nominated should be trained, assessed and certified before they assume accountability. Otherwise this risks being a 'checkbox' exercise wherein somebody in the IT team is randomly assigned the role in order to meet base compliance obligations.

We suggest also that this accountability requirement have an organisational size threshold. While we agree with the removal of the small business exemption, small businesses would often not have the capacity to assign a particular individual to the role.

Section 18: Rights of the Individual

Proposal 18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:

(a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)

(b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual

(c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual

(d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information

(e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual

This right should also cover generated and inferred information, such as marketing and preference profiles (with no exceptions for 'commercial in confidence' or 'trade secrets').

We would note that many APP entities do not currently have any processes or systems in place to respond to such requests. It should be a requirement that entities have in place formal systems to respond to such requests (and a fee if appropriate) as well as a designated contact point and a timeframe for response. Copyright law could provide a

model for this – there must be a designated contact point for such requests and there are time limits on when takedown happens.

However, consideration should be given to the small business exception here and the reasonable capacity of businesses of different sizes to respond to such requests.

Proposal 18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.

The proposal and the explanatory text are vague on possible remedies and outcomes of such a process. A person objects, and the APP entity responds (or perhaps fails to respond). We are unclear on what the next step is or who oversees and mediates such disputes.

Proposal 18.3 Introduce a right to erasure with the following features:

(a) An individual may seek to exercise the right to erasure for any of their personal information.

(b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.

As noted in the explanatory text, this should explicitly not apply to aggregated de-identified data, except when justified under other legislation (National Security regulations, for example).

Consideration also needs to be given where this conflicts with other statutes and data retention rules. For example, a former employee cannot request that their employee or contractor records be deleted without impacting the Work Health and Safety Act. Entities may need to keep this data for up to six or seven years and in some circumstances, even longer (in the case of a workers compensation claim, for example).

Proposal 18.4 Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.

Perhaps some clarifying points would be valuable here, to ensure that it relates to errors of fact and not subjective assessments. Otherwise this proposal has significant potential for abuse.

Proposal 18.5 Introduce a right to de-index online search results containing personal information which is:

(a) sensitive information [e.g. medical history], or

(b) information about a child, or

(c) excessively detailed [e.g. home address and personal phone number], or

(d) inaccurate, out-of-date, incomplete, irrelevant, or misleading.

The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.

We agree this is positive, following the EU guidelines, although as is the case in the EU, full compliance may be a challenge for engine providers given the scope and rapid evolution of such engines. In the event that indexers respond with different results (for example, if Wikipedia and Google disagree) an OAIC-approved independent third party will need to arbitrate and agree a formal response, free of influence or bias, and publish a finding.

(d) is also potentially a significant problem, with substantial scope for abuse of the system. The terms 'incomplete', 'irrelevant' and 'misleading' may need some clarity in the legislation or explanatory notes to limit the number of 'nuisance' requests providers will have to deal with.

Section 19: Automated decision making

Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.

This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.

While greater transparency and explainability around automated decision-making is welcome, regulations should go further to limit the use of ADM in line with Article 22 of the GDPR, which highlights a right to human intervention in decision-making processes if requested. Companies should be required to have processes in place in cases where an automated decision is contested.

Section 20: Direct marketing, targeting and trading

Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.

As noted in our response to 18.1, users should also be able to see what information has been gathered and what it is being used for.

Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.

It must be positive consent, not buried in a 'user agreement' or other legalistic document that will be unlikely to be read or considered by the majority of individuals. Such consent must be unbundled and explicit, and in principle consent to selling an individual's data should never be a mandatory condition of using a good or service.

In addition, clarity could also be provided with respect to certain activities that work across multiple entities, and what 'trade' means in this context. For example, where do programs like Flybuys or Frequent Flyer Points sit within this regime? Would there need to be explicit opt-in requirements for each 'purchase' using Frequent Flyer Points, or would a general release given on sign-up be sufficient?

Section 21: Security, retention and destruction

Proposal 21.3 Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

Cyber security certification can provide a model where companies can prove that they have undertaken adequate steps to ensure the safety of data. There are both national and international frameworks that could be being used for benchmarking (current ACSC advice tends to be government-focused).

