CHOICE

SUBMISSION TO THE ATTORNEY-GENERAL'S DEPARTMENT

PRIVACY ACT REVIEW

MARCH 2023

57 Carrington Road Marrickville NSW 2204

Phone 02 9577 3333 | Email campaigns@choice.com.au | www.choice.com.au

CHOICE

About Us

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.

CHOICE

Contents

CHOICE

Introduction

Australia's privacy laws are stuck in the 1980s, when consumer data collected by businesses was often limited to home phone numbers and home addresses. Now with highly advanced digital technology becoming more common, businesses are collecting more data – from email addresses and IP addresses to shopping behaviour, browsing history, and even biometric data like facial features and genetic code.

This dramatic surge in data collection has exacerbated power imbalances between businesses and consumers. Businesses can track, analyse, and understand consumers in ways never thought possible. This allows businesses to manipulate consumer behaviour, provide or exclude consumers from their goods and services based on deeply personal characteristics, and discover consumers' private values, beliefs, and activities.

This has heightened privacy risks – a single data breach can expose extremely sensitive information from millions of people. Additionally, the advent of automated decision-making has ushered in risks of discrimination and exclusion based on algorithmic analysis of personal data. This is a pressing concern for all consumers, particularly from groups experiencing vulnerability.

In response to these risks, consumer expectations have changed. Many have lost trust in businesses' ability to treat their data in a fair and safe manner. Consumers also know that businesses have so far dodged accountability by exerting their market power, forcing people to consent to their own harms rather than try and mitigate those harms in the first place. Reforms in other areas of consumer protection have forced manufacturers to make safer products, whether they are car airbags or children's toys, rather than just disclosing harms – and consumers expect the same fair and reasonable data protections from businesses.

The Privacy Act Review (**'the Review'**) is a chance to reset this power imbalance to create a fairer and safer system. Modernising Australia's privacy laws will make them more fit-for-purpose in an increasingly digital world, and create an even playing field between consumers and businesses. In this Review, CHOICE has identified three key priority areas to make a fairer market possible:

1. **Establish a "fair and reasonable" test for data collection.** This strengthened definition will require businesses to only collect and use data for the purpose of providing consumers with a good or service, and remove unneeded data in a timely manner.

2. **A broader definition of "personal information".** A broader definition of personal information which includes information that "relates to" an individual will ensure the privacy framework is relevant in today's digital environment.

3. **Ensure people have stronger consumer protections from all businesses and harmful emerging practices.** Urgent regulation of emerging harms including automated decision-making ('**ADM**') and facial recognition is needed to protect people from harm. The small business exemption should also be removed to ensure people have consistent protections.

Almost every consumer CHOICE asked (99.6%) believed that all businesses should have a legal obligation to consider their safety and well-being when handling personal information.[1] People shared with CHOICE experiences of data misuse and data breaches, being forced to disclose unnecessary amounts of data to purchase goods and services, and being needlessly inundated with targeted advertising. These consumer experiences have informed CHOICE's response to the Review and are quoted throughout the submission.

The Review is a major step in the right direction. While there are opportunities to strengthen some proposals, CHOICE urges the Government to implement many of the Review's recommendations.

[1] CHOICE, 2023, 'Privacy Reform', March, 9253 responses from CHOICE supporters.

CHOICE

Recommendations

Summary of Privacy Act recommendations

#	Proposal (in brief)	CHOICE position
4.1	Redefine personal information from “about” to “relates to”.	Support.
4.2	Include a non-exhaustive list of information which may be personal information.	Support. This can be strengthened with additional examples of information which are definitive types of personal information.
4.3	Redefine “collection” to cover information obtained from any source and by any means.	Support.
4.4	Include a non-exhaustive list of circumstances to assess “reasonably identifiable”.	Amend to include as a factor that an individual is “reasonably identifiable” if they are able to be distinguished from all others, even if their identity is not known.
6.1	Remove the small business exemption.	Support.
6.2	In the short-term, remove small business exemption from businesses collecting biometric information and trading in personal information.	Support. This short-term measure should be expanded to include other high-risk practices which use sensitive information.
12.1	Fair and reasonable collection, use, and disclosure of data.	Support.
12.2	Factors in determining fair and reasonable collection, use, and disclosure of data.	Support. Safety and fairness should be factors in determining reasonable use.
13.1	APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.	Support. A risk-based framework for prohibited or restricted practices should be included either into legislation or OAIC guidance.
13.2	Consider risk assessment for facial recognition and biometric information in 13.1 requirements.	Support.
18.1	Right to access.	Support. However Proposal 18.1(e) which would allow

