CHOICE

FEBRUARY 2022

Submission to the Attorney General's Department
Privacy Act Review - Discussion Paper

Contents

ABOUT

About CHOICE

CHOICE is the leading consumer advocacy group in Australia. CHOICE is independent, not-for-profit and member-funded. Our mission is simple: we work for fair, just and safe markets that meet the needs of Australian consumers. We do that through our independent testing, advocacy and journalism.

INTRODUCTION

CHOICE welcomes the opportunity to contribute to the Review of the *Privacy Act 1988 (Cth)* ('**the Review**'). As Australia's largest consumer advocacy group, CHOICE supports measures that protect the rights of consumers both offline and online. As more people use the internet to access essential services and make consumer transactions, it is crucial that regulatory measures are fit for purpose and work to correct power imbalances that are prevalent in the digital space.

Big data is big business and the use of personal customer data by businesses of all sizes will increasingly have material implications for consumers. CHOICE welcomes the range of reform options presented in the Privacy Act Review Discussion Paper (October 2021). We support the introduction of reforms that place consumer needs at the fore, enabling them to better control and protect their data.

Too much emphasis has been placed on the obligations of the individual in how they manage and control their privacy in relation to an entity. While recognising that this approach has been adopted in the past, the Privacy Act Review should refocus on the needs of the collective. Individual consent as the primary means of controlling privacy should be replaced by organisational accountability where privacy-by-design is embedded into an entity's practices.

This shift has been accomplished in other sectors within Australia with relative success. For example, in the financial services sector, disclosure of a conflict of interest to a client was traditionally viewed as the primary way to ensure meaningful consent. However, empirical research found this often has the inverse effect where disclosure of conflicts of interest actually increased customer trust in the broker, when it should have led customers to be more critical about the advice.[1] Now, in financial services, brokers and advisers have a best interest duty to ensure that the needs of the customer are placed first. This shift moved the onus from the individual back to the firm, which is best placed to mitigate and minimise harm.

Disclosure of a harmful practice does not remove the harm. Notice and consent mechanisms, while useful, need to be supported by regulations where consumers are not put in a position where they must choose between accessing a product or service and forgoing their privacy or agency. Any reform to the Privacy Act needs to ensure that entities do no harm rather than set requirements for how a consumer can choose not to be harmed.

[1]Lacko, J and Pappalardo, J 2004, 'The effect of mortgage broker compensation disclosures on consumers and competition: a controlled experiment', Federal Trade Commission, accessed on 28 January 2022, https://www.ftc.gov/reports/effect-mortgage-broker-compensation-disclosures-consumers-competition-controlled-experiment

RECOMMENDATIONS

CHOICE's recommendations to the Review are underpinned by three desired outcomes. These are:

1. Recognition of the increasing value of data in the Australian economy.
2. Increased corporate responsibility where information asymmetries between consumers and entities are not exploited.
3. Well-resourced regulators that hold appropriate and relevant powers.

1. Recognition of the increasing value of data in the Australian economy

CHOICE is pleased with the proposed changes to the definition of 'personal information'. In particular, CHOICE supports Proposal 2.4 which amends the definition of 'collection' to cover information that is inferred and generated. **Expanding the definition of 'personal information' recognises the increasing value of data in the Australian economy. Generated insights on consumer behaviour, sentiment and preferences are of equal use and value to traditional types of personal information and should be appropriately regulated.**

The business model of customer loyalty schemes is dependent on the collection, use and onselling of consumer data, including inferred and generated insights. These schemes are widely used in the Australian context, with almost 90 per cent of Australian consumers estimated to be a member of a loyalty scheme.[2] The popularity of customer loyalty schemes combined with the risk of harm that has been identified by the Australian Competition and Consumer Commission ('**ACCC**') in its review of customer loyalty schemes strongly indicate that this sector should be captured under the Privacy Act.[3] CHOICE recommends that customer loyalty schemes are included in the scope of the Privacy Act. They should not be given any special exclusions or carve-outs.