Proposal 21.7 Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.

Guidance from the OAIC would be valuable in this regard, since APP entities might have vastly different perspectives on what an appropriate period is. Targeting information, for example, might be construed as 'evergreen' by a company, as might basic customer records (even if there has been no contact between entity and individual for years). The current framing of the proposal leaves it almost entirely in the hands of organisations to determine how long they hold data.

In principle, data should only be held for the period of time it is required and then it should be expunged. Recent breaches, including the Optus and Latitude breaches, have shown that organisations are holding data until long after it has been necessary to do so, substantially exacerbating the effects of those breaches. At the very least, there should be a specific maximum retention period for customer records after there has been no contact between the customer and the entity.

It should also be made clear that these periods must respect the data retention requirements contained in other Acts.

Section 25: Enforcement

Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:

(a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.

(b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.

Consideration should also be given to the size (revenue/employees) of the APP entity, especially with proposed removal of the small business exception.

For very large organisations, compliance costs may exceed breach costs, disincentivising compliance, while smaller businesses would potentially be excessively punished.

We would also consider even higher tiers of penalty for wilful breaches of the code, where an APP entity knows it is in breach but continues operations, accepting any potential civil penalties as a "cost of doing business".

In those cases civil penalties may not be sufficient, and we would recommend investigating criminal penalties for those who knowingly and wilfully breach privacy laws. For these entities there must be a significant penalty which a Board or executive will take seriously, and Directors responsible for those choices should face potential jail time for repeated offences.

Section 26: A direct right of action

Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.

While ACS agrees with this in principle, care must be taken in the drafting of these laws to ensure that courts and APP entities are not overwhelmed with cases (individual and class action). In essence, the Privacy Commissioner would cease to be the gatekeeper to the courts in relation to infringements of the Privacy Act. This may decrease the rate of increase in pressure on resources of the Privacy Commissioner, but the new right needs to be carefully thought out and circumscribed to ensure that it is fit for purpose.

The Australian Law Reform Commission has published a useful model for this kind of direct right of action[3], which applies to serious cases.

If it is to be implemented, we also would suggest a periodic review of this amendment after we see the volume and nature of the outcomes in practice.

Changes should also harmonise with changes under consideration related to cyber security. An APP entity that has undertaken reasonable steps to protect itself from cyber crime, but still falls victim to an attack (since there is no 100% certain defence), should not be inundated with individual or class action suits unless it has breached the Privacy Act in other matters.

Section 28: Notifiable data breaches scheme

Proposal 28.2

(a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.

(b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.

(c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.

We strongly support these recommendations for a 72-hour notification period, which brings us more in line with GDPR.

We are not convinced by some of the arguments that have been advanced to change it to “as soon as practicable”. We have seen entities playing fast and loose with notification timelines, avoiding notification as long as possible by claiming uncertainty. According to the OAIC’s data, 29% of breaches are taking more than a month to report

[3] See Serious Invasions of Privacy in the Digital Era (ALRC Report 123) https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/

to the OAIC. Between July and December 2022, there were three breaches that were not reported for more than a year after the entity became aware of them.[4]

We would also strongly support a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.

Proposal 28.3 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information.

Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.

Language with respect to remedy/compensation would potentially be valuable here. What are an entity's obligations to individuals who have had their privacy compromised?

We recommend developing a regulatory framework that supports victims of data breach. Adopting the philosophy that it is better to plan how to deal with cases of violation of individual privacy rather than look for solutions after the fact, regulated action plans and a framework for compensation should be developed. Frameworks already exist for credit card and payments fraud, so the recommendation is to extend this to other forms of digital services.

In cases where a government entity is affected, and an exemption exists, reporting mechanisms and recourse processes should apply anonymously. For example, if the details of a criminal record is breached, but the attacker does not publish those records, the APP should report to AG's Department within NDB timescales and a root cause found and addressed, even when the cause is expensive to correct.

Even the government should not be able to hide poor practices by remaining silent about breaches, or trust in the process will not be considered to be fair.

- ENDS -

[4] See https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2022