		businesses to charge a nominal fee to access data should be removed.
18.2	Right to object to collection, use, or disclosure of personal information.	Support.
18.3	Right to erasure.	Support. However, there should be clear guidance on what information should be quarantined for law enforcement reasons.
18.4	Right to correction.	Support.
18.5	Right to de-index online search results containing personal information.	Support.
18.6	Exceptions to all rights of the individual.	Support. However, 18.6(c) should be amended to specify the limited circumstances where technical exceptions can apply, and prohibit businesses from purposely creating technical impossibilities.
18.7	Informing individuals about their rights.	Support.
18.8	Reasonable assistance to individuals.	Support.
18.9	Reasonable steps to respond to individuals.	Support.
18.10	Reasonable timeframe to acknowledge receipt of individuals requesting their rights.	Support.
19.1	Privacy policies setting out types of information used in substantially automated decisions.	Support.
19.2	High-level indicators of decisions with legal and similarly significant effects.	Support.
19.3	Right to request information about how automated decisions are made.	Support.
20.1	Introduce definitions for direct marketing, targeting, and trading.	Support.
20.2	Unqualified right to opt-out of personal information being used or disclosed for direct marketing purposes.	Support with amendments. Direct marketing without consumer consent should be prohibited and individuals should have to opt-in to receive direct marketing.

20.3	Unqualified right to opt-out of personal information being used for targeted advertising.	Support. However, targeted advertising should be captured by amending Proposal 4.4 to define an individual as "reasonably identifiable" if they are able to be distinguished from all others, even if their identity is not known.
20.4	Consent must be obtained to trade in personal information.	Amend to prohibit trade in personal information.
25.1	Tiers of civil penalty provisions.	Support.
25.2	Remove the word "repeated" and clarify "serious" with recommended features.	Support.
26.1	Direct right of action.	Support.
27.1	Statutory tort for serious invasions of privacy.	Support.

Summary of additional reforms

CHOICE also supports the Federal Government adopting additional reforms to strengthen Australia's privacy framework. The Federal Government should:

Recommendations
Introduce a best interests duty for data holders by extending the best interests of the child in Proposals 16.4 to all consumers.
Initiate a broad-ranging inquiry into the use and harms of automated decision-making and artificial intelligence. This inquiry should consider whether risk-based regulation is appropriate to manage the emerging risks.
Introduce legislation to regulate the use of facial recognition technology. This should incorporate a risk-based framework for the development and use of FRT. It should prohibit high-risk uses of FRT aside from limited exemptions.
Increase funding for the Office of the Australian Information Commissioner to ensure it is well-resourced to enforce the law.
Legislate a prohibition on unfair trading practices into the Australia Consumer Law and the *Australian Securities and Investment Commissions Act 2001 (Cth).*

1. Safety and care in data use

Implement a fair and reasonable use test

> *"I can't help feeling that there is a lack of respect from businesses for all the personal information they collect, and a lack of duty of care to their obligation to protect all this information. We customers should feel safe and confident that we are protected, but the way things are going we cannot trust anybody."*[2]
>
> – Rhea's* story

Businesses regularly collect excessive or unnecessary amounts of consumer data which they do not need. 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 on-selling, direct marketing, or informing artificial intelligence models. Businesses should be required to minimise and mitigate harm, rather than simply asking a consumer to consent to potential harm arising from the collection, use or disclosure of personal information.

CHOICE supports Proposal 12.1 which will amend the Privacy Act to require that the collection, use and disclosure of personal information must be fair and reasonable. Businesses should only collect and use data for the purpose of providing consumers a good or service, and remove unneeded data in a timely manner. Nationally representative research by CHOICE found that 64% of consumers were concerned about businesses collecting data about them, including capturing their behaviours, location, attitudes, and transactions.[3]

Businesses should bear the burden of identifying and mitigating privacy risks in their practices – not individuals. This is particularly clear when businesses are engaging in high-risk 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.

[2] CHOICE, 2023, 'Privacy Reform', March, 9253 responses from CHOICE supporters. All names have been pseudonymised for privacy reasons.
[3] CHOICE Consumer Pulse January 2023 is based on a survey of 1,030 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from January 23rd to February 14th 2023.

CHOICE also supports Proposal 12.2 to legislate factors which may be taken into account in the fair and reasonable use test. These factors should also be strengthened to have a stronger focus on prioritising safety for consumers. Safety and fairness should be factors in determining reasonable use. CHOICE supports clarification in Proposal 12.2(e) – "whether the impact on privacy is proportionate to the benefit" – in the Explanatory Memorandum, which should clarify that benefits are for individuals and not businesses, and only in specific situations where public interest is relevant.

