Submission by the
Financial Rights Legal Centre
Consumer Action Law Centre
Financial Counselling Australia

Attorney-General's Department

Privacy Act Review, Issues Paper, October 2020

November 2020

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 |
info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters.

About the Consumer Action Law Centre

Consumer Action is an independent, not-for profit consumer organisation with deep expertise in consumer and consumer credit laws, policy and direct knowledge of people's experience of modern markets. We work for a just marketplace, where people have power and business plays fair. We make life easier for people experiencing vulnerability and disadvantage in Australia, through financial counselling, legal advice, legal representation, policy work and campaigns. Based in Melbourne, our direct services assist Victorians and our advocacy supports a just market place for all Australians.

About Financial Counselling Australia

Financial Counselling Australia is the peak body for financial counsellors. Financial counsellors assist people experiencing financial difficulty by providing information, support and advocacy. Working in not-for-profit community organisations, financial counselling services are free, independent and confidential.

Introduction

Thank you for the opportunity to comment on the *Privacy Act* Review Issues Paper.

This is a joint submission from:

- The Financial Rights Legal Centre (Financial Rights);
- Consumer Action Law Centre (Consumer Action); and
- Financial Counselling Australia

This review of the *Privacy Act 1988* is well overdue. The pace of technological change towards a data saturated economy; the development of business models and markets centred on the harvesting of surplus behavioural data for predictive purposes; and the multiple, fragmented and haphazard approach to regulating the impacts of these changes has meant that the *Privacy Act* has become out of date and not fit for purpose in protecting Australian's privacy rights.

Australians want a safe and secure data environment that puts their privacy ahead of the increasingly rapacious data desires of industry. There is strong and clear evidence for this. According to OAIC's 2020 Community Attitudes to Privacy survey:[1]

- Australians consider the protection of their personal information to be a major concern in their life (70%)
- Australians would like the government to do more to protect the privacy of their data. (83%)
- Australians want to be protected against harmful practices (84%)
- Australians want increased rights around certain issues such as asking businesses to delete information (84%)
- Australians want the right to seek compensation in the courts for a breach of privacy (78%)
- Australians want to know when their personal information is used in automated decision-making if it could affect them (77%)
- Australians want the right to object to certain data practices while still being able to access and use the service (77%)

[1] OAIC, 2020 Australian Community Attitudes to Privacy Survey, September 2020, https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

- Australians are concerned about their children's privacy (91%)
- Australians do not want companies sharing their information for secondary purposes (81%).

This review therefore provides a critical opportunity to overhaul the regime to:

- build a *Privacy Act* that actually acknowledges, enlivens and appropriately re-balances Australians' right to privacy;
- create a holistic, principled, regulatory framework to protect our right to privacy, one that is fit for purpose in a data driven world;
- develop a robust Act that keeps apace of current and inevitable future changes in our economy; and
- meet community expectations and addresses Australians' concerns.

This submission addresses the important questions raised in the issues paper and outlines an approach that places the consumer and the community's interest at the heart and centre of much needed reform. In summary, this submission recommends:

- updating the Objectives of the Act to among other things recognise that Australians have a right to privacy and the Act must promote the protection of that right;
- updating concepts within the act (like "personal information") to keep pace with the rate of change;
- removing exemptions for small business;
- acknowledging the failures of disclosure, notice and consent as an effective regulatory tool that places all responsibility on consumers and shifting towards a regime that:
    - builds privacy and safety into the very design of data collection and handling processes;
    - overhauls notification and consent process to make them more effective – to the extent that they can be; and
    - targets consumer harm via other regulatory means.
- introducing higher privacy standards including:
    - restricting, limiting or prohibiting certain uses and disclosures that are anathema to privacy rights such as:
        - screen-scraping;
        - the secondary use and sale of personal data for targeted advertising purposes;