2. Increased corporate responsibility where information asymmetries between consumers and entities are not exploited

CHOICE supports proposals which ensure entities do no harm rather than simply asking a consumer to consent to potential harm arising from the collection, use or disclosure of personal information. Entities should work in the best interests of those whose data they collect, use or disclose. This would allow for a norm shift in which entities consider first and foremost the user of the product and service and assess potential risks from that perspective.

---

[2] ACCC 2019, *Customer loyalty schemes - final report*, accessed on 28 January 2022, https://www.accc.gov.au/publications/customer-loyalty-schemes-final-report, p 6

[3] ACCC 2019, *Changes needed to protect consumers using customer loyalty schemes*, Release number 228/19, accessed on 28 January 2022, https://www.accc.gov.au/media-release/changes-needed-to-protect-consumers-using-customer-loyalty-schemes

Specifically, CHOICE supports Proposals 10.1 and 10.2 which stipulate that information handling must be fair and reasonable in the circumstances. **It is simple: when a consumer provides their information, they expect it to be used for the express purpose of providing the good or service. They do not expect that it will be used for other purposes, including onselling, direct marketing, and informing artificial intelligence models.** We maintain that entities should be accountable to consumers and only use information provided for purposes that are reasonably expected to provide a good or service. When entities are providing consumer data to third parties, the types and names of these third parties and potential uses of the data should be provided in a privacy policy to increase transparency for consumers.

There are certain acts and practices which should be restricted and prohibited under the Privacy Act. Prohibited practices should include the sale of personal information on a large scale (data broking) and AI systems used in social scoring[4].

The burden of responsibility should not be placed on the individual but rather on the entity to regulate their practices and identify and mitigate privacy risks. This is particularly pertinent when the entity may be engaging in restricted activities. A useful parallel can be drawn to product safety. The manufacturer is best placed to design and incorporate safety features into a product rather than this responsibility being placed on a consumer to assess, based on limited information at point of sale, whether a product is inherently safe or may cause harm.

We recognise the value of the proposed Privacy Impact Assessments (PIA) model but believe this could also go further. Instead of simply being an internal record keeping requirement, entities engaged in high risk practices should submit these PIAs to the Office of the Australian Information Commissioner ('**OAIC**'). The OAIC would review the PIAs to ensure compliance with the Privacy Act.

When an entity is using automated decision making (ADM), particularly in essential markets, they should be upfront with its use to determine decisions about consumers, be transparent about how decisions are made and provide mechanisms to challenge decisions. A risk framework which categorises use of ADM into low, high and unacceptable risk could be provided by the OAIC to assist entities in understanding what is a 'no go' zone. The OAIC should also release guidance on high risk and restricted practices for entities.

Finally, consumer privacy should be treated the same regardless of the size, structure or sector of an entity. CHOICE supports the removal of the exemption for small businesses.

[4] Social scoring, sometimes called social credit, is an automated system used to assess a person's trustworthiness or likely future behaviour. Similar to credit reporting that judges a person's ability to repay a debt from their past financial behaviours, social scoring algorithms attempt to predict how likely a person is to behave a certain way based on their past behaviours, as gleaned from personal data.

3. Well resourced regulators with appropriate powers

An effective regulator is one that is well resourced and responsive to emerging issues. CHOICE supports additional enforcement powers for the OAIC, in line with other regulatory bodies like the ACCC.

The Government should establish a federal ombudsman that handles privacy complaints. This will support the OAIC in its regulatory efforts and sector analysis. This ombudsman does not necessarily have to deal exclusively with privacy complaints. As suggested by the Consumer Policy Research Centre, an ombudsman could handle complaints that arise in the digital context.

The ombudsman should regularly report complaints data including issues raised and outcomes. This would assist the OAIC, consumer protection regulators and consumer advocacy organisations to target their work.