Recommendations

Support Proposal 12.1 to amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.

Support Proposal 12.2 that when determining whether a collection, use or disclosure is fair and reasonable in the circumstances, matters proposed by the Review may be taken into account. Safety and fairness should be factors in determining reasonable use.

Legislate a best interests duty for data holders

> *"Protecting the interests of their customers should be paramount – we should not be made to feel unsafe for the sake of business profits."*
>
> – Mark's* story

CHOICE recommends that a fair and reasonable use test should be supported by a general best interests duty for data holders. Businesses should work in the best interests of those whose data they collect, use or disclose. Currently, only 12% of consumers trust companies to use the data they collect about them responsibly and in their interests.[4] A best interests duty would require businesses to consider their product and service users and assess potential risks from that perspective. This is a position held by other advocates in the consumer movement including the Consumer Policy Research Centre and Financial Rights Legal Centre. A best interests duty would recognise that consumer data is of significant value and importance to consumers. It would ensure there are strong obligations on businesses to treat their data with safety and care.

A best interests duty for data holders could be modelled on the best financial interests duty in superannuation. Trustees and directors of superannuation funds are required to act in the best

[4] CHOICE, 2023, 'Consumer Pulse January 2023'.

financial interests of their superannuation members.[5] This relationship of "one-to-many" could be applied to the privacy framework with businesses being required to act in the best interests of all their customers. The duty also has a reversal of the evidential burden, so trustees have to provide evidence to support the contention they are acting in the best financial interests of their members.[6]

CHOICE supports Proposals 16.4 which would require businesses to consider the best interests of the child as part of the fair and reasonable test. All consumers, especially people with a disability or people experiencing vulnerability, deserve protection from data misuse and other harms. The Federal Government should extend this proposed best interests duty to include all consumers, not just children.This would align with overseas jurisdictions that have analogous duties, including the Consumer Duty in the United Kingdom.[7]

Recommendation

The Federal Government should introduce a best interests duty for data holders by extending the best interests of the child in **Proposal 16.4** to all consumers.

2. Widening the scope of protected data

Redefine personal information

> *"Businesses need to be transparent, they need to disclose (if requested) all data points they hold on you, including those that are inferred…"*
>
> – Oscar's* story

The Review's Proposals 4.1 to 4.3 will strengthen the framework for personal information collection and consumer protections. Personal information is narrowly defined in the Privacy Act as information "about an identified individual, or an individual who is reasonably identifiable".[8] However, in a digital context, this creates loopholes for inferred data (new data generated through personal information, like consumer profiles and behaviour) and technical data (such as location data, IP addresses, device IDs). This inferred and technical data is increasingly

[5] Superannuation Industry (Supervision) Act 1993, s52.
[6] Superannuation Industry (Supervision) Act 1993, s220A.
[7] Financial Conduct Authority UK, 2022, 'A new Consumer Duty – Feedback to CP21/36 and final rules', https://www.fca.org.uk/publication/policy/ps22-9.pdf.
[8] *Privacy Act 1988*, s6(1).

valuable in the data economy, with businesses of varying sizes using this information to personalise offerings, as well as target and profile consumers. As long as businesses can target individual consumers based on inferred and technical data – even if it's de-identified – consumers can still be harmed by predatory practices. It is crucial that these types of information are incorporated into the definition of "personal information".

CHOICE strongly supports Proposal 4.1 to amend the definition of personal information to information which "relates to" an individual. This new definition will expand the range of information covered by the definition, ensuring that the Privacy Act is fit-for-purpose and relevant as new types of personal information emerge in the future. CHOICE also supports Proposal 4.3 to amend the definition of collection to expressly cover information obtained from any source and by any means, including inferred or generated information. Additionally, Proposal 4.2 to include a non-exhaustive list of information which may be considered personal information to assist APP entities (such as relevant businesses) will also help protect personal information.

While Proposals 4.1 to 4.3 provide consumers with more protection over their identified data, people may still be harmed by inadequate protections for possibly identifiable or de-identified data. Research has demonstrated that de-identified data is often re-identifiable.[9] For example, a team of researchers from the University of Melbourne re-identified de-identified data in an open medical dataset.[10] In order to address some of these concerns, Proposal 4.4 should be amended in line with Salinger Privacy's proposed recommendations on 'individuation'. Individuation is when an individual can be reasonably identifiable if they can be "singled out" in a crowd, even if their identity is not known. This will ensure consumers are protected from individuating data practices even when businesses claim their personal identity is not expressly known, such as in targeted advertising.

Recommendations

Support Proposal 4.1 to redefine personal information from "about" to "relates to".