        - direct marketing;
        - the collection of genetic test results as a requirement for providing goods and services or entering into a contract including life insurance;
        - the offering of incentives to consent to the commercial exploitation of personal data;
        - the for-profit trade in personal data through data brokers/data vultures;
        - profiling that leads to unfair, unethical or discriminatory treatment contrary to human rights law;
        - collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual;
        - requiring passwords to social media accounts for the purpose of employee screening;
        - publishing personal information with the intended purpose of charging individuals for its removal;
        - collection of location data unconnected to the fulfillment of a service.
    - establishing a right to erasure, a direct right of action, a statutory tort and an unfair trade practices law;
    - strengthening the right to access one's personal data and information about its use and disclosure; the right to correction;
    - improving consumer protections for overseas data flows;
    - preventing the unnecessary collection of personal information in line with the data minimisation principle;
    - requiring mandatory deletion;
    - shifting the onus of privacy protection on to entities by creating fiduciary obligations on trustees to manage and exercise data privacy rights on behalf of, and in the best interests of, consumers.
- establishing specific privacy protections for children;
- increasing security requirements on those who collect and handle personal information;
- bolstering access and transparency rights; and
- addressing the complex web of legislative, regulatory and self-regulatory regimes that impact upon privacy through a principles-based governance framework.

Objectives of the Privacy Act

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

The objectives of the Privacy Act are out of step with community expectations. Increasing threats to privacy borne of the ubiquity of digital technologies and the development of business models and markets centred on the harvesting of surplus behavioural data for predictive purposes rather than serving the genuine needs of people have rendered the current law impotent.[2]

Australians generally consider that they have a 'right to privacy'—notwithstanding the absence of a national charter of rights. The Privacy Act needs to be strengthened to recognise this right to privacy.

The objectives of the Privacy Act should be updated to include the following objectives[3]:

a. recognise that individuals have a "right to privacy" and the Act promotes the protection of that right – rather than simply "promoting the protection of the privacy of individuals: under Section 2A(a);[4]

b. recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance protecting the privacy of individuals with other public interests – this is opposed to the current balance with the interests of entities in carrying out their functions or activities under Section 2A(b);

c. promote the *fair*, *safe*, responsible and transparent handling of personal information by agencies and organisations – to fill out the intention of the current reference to only "responsible" handling of personal information as currently referenced under Section 2A(d);

d. facilitate a *transparent and fair* credit reporting system that ensures that the privacy of individuals is protected – as opposed to "facilitating an efficient credit reporting

[2] This is the foundational idea behind the concept of 'surveillance capitalism': *"Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to product or service improvement, the rest are declared as proprietary behavioural surplus, fed into advanced manufacturing processes known as "machine intelligence," and fabricated into prediction products that anticipate what you will do now, soon and later. Finally these prediction products are traded in a new kind of marketplace for behavioural predications that I call behavioural futures markets."* Page 8 *The Age of Surveillance Capitalism*, Shosana Zuboff, 2019

[3] Some of which have previously been identified by Recommendation 5-4 of the ALRC 2008 report *For Your Information Australian Privacy Law and Practice*

[4] Recommendation 5-4(b) of the ALRC Report.

system while ensuring that the privacy of individuals is respected" currently under Section 2A(e);

e. provide *an avenue* for individuals to seek redress when there has been an alleged interference with their right to privacy – enhancing the current description under Section 2A(g);

f. provide an avenue for individuals to gain a comprehensible explanation about the handling of their personal information – an additional objective that is required to make Section 2A(g) meaningful - ie in order to be able to complain consumers need to understand what is happening to their information;

g. provide the basis for nationally consistent regulation of privacy and the handling of personal information – as is currently the case under Section 2A(c);

h. protecting the privacy of individuals in the flow of information across national borders enhancing the current description under Section 2A(f);

i. implementing Australia's obligations at international law in relation to privacy; (as already reflected in Section 2A(h)).

As we have outlined in previous submissions, the current application of the privacy laws tends to err on the side of being against the consumer interest.[5] This is because the Act seeks to balance privacy with the interest of business entities rather than with the public interest or other competing rights.

It is therefore critical that Section 2A(b) "recognis[ing] that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities" be removed and replaced.

It is not appropriate to balance the interests of the right to privacy with the right to businesses to carry out functions or activities that seek to exploit people's privacy for profit.

Business models have been developed that trade in acquiring, dealing and selling personal data much of which threatens the right of privacy and other public goods and produces few, if any, benefits to society.

The APPs currently only require APP entities to collect personal information by fair and lawful means, but do not contain any requirement that the use and disclosure of personal information must also be fair and lawful.[6]

The *Privacy Act* needs to facilitate the fair, reasonable and transparent collection, use and disclosure of personal data that serve public interest objectives.