Summary of recommendations

Proposal number	Discussion Paper - Draft Recommendations	CHOICE position
2.1, 2.2, 2.3, 2.4, 2.5	Definition of personal information	Support.
3.1, 3.2	Flexibility of the APPs	Support.
4	Small business exemption	Support the removal of the exemption.
8.1, 8.2, 8.3	Notice of collection of personal information	Support but APP 5 notices under APP 5.2 should also include the names of third parties as well as the types of third parties to whom the entity may disclose the personal information.
9.1	Consent to the collection, use and disclosure of personal information	Support, noting that entities should abide by the reasonable expectations of individuals when it comes to the collection, use and disclosure of personal information. Entities should not use information for purposes other than reasonably expected to provide a good or service.
10.1, 10.2, 10.3	Additional protections for collection, use and disclosure of personal information	Support.
11.1	Restricted and prohibited acts and practices	Support Option 1 but the condition of 'large scale' should be removed. 'The sale of personal information on a large scale' should be categorised as a prohibited practice.
12.1	Pro-privacy default settings	Support.
16.1, 16.2, 16.3	Direct marketing, targeted advertising and profiling	Support. Customer loyalty schemes should also be tightly regulated in line with other forms of direct marketing.
17.1	Automated decision-making (ADM)	Support. The Act should introduce 'no-go' zones and the requirement for entities to proactively state their use of ADM when consumers seek their services. There should be clear mechanisms for consumers to challenge automated decisions made by an entity.

Part 1: Scope and application of the Privacy Act

Definition of ‘personal information’: Proposals 2.1-2.5

CHOICE supports the proposed amendments to the definition of ‘personal information’ as put forward in proposals 2.1 to 2.5. This less prescriptive definition expands the range of information capable of being covered by the definition, ensuring that the Privacy Act is fit for purpose and relevant as new types of personal information may emerge in the future.

Consumers are already subject to practices where traditional types of personal information such as name, address, age, date of birth and contact details, are now being collected alongside other types of information, such as inferred or generated information. This inferred or generated information is increasingly valuable in the data economy, with businesses of varying sizes using this information to personalise offerings, target and profile consumers. It is crucial that these types of information are incorporated into the definition of ‘personal information’.

CHOICE supports the proposed non-exhaustive list of technical information presented on page 27 of the Discussion Paper. The expanded definition of personal information should include:

- an identifier such as a name;
- an identification number;
- location data;
- an online identifier, for example IP addresses and device ID numbers; and
- one or more factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person.

Flexibility of the APPs: Proposals 3.1-3.2

CHOICE supports Proposals 3.1 and 3.2 to allow the Information Commissioner to make an Australian Privacy Principles (‘**APP**’) code, either temporary or permanent, on the direction or approval of the Attorney-General where it is in the public interest to do so without first having to seek an industry code developer and where there is unlikely to be an appropriate industry representative to develop the code.

It is not appropriate for APP codes to be developed solely by industry participants as the codes developed in this way will likely favour the needs and practices of businesses, leading to distorted outcomes for consumers. As an independent representative, the Information Commissioner is best placed to develop APP codes, in close consultation with civil society (including consumer advocates and privacy experts) alongside industry representatives.

Small business exemption

CHOICE supports the removal of the small business exemption from the Privacy Act in order to standardise privacy protections for consumers across the economy. Businesses of all sizes should strive to ensure the privacy of their customers is safeguarded. It should not be up to the consumer to determine the level of risk they will accept depending on the size of the business they are interacting with. In line with other consumer protection frameworks like the Australian Consumer Law, people should be able to expect a baseline of protection regardless of the size of business.

A consistent and uniform approach to privacy across the economy will increase trust and confidence amongst consumers as they can make assumptions that their personal information is being treated in accordance with the law, regardless of the size of the business they interact with.

CHOICE encourages the OAIC to support small businesses to meet their compliance obligations through education and support services. This can only be achieved through adequate funding provided to the OAIC to undertake this work. CHOICE has seen similar work carried out by the ACCC in relation to product safety requirements under the Australian Consumer Law.[5]

[5] ACCC 2022, *Compliance*, accessed on 28 January 2022, https://www.productsafety.gov.au/product-safety-laws/compliance

Part 2: Protections

Notice of collection of personal information: Proposals 8.1-8.3

CHOICE supports the introduction of an express requirement in APP 5 that privacy notices must be 'clear, current and understandable'.