Support Proposal 4.2 to include a non-exhaustive list of information which may be personal information. This can be strengthened with additional examples of information which are definitive types of personal information.

[9] Culnane C, Leins K., 2020, 'Misconceptions in Privacy Protection and Regulation', Law in Context, *36(2)*, pp. 49-60.
[10] ZDNet, 2017, 'Re-identification possible with Australian de-identified Medicare and PBS open data', https://www.zdnet.com/article/re-identification-possible-with-australian-de-identified-medicare-and-pbs-open-data.

Support Proposal 4.3 to amend the definition of "collection" to expressly cover information obtained from any source and by any means, including inferred or generated information.

Amend Proposal 4.4 to include as a factor that an individual is "reasonably identifiable" if they are able to be distinguished from all others, even if their identity is not known.

Consumers should have consistent protections

> *"...Businesses need to understand they are the caretaker of their customers' data, not the owner, and should treat data as such. Small businesses in particular need specific training on data security. All businesses should have to acknowledge understanding of the revised Privacy Act in order to retain their ABN. Failure should come with severe consequences such as deregistration. Businesses should undergo privacy audits in line with financial audits and work safe inspections."*
>
> – Marilyn's* story

CHOICE supports Proposal 6.1 to remove the small business exemption from the Privacy Act. This will ensure consistent privacy protections for consumers across the economy. Businesses of all sizes should be required 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.

For consumers, the size of the business is irrelevant to the harm they experience from a data breach or data misuse. In line with other consumer protection frameworks like the Australian Consumer Law ('**ACL**'), people should be able to expect a baseline of protection regardless of the size of business. CHOICE's survey of over 9,000 supporters found that 99.63% believed all businesses should have a legal obligation to consider safety and well-being when handling their personal information.[11]

CHOICE supports the Review's proposal for the Office of Australian Information Commissioner ('**OAIC**') to assist small businesses to meet their compliance obligations through tailored education and support services. The Australian Consumer and Competition Commission ('**ACCC**') performs a similar role to assist small businesses to understand product safety requirements under the ACL. Small business compliance with the Privacy Act should happen in a timely manner, to protect all consumers before more people are harmed.

[11] CHOICE, 2023, 'Privacy Reform', March, 9253 responses from CHOICE supporters.

Given the scope of potential harm, the small business exemption as it relates to biometric data must be dealt with urgently. CHOICE supports Proposal 6.2(a) for the Federal Government to make short-term amendments to prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption. The Government should also adopt Proposal 6.2(b) and remove the exemption for small businesses that obtain consent to trade in personal information. CHOICE recommends the Federal Government expand this list of sub-clauses to include other small businesses which handle sensitive and high-risk data.

Urgent action should be a temporary measure, as the entire small business exemption should be removed to ensure consistent privacy protections for all consumers.

Recommendations

Support Proposal 6.1 to remove the small business exemption.

Support Proposal 6.2 to remove in the short-term the small business exemption for the collection of biometric information for use in facial recognition technology and small businesses that obtain consent to trade in personal information. This short-term measure should be expanded to include other high-risk practices which use sensitive information.

Strengthen the legal rights of consumers

> *"Customers should have absolute control as to what data can be stored and shared as the current system simply tells us what they will do with our data and if we don't accept it, then we cannot use that platform/service. It is very unfair. So it is basically putting the controls to the customer's hand since it is not theirs to share or use for any gain."*
>
> – Jakub's* story

In principle, CHOICE supports Proposals 18.1 to 18.10 which will provide people with stronger legal rights in the digital economy. However, a number of these proposals need to be strengthened or amended.

Proposal 18.1(e) would allow businesses to charge a "nominal fee" for accessing an individual's data. It is unfair to require individuals to pay to access their own data, data that was collected by businesses for their own interests. This would also create additional barriers to people with lower incomes. The United Kingdom Government considered whether it should re-introduce a

nominal fee for processing data requests.[12] However, it decided in 2022 to not introduce a fee, citing the view of stakeholders that it "could disadvantage more vulnerable people in society."[13] The Australian Government should align with the United Kingdom and not allow businesses to charge a fee for a person to access their own data.

CHOICE supports a right to erasure in Proposal 18.3. This will empower consumers to have greater agency over their own personal data and give tangible effect to withdrawal of consent. Research by the Consumer Policy Research Centre in 2020 found that 89% of consumers considered this right to be fair (71% very fair and 18% fair).[14] Proposal 18.3(c) would allow businesses to quarantine certain limited information as opposed to erasing it if it could be required for law enforcement purposes. Strong safeguards are needed to prevent businesses from using this exemption as a loophole to needlessly keep people's data. A definitive list should be produced on what kind of information this is or how it will be determined, as well as protocols for how to make this practicable.