---

[5] See Financial Rights Legal Centre, Submission to the ACCC Digital Platforms Inquiry, February 2019, p. 11 https://www.accc.gov.au/system/files/Financial%20Rights%20Legal%20Centre%20%28February%202019%29.PDF

[6] ACCC page 478

The Government needs to consider prohibiting certain uses and disclosures that inappropriately impact on, or undermine, the right to privacy: see further discussion below at **Question 40.**

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?

The definition of "personal information" is currently too limited and needs to capture technical information and inferred information.

GPDR Article 4(1) re: personal data recognises that a name is only one way that a person can be identified. Various online technical identifiers may equally identify an individual. Article 4(1) specifies that:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject')"; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Recital 30 expands on the relevance of online identifiers:

> *Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*

Under the GDPR, therefore, unique identifiers can constitute personal data. The same should apply under the *Privacy Act*.

'Personal information' in the *Privacy Act* should therefore include technical information such as an IP address, a URL, or other information and metadata which can be used to identify an individual, thus clarifying the effect of the decision of the Federal Court in *Telstra v Privacy Commissioner*.

3. Should the definition of personal information be updated to expressly include inferred personal information?

The definition of 'personal information' should be further expanded to capture inferred data and information – information collected and analysed revealing something new about an individual or data drawn from the profiling of or tracking of behaviours or movements such that an individual can be singled out (i.e. disambiguated from a crowd or cohort).[7]

[7] Australian Privacy Foundation https://www.accc.gov.au/system/files/Australian%20Privacy%20Foundation%20%28February%202019%29.PDF

Strategies and analysis that single out unique individuals and create a detailed picture of consumers expose consumers to growing risks of re-identification, manipulation, exclusion and discrimination. Including inferred information within the definition of personal information will provide consumers with improved protections under the *Privacy Act*.

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

Personal information will be 'de-identified' if the information is no longer about an identifiable individual or an individual who is *reasonably* identifiable: s 6(1). The OAIC have stated in their guidance on de-identification that de-identified information may technically be able to be re-identified, but it will not be 'reasonably identifiable' if there is almost no *likelihood* of identification occurring.[8]

There are however strong arguments that de-identification efforts are increasingly ineffective.[9]

The EU does away with the concept of de-identified data and focuses on anonymous and pseudonymous data.

"Anonymous data" is only considered as such if re-identification is *impossible*, that is, re-identifying an individual is impossible by any party and by all means likely reasonably to be used in an attempt to re-identify.[10]

"Pseudonymous data" is defined as:

> *"the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."*

Pseudonymisation is in practice only a security measure and in the EU it does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR:

> *Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.*

---

[8] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (Web Page, 21 March 2018).

[9] See, eg, Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 Law in Context/ Katherine Kemp outlines problems with current de-identification practices: https://www.accc.gov.au/system/files/Dr%20Katharine%20Kemp%20%2826%20April%202020%29.pdf "Firms stating that certain of their data practices only involve "de-identified", "anonymised" or "aggregated" data imply that this data is not about an identified individual or an individual who is reasonably identifiable. It is clear, however, that many businesses aim to distinguish, profile and interact with individual consumers by using "de-identified" data. They often achieve this objective by using "unique identifiers", that is, unique strings of numbers and/or letters that are assigned to a particular device or individual in the absence of a name or email address"

[10] Recital 26 of the EU General Data Protection Directive excludes anonymized data from EU data protection law.

The EU approach is therefore a stronger set of protections for consumers and should act as the basis for amending the *Privacy Act*.

5. **Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?**

No.

Flexibility of the APPs in regulating and protecting privacy

6. **Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?**

Scalability through the use of the phrase "reasonably necessary" and "reasonable expectation" ensures that an already inappropriate balance test between protecting privacy and the interests of businesses weighs the scales heavily in favour of the entities being regulated. Regulated businesses large and small will err on the side of lower costs rather than upholding the right to privacy, no matter how often reputational cost is put forward as a motivator. Relying on businesses to undertake a reputational cost benefit analysis has led to minimal improvements in privacy protections for consumers.

Greater prescription is required to ensure that the right to privacy is no longer trumped by commercial interests. Privacy rights should not be dependent on the vagaries of whether a consumer chooses to use the services of goods of a small, medium or big business.