CHOICE has undertaken research into the length and number of privacy policies that consumers must consent to in order to access goods and services. On average, Australians are asked to read and consent to 116 privacy policies or 467,000 words, equivalent to 31 hours in reading time.[6] CHOICE also conducted an analysis of 75 privacy policies. We found that they average 4,000 words and take approximately 16 minutes to read. However, the longest privacy policy we analysed contained 14,861 words and would take nearly an hour to read. Additionally, most privacy policies have poor readability, with a third requiring university-level reading skills to easily understand them.[7]

It is unfeasible for the average consumer to regularly read through such lengthy and complex privacy policies, which are usually accompanied by a suite of other 'terms of use' policies. Increasing the clarity of privacy policies will allow for more meaningful consent and increase transparency for users.

CHOICE supports the proposal (8.2) to clarify the interaction between privacy notices and privacy policies. A privacy notice that clearly indicates what is most relevant to an individual to make a consensual decision is critical in empowering consumers. The matters detailed in Proposal 8.2 are useful for a consumer to make an informed decision.

In regards to the 'the types of third parties to whom the entity may disclose the personal information', CHOICE would like to see the names of third parties clearly identified within privacy policies. This has recently been proposed in the *New York Privacy Act 2021* which proposes that companies need to provide the identity of each processor, including third parties to whom personal data is disclosed, transferred, or sold.[8] The inclusion of the identification of third parties within privacy policies would allow for increased transparency for consumers and increase accountability for those entities that collect, share and use personal information.

CHOICE supports Proposal 8.3 to introduce standardised privacy notices that include standardised layouts, wording and icons. CHOICE has seen the successful implementation of

[6] Longmire, M 2022, *Drowning in privacy policies: CHOICE calls for reform*, CHOICE, 28 January, accessed on 28 January 2022, https://www.choice.com.au/privacyreform

[7] Blakkarly, J 2022, *Privacy policy comparison reveals half have poor readability,* CHOICE, 28 January, accessed on 28 January 2022, https://www.choice.com.au/consumers-and-data/protecting-your-data/data-laws-and-regulation/articles/privacy-policy-comparison

[8] *Assembly Bill A680B* (NY), accessed on 3 February 2022, https://www.nysenate.gov/legislation/bills/2021/A680

standardised notices in a range of consumer markets, including in food labelling through the country of origin labelling scheme and in energy labelling for whitegoods. As with any initiative that aims to provide consumers with useful information to aid in their decision making, any standardised privacy notices should be tested among consumers to ensure their effectiveness.

Consent to the collection, use and disclosure of personal information: Proposals 9.1-10.3

CHOICE broadly supports that consent be defined in the Act as being 'voluntary, informed, current, specific, and an unambiguous indication through clear action' (Proposal 9.1). However, CHOICE is concerned by the overreliance on consent as a solution to empowering consumers in relation to their privacy.

Instead, entities should abide by the reasonable expectations of individuals when it comes to the collection, use and disclosure of personal information. Entities should not use information for purposes other than reasonably expected to provide a good or service. We reiterate that instead of requiring an individual to understand the nuances of how a product or service may be harmful for them, it is preferable to prevent the harm itself.

CHOICE supports Proposal 10.1 and 10.2 where the collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

CHOICE also supports Proposal 10.3 where an entity that does not collect information directly from an individual must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Restricted and prohibited acts and practices: Proposal 11.1

Principles

CHOICE supports Option 1 in Proposal 11.1 as this option aligns with CHOICE's view that the burden of responsibility should not be placed on the individual but rather on the entity to regulate their practices and identify and mitigate privacy risks. This is particularly relevant when the entity may be engaging in restricted activities. As stated above, a parallel can be drawn to product safety in which the manufacturer is best placed to design and incorporate safety features into a product rather than this responsibility being placed on a consumer to assess harm.