Proposal 18.6(c) would allow technical exceptions to all rights of the individual where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request. The ambiguity of these terms may allow businesses to find loopholes to comply with these rights, or create data systems which would make it technically impossible to comply with the rights. In order to protect the rights of the individual and their data, Proposal 18.6(c) should be amended with an exhaustive and definitive list of instances where technical impossibilities would be accepted.

Recommendations

Support Proposal 18.1 to provide individuals with a right to access, and an explanation about, their personal information if they request it, with a list of recommended features. However Proposal 18.1(e) which would allow businesses to charge a nominal fee to access data should be removed.

Support Proposal 18.2 to introduce a right to object to the collection, use or disclosure of personal information.

[12] United Kingdom Government, 2022, 'Data: a new direction - government response to consultation: Consultative Outcome', https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation
[13] United Kingdom Government, 2022
[14] Consumer Policy Research Centre, 2020, '2020 Data and Technology Consumer Survey', https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.

Support Proposal 18.3 to introduce a right to erasure with a list of recommended features. However, there should be clear guidance on what information should be quarantined for law enforcement reasons.

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

Support Proposal 18.5 to introduce a right to de-index online search results containing personal information.

Amend Proposal 18.6 to specify the limited circumstances where technical exceptions can apply, and prohibit businesses from purposely creating technical impossibilities.

Support Proposal 18.7 that individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.

Support Proposal 18.8 that an APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.

Support Proposal 18.9 that an APP entity must take reasonable steps to respond to an exercise of a right of an individual.

Support Proposal 18.10 that an organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding.

Regulate automated decision-making

> *"I don't like businesses using my responses to influence the information they subsequently choose to give me. I much prefer to have a free choice and not be subject to algorithms which serve the interests of the business, contrary to my own interests."*
>
> – Elsa's* story

Automated decision-making (**'ADM'**) is playing an increasing role in people's lives as more businesses incorporate it into their practices. Businesses that collect personal data can use this data to make automated decisions about a consumer's access to the service or prices of goods.

The Review notes the Privacy Act does not expressly regulate ADM, but this technology still has major privacy and transparency implications.

ADM can create and exacerbate existing discrimination, bias and market inequalities. Businesses often use ADM with limited or no accountability to the consumer about the decisions being made about them. This is especially concerning when ADM is used in essential markets as it can result in harmful outcomes such as refusal or exclusion from essential services, higher costs and price discrimination. Consumers have no way of knowing an entity is using ADM, what personal, technical, or inferred data is being considered as part of the automated decision, or how to challenge those automated decisions.

There is widespread community concern about the use of ADM by businesses. Nationally representative research conducted by CHOICE in January 2023 found that 70% of consumers were concerned about their data being used in automated decision-making which may affect their access to products and services.[15]

CHOICE supports Proposals 19.1, 19.2 and 19.3 which will give consumers more transparency into substantial decisions made by ADM which will affect them, as well as creating guidelines on what some of these decisions may be. CHOICE supports clear guidance in the Explanatory Memorandum on what "legal or similarly significant effects" covers. This will give consumers more confidence in the digital marketplace. CHOICE investigations into Airbnb and Tinder found possible uses of algorithms to, respectively, exclude or differentiate pricing for customers.[16] Detailing whether cases like this are considered "legal or similarly significant effects" will give consumers more assurance that ADM and AI will not be used to unjustifiably affect their access to goods and services.

Policy solutions addressing the harms of ADM must be focused on algorithmic fairness and transparency. Businesses which develop or use algorithms should be required to ensure their algorithms meet community expectations on fairness, safety and accuracy. The regulation of ADM and AI are issues which go beyond the scope of the Review. CHOICE also supports a broad-ranging Government inquiry into the regulation of ADM and AI and acknowledges work is being undertaken by the Department of Industry, Science and Resources. However, the inquiry into ADM and AI should be holistic, as it impacts on a wide range of issues, including consumer markets, digital platforms, individual rights, and financial services.

[15] CHOICE, 2023, 'Consumer Pulse January 2023'.
[16] CHOICE, 2022, 'Is Airbnb using an algorithm to ban users from the platform?', https://www.choice.com.au/airbnb; CHOICE, 2020, 'Tinder charges older people more', https://www.choice.com.au/tinderprices.

We recommend the Federal Government consider introducing stronger regulation on the use of ADM and artificial intelligence ('**AI**') in consumer markets. For example, the Federal Government should introduce both "no-go" zones and the requirement for businesses to proactively state their use of ADM when consumers seek their services. There should also be clear mechanisms for consumers to challenge automated decisions made by an entity.