Exemptions

Small business exemption

7. Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unneccessary compliance costs on small business?

No. No other jurisdiction has this exemption. Its removal has been recommended by a number of inquiries.[11]

The assumption that private sector organisations pose varying levels of risk to privacy is redundant given the ubiquitous digitalisation and networked connectivity of the economy. All entities collecting using, holding, analysing and disclosing data are subject to the threat of data breaches and open to mis-use or mis-handling. The size of the business should therefore no longer be a factor as to whether there is a low or high privacy risk. If anything – the lack of regulations and requirements has led to small businesses taking more privacy risks since they do not have to meet the current standards that apply to larger buisinesses.

This is acknowledged by the Issues Paper:

> *technology has changed the way that small businesses operate. These advancements may mean that small businesses are increasingly handling personal information and may now pose a higher privacy risk than previously. Consumer attitudes to privacy may also have evolved since the introduction of the private sector amendments. The results of the 2020 ACAP survey show 71 per cent of survey participants think small businesses should be covered by the Privacy Act.*[12]

No entity – small business, sole trader or otherwise – has the automatic right to conduct business in a manner that is inherently unsafe. All businesses irrespective of their size should respect and adhere to the right of privacy. No business should shirk from this responsibility. If they cannot afford to do so, then government needs to step in to support these businesses to meet these basic expectations, rather than providing an exemption.

This is a critical issue in the financial services sector particularly given recent proposals by the ACCC to allow non-accredited parties under the CDR regime to obtain CDR data.

We note too that the small business exemption is of particular concern to the EU and is a key outstanding issue between the EU and Australia.[13]

---

[11] The '*The real Big Brother: Inquiry into the Privacy Act 1988*' the Senate Legal and Constitutional References Committee recommended its removal. The ALRC Report 108 recommended its removal.

[12] Page 24; OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 60.

[13] Page 61 Issues Paper

8. **Is the current threshold appropriately pitched or should the definition of small business be amended?**

    a. **If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as number of employees or value of assets or should the definition be amended in another way?**

No exemption should be in place. The other factors listed here – number of employees, value of assets – have nothing to do with what the key objective of the *Privacy Act* should be: to uphold the right to privacy. One's privacy can be breached by a company with one employee and a company of 1000 employees. It is fundamentally unfair that a consumer who engages with a small business has fewer protections than someone who engages with a larger business.

9. **Are there businesses or acts and practices that should or should not be covered by the small business exemption?**

Again, we do not support a small business exemption. Any business that handles personal information should meet the requirements.

If this is not accepted, then at a minimum businesses that are currently proposed by the ACCC to be able to access and handle Consumer Data Right data as a non-accredited party should be subject to the *Privacy Act*.[14] This includes: accountants, lawyers, tax agents, BAS agents, financial advisors, financial counsellors, and mortgage brokers.

10. **Would it be appropriate for small businesses to be required to comply with some but not all of the APPs?**

    a. **If so, what obligations should be placed on small businesses?**

    b. **What would be the financial implications for small business?**

No.

11. **Would there be benefits to small business if they were required to comply with some or all of the APPs?**

The cost of complying with all of the APPs is outweighed by the benefits that will accrue to to small business. These benefits include:

- increased trust and confidence in small businesses' ability to safely and securely handle data;

[14] CDR rules expansion amendments Consultation Paper September 2020. https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf

- reduced likelihood of consumer complaints;
- placing small business on the same playing field as bigger businesses.

Lowering compliance costs should not be a reason to limit a consumer's right to privacy and places consumers who use exempted services at an unfair disadvantage.

12. Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their personal information?

No.

Employee records exemption

13. Is the personal information of employees adequately protected by the current scope of the employee records exemption?

No comment

14. If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

No comment

15. Should some but not all of the APPs apply to employee records, or certain types of employee records?

No comment

Political parties exemption

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

No comment

Journalism exemption

17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?

No comment

18. **Should the scope of organisations covered by the journalism exemption be altered?**

No comment

19. **Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?**

No comment

Notice of Collection of Personal Information

Improving awareness of relevant matters

20. Does notice help people to understand and manage their personal information?

Reliance on disclosure as a regulatory tool is ineffective[15]. The prevalence of wrap-click itunes-style agreements, long form terms and conditions and links to complex legalese means that people do simply not read or engage with them. This is exacerbated once vulnerabilities are taken into account – such as people with intellectual and physical disabilities, children, those with lower reading ages etc.