However, the proposal does not go far enough. CHOICE would like to see the introduction of an obligation for entities to act in the interests of people whose data they hold and use. This could take the form of a best interest duty, as is being explored by some jurisdictions in the United States, or a broader obligation to act in the collective interests of a large group, similar to obligations that apply to superannuation fund trustees. This would allow for a norm shift in which

entities consider first and foremost the user of the product and service and assess potential risks from that perspective.

Categories of risk

There are certain acts and practices which should be categorised as restricted or prohibited due to the risk of harm posed to consumers. These practices exploit information asymmetries between the entity and consumers and can result in discrimination, refusal or exclusion from essential services or products, and may exacerbate vulnerability.

It is crucial that identified restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures if they are engaging in these high-risk practices, including lodging a PIA for approval with the OAIC (see page 14). CHOICE agrees with the proposed restricted practices in Option 1 but queries the usefulness of the 'large scale' condition. If an entity is engaging in a restricted practice, which due to the sensitive nature of the information it is holding could cause harm, it should not matter if the information collected is from 10 or 10 million people. As such, the 'large scale' qualifier should be removed in Option 1.Equally, 'the sale of personal information on a large scale' should be categorised as a prohibited practice.

Option 1 as proposed in the Discussion Paper:APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- Direct marketing, including online targeted advertising on a large scale;
- The collection, use or disclosure of sensitive information on a large scale;
- The collection, use or disclosure of children's personal information on a large scale;
- The collection, use or disclosure of location data on a large scale;
- The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software;
- The sale of personal information on a large scale;
- The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale;
- The collection, use or disclosure of personal information for the purposes of automated decision making with legal or significant effects; or
- Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

CHOICE suggests the following for **restricted acts or practices**:

- AI informed decision-making including profiling;
- the use of methods of tracking that individuals cannot control, for example, device fingerprinting;
- the offering of incentives to consent to the commercial exploitation of personal data i.e. customer loyalty schemes;
- the secondary use of data for targeted/ personalised marketing;

- online tracking for targeted/ personalised marketing purposes; and
- AI systems that evaluate creditworthiness.

CHOICE suggests the following for **prohibited acts or practices**:

- the collection of physical biometric data[9] including genetic data as a requirement for providing goods and services or entering into a contract including life insurance;
- the for-profit trade in personal data through data brokers i.e. the sale of personal information on a large scale;
- publishing personal information with the intended purpose of charging individuals for its removal;
- covert surveillance by an organisation through audio or video functionality of the individual's own device unconnected to the fulfillment of a service;
- AI systems used in social scoring[10]; and
- the collection of location data unconnected to the fulfillment of a service.

Guidance

Identified prohibited practices should be legislated in the Act with clear guidance provided by the Commissioner on what constitutes 'fair and reasonable' so that an entity engaging in any emerging practices can make an assessment as to whether the practice could be classified as prohibited or high-risk. The Commissioner should be able to amend the list of restricted and prohibited practices and provide guidance on these, if new and emerging high risk practices are identified, from time to time.

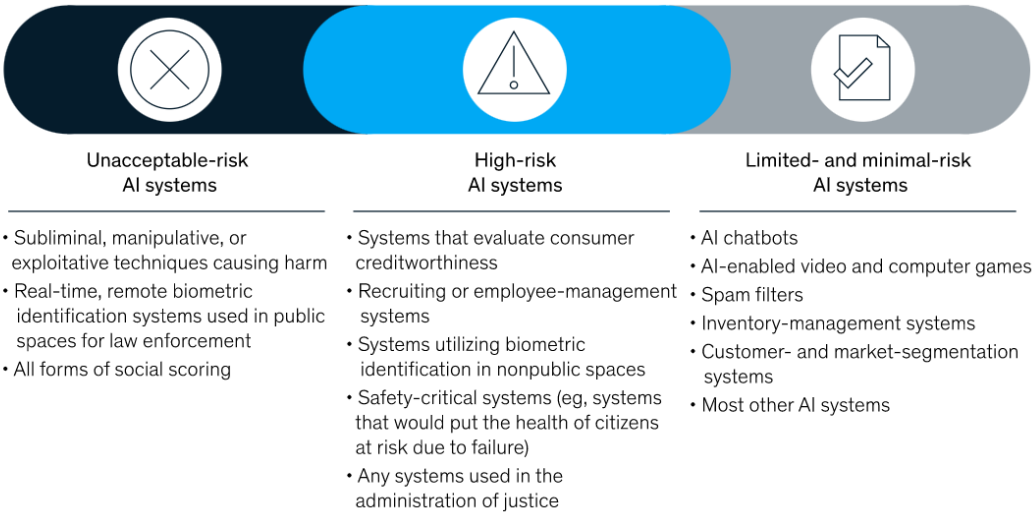
Similarly, the Commissioner could develop a risk framework for restricted practices to assist entities in identifying the potential harms arising from such practices and strategies to mitigate these. CHOICE refers to the European Commission's proposed AI regulations which details three levels of risk which are unacceptable, high and limited/minimal risk.[11]