This review into AI should also consider the appropriateness of legislating a risk-based framework to restrict and prohibit certain uses of ADM. CHOICE supports the Federal Government legislating a risk-based framework to restrict and prohibit certain uses of ADM. This can be achieved either by expanding OAIC's Privacy Impact Assessment ('**PIA**') compliance scheme to cover businesses and to incorporate a risk-based framework on ADM or establishing separate legislation which regulates the use of artificial intelligence including ADM.

Recommendations

Support Proposal 19.1 that privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

Support Proposal 19.2 that high-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act.

Support Proposal 19.3 to introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

The Federal Government should initiate a broad-ranging **inquiry into the use and harms of automated decision-making and artificial intelligence.** This inquiry should consider whether risk-based regulation is appropriate to manage the emerging risks.

Protect people from facial recognition and other biometric technology

> *"Tech companies i.e. [search engine] obviously use people's data to target them with advertising, demonstrating that they are collecting certain types of data without 'informed' consent. While this is currently being used for marketing, in future people may be denied access to products or services based on data that tech companies have obtained, or via the racial and other profiling which occurs*

when biometrics and facial recognition are used (usually without any consent whatsoever).“

– Amirah’s* story

Data collection by businesses has advanced considerably since the establishment of the Privacy Act in the 1980s – from phone numbers and addresses to capturing biometric data like facial features through facial recognition technology (**‘FRT’**)**.** The use of FRT has a number of risks, including data breaches involving biometric data, inaccurate assessments leading to exclusions, and could also hardcode biases such as racial discrimination. CHOICE is concerned that FRT could also be used to further enrich and monetise consumer data. CHOICE’s investigation uncovered the use of facial recognition technology by major retailers in Australia.[17] As a result of this investigation, OAIC commenced an investigation into Bunnings Group Limited and Kmart Australia Limited’s use of facial recognition.

CHOICE supports the Review’s proposals relating to FRT. In the short-term, Proposal 6.2(a) will prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption. Proposal 13.2 considers how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities.

Businesses are increasingly adopting this technology and more needs to be done to restrict or prohibit its use. There is an urgency to regulate the FRT given the market asymmetries and human rights implications of its use. Consumers deserve assurance that their biometric information is not being exploited while comprehensive legislation lags behind.

CHOICE strongly supports the FRT model law proposed by Professor Ed Santow and the UTS Human Technology Institute.[18] This model law takes a human rights risk-based approach and prohibits high-risk uses unless exemptions were granted by OAIC, for national security and law enforcement, or for genuine academic research. There is widespread community support for regulating FRT. A nationally representative survey conducted in March 2022 found that three in four Australians agree that regulation is needed to prevent harms caused by facial recognition in

[17] CHOICE, 2022, ‘Kmart, Bunnings and The Good Guys using facial recognition technology in stores’, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store

[18] Human Technology Institute, 2022, Facial Recognition Technology: Towards a model law, https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf.

retail settings.[19] The Federal Government has an opportunity to implement an innovative and sorely needed piece of legislation to protect the safety and privacy of consumers.

Recommendations

Support Proposal 6.2(a) to prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption.

Support Proposal 13.2 to consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities.

The Federal Government should legislate a **facial recognition technology law.** This should incorporate a risk-based framework for the development and use of FRT. It should prohibit high-risk uses of FRT aside from limited exemptions. This could be achieved by incorporating HTI's model law on FRT into the Privacy Act or legislating the model law on FRT separately.

Direct marketing, targeting and trading

> *"I have major concerns about how businesses capture and monetise consumer data. It concerns me that businesses are enabled through data collection to predict customer behaviour. Customers are now bombarded with advertising which is unsolicited and unwanted. The on-selling of data to other businesses should be stopped. I see most data collection as an invasion of my privacy. It is a practice which is increasingly abused, leading to the mistrust and suspicion of many businesses."*
>
> – Antonia's* story

CHOICE supports Proposal 20.1 to introduce definitions in the Privacy Act for direct marketing, targeting and trading. Nationally representative research by CHOICE found that consumers are concerned about data practices associated with marketing. 56% of consumers were concerned

[19] CHOICE Consumer Pulse March 2022 is based on a survey of 1,034 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from the 22nd of March to 7th of April 2022.

about how their data is used to personalise products or services which are advertised or marketed to them.[20]

Consumers should have the unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes and targeted advertising purposes, outlined in Proposal 20.2 and Proposal 20.3. However as it is currently expressed, this places the onus solely on consumers to opt-out of harmful practices. Businesses should be required to acquire opt-in consent before using direct marketing and targeted advertising, as well as allowing individuals to subsequently opt-out.

Businesses can use targeted advertising without expressly identifiable information. This is still a concern as consumers can still be individually tracked, analysed, and marketed to by businesses. This means they are individuated from others. CHOICE supports amending Proposal 4.4 to define an individual as "reasonably identifiable" if they are able to be distinguished from all others, even if their identity is not known. This will restrain the use of harmful targeted advertising towards individuals. This will also place the responsibility for not using harmful practices on businesses, rather than requiring consumers to opt-out of all harmful practices, especially in situations where this is not possible.

CHOICE also opposes the loophole in Proposal 20.2 which would allow entities to still collect personal information for direct marketing without consent, provided it is not sensitive information and the consumer has the ability to opt-out. This kind of data collection can potentially individuate people and deduce sensitive information. It is unfeasible and onerous to require individuals to opt-out of every instance of non-consensual direct marketing.

While Proposal 20.4 would be an improvement, CHOICE recommends that trade in personal information should be prohibited. This practice carries significant risks of data breaches, exploitative practices and misuse, and deprives consumers of the financial and personal values of their own data. Data brokers hold thousands of attributes on billions of people, gained by scraping the web and buying and collecting information from a multitude of sources. These vast data sources can be used for personalised pricing and for discriminatory applications of automated decision-making.

There is widespread community concern about the practices of data brokers. Nationally representative CHOICE research found that 76% of consumers were concerned by businesses selling their data to data brokers.[21] When CHOICE asked over 9,000 of its supporters in March,

[20] CHOICE, 2023, 'Consumer Pulse January 2023'.
[21] CHOICE, 2023, 'Consumer Pulse January 2023'.

98% believed all businesses should be banned from on-selling personal information to other companies.[22]

Recommendations

Support Proposal 20.1 to introduce definitions for direct marketing, targeting and trading.

Support Proposal 20.2 to provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. However, direct marketing without consumer consent should be prohibited and individuals should have to opt-in to receive direct marketing.

Support Proposal 20.3 to provide individuals with an unqualified right to opt-out of receiving targeted advertising. However, targeted advertising should be captured by amending Proposal 4.4 to define an individual as "reasonably identifiable" if they are able to be distinguished from all others, even if their identity is not known.

Amend Proposal 20.4 to prohibit the trade in personal information.

3. Effective enforcement

Establish mandatory impact assessments for high-risk activities

> *"Having worked in an organisation that had to collect personal data for business purposes and for regulatory reporting, we were very careful with the data. We sourced software providers that had information security certification, and we didn't send unsolicited emails. I don't even like receiving emails from multiple brands that are owned by the same company when I signed up to only one brand."*
>
> – Emmanuel's* story

CHOICE supports the Review's Proposal 13.1 which will require that all entities covered by the Act to conduct a Privacy Impact Assessment (**PIA**) before commencing an activity which is likely to have a significant impact on the privacy of individuals. Private businesses collect and handle

[22] CHOICE, 2023, 'Privacy Reform', March, 9253 responses from CHOICE supporters.

vast amounts of consumer data. However, they are not held to the same standards of responsibility which are required of government agencies which have to use PIAs.

To be effective, PIAs must 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 Privacy Act and give OAIC proactive oversight over potential risks arising from restricted practices.

CHOICE also supports the recommendation that certain specific high-risk practices triggering a mandatory PIA are in the Privacy Act or included in OAIC guidance. The review should consider the following non-exhaustive list 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;
- AI systems that evaluate creditworthiness; and
- behavioural tracking for content generation.

CHOICE also suggests the following non-exhaustive list for prohibited acts or practices:

- the collection of physical biometric data 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 fulfilment of a service;
- AI systems used in social scoring to deny services or discriminate against consumers; and

- the collection of location data unconnected to the fulfilment of a service.

Recommendation

Support Proposal 13.1 that APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. A risk-based framework for prohibited or restricted practices should be included either into legislation or OAIC guidance.

Infringement notice powers and a tiered penalty system

> *"There must be hefty penalties for all businesses that fail to protect data. If businesses want to collect data, they must protect it, no excuses! The law must be framed so that any failure to protect data is considered a breach. The penalties need to be commensurate with the level of lost data – the larger the breach the higher the penalty."*
>
> – Niamh's* story

The Federal Government should appropriately resource and empower regulators to protect consumers in digital environments. The Privacy Act's current one-size-fits-all approach to only allowing penalties for serious and repeated interferences of privacy hampers the ability of OAIC to enforce the law. There has only been one business, Facebook, taken to court by OAIC. Regulations and laws are only as strong as their enforcement. Consumers have been let down by governments inadequately resourcing regulators, which has allowed businesses significant leeway to interfere with their privacy.