[9] Physical identification methods may include face shape and geometry, fingerprints, the shape and structure of the skull, retina or iris, palm, hand, or finger geometry, facial thermography, hand thermography.
Recfaces 2020, *Types of biometrics*, accessed on 28 January 2022, https://recfaces.com/articles/types-of-biometrics

[10] Social scoring, sometimes called social credit, is an automated system used to assess a person's trustworthiness or likely future behaviour. Similar to credit reporting that judges a person's ability to repay a debt from their past financial behaviours, social scoring algorithms attempt to predict how likely a person is to behave a certain way based on their past behaviours, as gleaned from personal data.

[11] European Commission 2021, *Regulatory framework proposal on artificial intelligence,* accessed on 28 January 2022, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

The European Union's draft AI regulations classify AI systems into three risk categories.



McKinsey & Company, 2021[12]

Privacy Impact Assessments

We see value in the proposed Privacy Impact Assessments (PIA) model but believe this could also go further. For the PIA model to be successful, PIAs should be:

- publicly available - to increase accountability to the public whose data may be used in a restricted practice.
- made available in an OAIC-approved standardised format - to allow easy comparison for policymakers, privacy and consumer advocates, and the public.
- reviewed and approved by OAIC for high risk restricted practices (those most likely to cause harm). This would keep entities accountable to the Act and give OAIC proactive oversight over potential risks arising from restricted practices.

Pro-privacy default settings: Proposal 12.1

CHOICE supports Option 1 for Proposal 12.1 where an entity that offers a product or service that contains multiple levels of privacy settings must pre-select those privacy settings to be the most restrictive. CHOICE believes that this default setting should restrict personal information handling that is not strictly necessary for the provision of the product or service. Equally, entities should not be able to exclude individuals who choose the pro-privacy default setting from accessing the product or service.

[12] McKinsey & Company 2021, *What the draft European AI regulations mean for business*, accessed on 28 January 2022, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/what-the-draft-european-union-ai-regulations-mean-for-business

Direct marketing, targeted advertising and profiling: Proposals 16.1-16.3

CHOICE supports the introduction of a right to object to any collection, use or disclosure of personal information by an entity for the purpose of direct marketing. In particular, we support Proposal 16.3 where APP entities would be required to include information in their privacy policy about whether the entity uses third parties in the provision of online marketing materials. APP entities would be required to disclose the details of third parties as well as information regarding the appropriate method of opting-out of online marketing materials.

Customer loyalty schemes

CHOICE believes that customer loyalty schemes should not be regulated differently to other forms of direct marketing. We encourage the Government to avoid creating distinctions and carve-outs for different sectors. Consumers should be able to trust that if they are interacting with a business of any size, structure or sector that their personal information will be handled appropriately and in accordance with the law. CHOICE recognises the popularity and perceived value of customer loyalty schemes to consumers; this is a key reason why this sector should be tightly regulated in line with other forms of direct marketing.