CHOICE supports Proposal 25.1 to create tiers of civil penalty provisions. A tiered system of penalties, based on the severity and size of the breach and the business, would give OAIC more options to better target regulatory responses. This proposal would also encourage businesses with smaller data breaches to disclose this information to OAIC and the public.

CHOICE also supports Proposal 25.2 to remove the word "repeated" as a necessary threshold alongside "serious", and to provide more clarity on what a "serious" interference with privacy means. Digital Rights Watch argues that businesses may see the "serious and repeated" threshold as a low risk, and potential fines as part of the cost of doing business.[23] Similarly, the

[23] Legal And Constitutional Affairs Legislation Committee Thursday, 17 November 2022.

Australian Privacy Foundation has observed that “the 'serious and repeated' test is a barrier to letting the regulator and the courts judge how to characterise each instance properly.”[24]

Recommendations

Support Proposal 25.1 to create tiers of civil penalty provisions to allow for better targeted regulatory responses.

Support Proposal 25.2 to amend section 13G of the Act to remove the word “repeated” and clarify that a “serious” interference with privacy may include the list of recommended features.

Statutory tort for invasions of privacy and direct right of action

> *“The customer seldom is given any information how the information will be used, is seldom given notice that their information may or will be on-sold, seldom given the right to opt out, and seldom given any worthwhile guarantees as to the security of the customer data banks – let alone having a reasonable chance of legal redress if they are subject to a data breach, or their personal data is misused.”*
>
> – Laurie’s* story

Consumers are best protected when there are effective and well-resourced regulators and dispute resolution bodies to protect their collective interests. This can be seen in the strength of Australia’s consumer protection regulators, the ACCC and ASIC, in improving outcomes for consumers in their relevant jurisdictions.

Consumers should have the right to represent their personal interests when faced with privacy harms, particularly for specific cases of individual harm that may not be broader or systemic in nature. CHOICE supports the creation of a direct right of action as described in Proposal 26.1. This will improve access to justice and assist in increasing consumer bargaining power. CHOICE also supports Proposal 27.1 which will establish a statutory tort for serious invasions of privacy.

[24] Legal And Constitutional Affairs Legislation Committee Thursday, 17 November 2022.

Recommendations

Support Proposal 26.1 to 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.

Support Proposal 27.1 to introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.

Adequate resourcing for OAIC

CHOICE recommends the Federal Government permanently increase funding to OAIC. This would make it fit-for-purpose and give the community the confidence in its regulatory powers to protect their interests.

In the aftermath of the Optus data breach, the Federal Government provided OAIC with $5.5 million to resource its investigation. However, multiple major data breaches have since occurred without further resourcing. Advocates have noted that OAIC is underfunded and has not been provided with adequate resources to enforce the law.[25] The Review recommends OAIC undertake a number of intensive tasks, including drafting new guidance and communicating to the community. This will require adequate resourcing for OAIC to achieve. CHOICE encourages the Federal Government to consider funding mechanisms to ensure OAIC is an effective regular and is well-resourced to undertake litigation.

Recommendation

The Federal Government should increase funding for the Office of the Australian Information Commissioner to ensure it is well-resourced to enforce the law.

4. Reforms beyond the Privacy Act

Economy-wide ban on unfair trading

While not within scope of the Review, the Federal Government should pass an economy-wide prohibition on unfair trading to strengthen consumer and privacy protections. CHOICE welcomed the commitment in September 2022 by Commonwealth, State, and Territory

[25] Legal And Constitutional Affairs Legislation Committee Thursday, 17 November 2022.

consumer affairs ministers to consult on this proposed reform.[26] The ACCC's ongoing Digital Platforms Inquiry has recommended a prohibition on unfair trading to protect people from online harm.[27] By tackling both unfair practices and privacy reform, the Federal Government can reset the balance needed for a safer marketplace for consumers, and promote secure and fair digital products and platforms.

Recommendation

The Federal Government should legislate a prohibition on unfair trading practices into the Australia Consumer Law and the Australian Securities and Investment Commissions Act 2001 (Cth).

[26] SA Attorney-General's Department, Consumer Affairs Ministers meet in Adelaide, 2022, https://www.agd.sa.gov.au/about-us/news/consumer-affairs-ministers-meet-in-adelaide.
[27] ACCC, 2022, Digital platform services inquiry Interim report No. 5 – Regulatory reform, p. 64.