The ACCC in its 2019 Review of Customer Loyalty Schemes has rigorously highlighted the harms of customer loyalty schemes left unregulated.[13] Harms include the profiling of consumers based on the data collected and the potential for different consumers being offered different prices for an identical product or service, as well as increasingly targeted advertising enabled by the sharing of consumer insights with third parties. CHOICE urges the Government to ensure that customer loyalty schemes are regulated in line with other entities undertaking direct marketing.

Automated decision making: Proposal 17.1

Automated decision making (ADM) is playing an increasingly larger role in people's lives as more organisations and businesses incorporate it into their practices. When used in essential markets, ADM unchecked can result in detrimental consumer outcomes such as refusal or exclusion from essential services, higher costs and discrimination. Often entities using ADM offer no accountability to the consumer whom decisions are being made about. Equally, the consumer has no mechanism for either knowing an entity is using ADM, what data is considered as part of the decision or how to challenge those automated decisions.

While notice is useful, we urge the Government to consider tighter controls on the use of artificial intelligence in consumer markets. For example, the Government should introduce both 'no-go' zones and the requirement for entities to proactively state their use of ADM when consumers seek their services. There should be clear mechanisms for consumers to challenge automated decisions made by an entity.

---

[13] ACCC 2019, *Customer loyalty schemes - final report*, accessed on 28 January 2022, https://www.accc.gov.au/publications/customer-loyalty-schemes-final-report

CHOICE supports Proposal 17.1 where privacy policies are required to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on people's rights. This should be supplemented with a list of non-exhaustive examples that meet this threshold.

Part 3: Regulation and enforcement

Enforcement: Proposals 24.1-24.9

We need well-resourced regulators with appropriate powers to ensure consumer rights and protections are safeguarded in a digital environment. To ensure this, CHOICE supports the following proposals:

- Proposal 24.1: introduce tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses.
- Proposal 24.2: clarify what is a 'serious' or 'repeated' interference with privacy
- Proposal 24.3: the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the Information Commissioner's investigation powers.
- Proposal 24.4: amend the Act to provide the Information Commissioner to undertake public inquiries and reviews into specified matters.
- Proposal 24.7: introduce an industry funding model similar to ASIC's incorporating two different levies:
    - A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and
    - A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.
- Proposal 24.8: amend the annual reporting requirements in the Australian Information Commissioner Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.

Alternative regulatory models

CHOICE supports Option 2 - the creation of a federal ombudsman that handles privacy complaints. This model would allow for the OAIC to undertake strategic reform and sector analysis while the ombudsman is dedicated to handling disputes.

We support the Consumer Policy Research Centre's hybrid proposal that this ombudsman should have a wider remit to encompass complaints arising from digital harms. If a consumer has a complaint that has arisen in a digital context, it would be easier for them to identify the digital ombudsman as the right place to seek redress than to determine what type of harm it is, such as a breach of privacy, discrimination or consumer rights. We note that not all breaches of privacy occur in a digital environment but that looking forward, the risk of harm and potential breaches of privacy are likely to occur online.

CHOICE recommends that the digital ombudsman should:

- be governed by a board with an independent chair and equal numbers of directors with industry and consumer backgrounds;
- be funded by industry through a transparent process;

- be free to consumers when they lodge a complaint;
- be subject to strong accountability mechanisms, including regular independent reviews (with the reports and the body's responses to recommendations reported publicly) and will have an 'independent assessor' to review how disputes are handled (but not to review the outcome of individual disputes);
- report entities that fail to comply to the appropriate regulator;
- monitor, address and report systemic issues to the relevant regulator e.g. OAIC, ACCC, Australian Human Rights Commission; and
- engage in outreach activities to raise awareness amongst consumers (in particular consumers experiencing vulnerability) and entities engaging in the digital economy (particularly small business).

A direct right of action: Proposal 25.1

CHOICE supports the creation of a direct right of action as described in Proposal 25.1, as this would assist in increasing consumer bargaining power and access to justice. We support the proposed design elements on page 190 of the Discussion Paper:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the Federal Circuit Court.
- The claimant would first need to make a complaint to the OAIC (or FPO) their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.