Information asymmetry impacts the ability for the consumer to understand. It places all the responsibility to comprehend and be informed of all relevant matters on the consumer.

In many circumstances the companies themselves do not understand what potential consequences may arise from the collection and use of the data.

Rather than forcing a consumer to understand how a product may be harmful for them, it is far preferable to hold organisations to account for providing that harmful product. This holds true for digital platforms as much as it does for other industries.

This is not to argue that notice should not be provided. It is clear that disclosure still has a role to play for instance, in contributing to transparency, integrity and efficiency, but it must be done effectively (see response to Question 22 below).

The measures to be taken should keep this mind and shift the onus away from consumers and raising their literacy back on to digital platforms and other providers to develop safer, more appropriate products and services in the marketplace.

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

The pendulum is too far swung towards minimising "regulatory burden" and lowering "compliance costs" as against enforcing the right to privacy.

Rather than relying on disclosure and placing the responsibility all on the consumer to be informed, obligations needs to be put in place to ensure that consumer protections are built in to the very design of data collection and handing processes. Businesses should be required to adhere to using the principles of

- privacy by design;
- security by design;

[15] ASIC REP 632 Disclosure: Why it shouldn't be the default, October 2019 https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/

- inclusiveness by design; and
- human rights by design.

We support introducing requirements recommended by ACCC[16] including:

- standardisation to simplify the information provided;
- using layered notices, standardised icons or phrases (but consumer tested);
- place requirements on the form and quality of the notice (see our response to the following section);
- Undertake a more prescriptive approach to the permitted and prohibited uses needs to be introduced - the more principled and vaguer, the more room to alter forms of uses and disclosures in such a way that the consumer will not comprehend and will be surprised by the use if informed afterwards.

22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?

Notification requirements under APP 5 to notify consumers of the collection of their data must be strengthened. It is currently left up to the APP entity to decide whether and how to provide notification under APP 5. This is no longer acceptable for a data-heavy economy.

In the *Privacy Act* context notice should be provided in all circumstances of collection and at the time of that collection, unless the individual already has the information or there is an overriding legal or public interest reason. Technology is available to make this happen.

This would mean that the elements of "reasonable in the circumstances" and "as soon as practicable" under APP5 needs to be removed.

Notification should be:

- concise,
- transparent,
- intelligible
- easily accessible
- simple to understand and written in clear and plain language (particularly if addressed to a child);
- provided free of charge;
- informs the consumer of every use and disclosure, and
- consumer tested;

[16] In Recommendation 16(c) of the Digital Platforms Inquiry Report

Notice should also adhere to the "no surprises" principle – that is a consumer should not be express surprise post-purchase when informed of any particular use to which they consented.

This requires a serious re-think in the approach to notification and consent requirements.

APP 5 should also explicitly specify the information that must be set out in the notification, including:

- the identity and contact details of the entity collecting data;
- the data and categories of data collected;
- the purposes for which each type of data is collected; and
- whether the data will be disclosed to any third parties and, if so, which third parties and for what purposes.

The Consumer Data Right requires that a participant "must take steps" to notify rather than "must take reasonable steps." This should be the case under APP5.

Under the ACCC CDR Rules, notification must include "the data that has been requested."[17] The conception of data here is more specific than that proposed by Recommendation 8(a) which is the "types of data." "Types of data" has the potential to be much broader. Consideration needs to be had regarding the level of data description that is appropriate and what will be most comprehensible to a consumer. Once that is decided there needs to be consistency across the CDR and the *Privacy Act*.

Article 13 of the GDPR requires notification of:

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing[18]
- transfer personal data to a third country or international organisation[19]
- the period for which the personal data will be stored[20]
- the existence of the right to request from the controller access to and rectification or erasure of personal data[21]
- where the processing is based[22]
- the right to lodge a complaint[23]

[17] Rule 9.3.2, ACCC Consumer Data Right Rules Framework, September 2018,

[18] Article 13(1)(c)

[19] Article 13(1)(f)

[20] Article 13(2)(a)

[21] Article 13(2)(b)

[22] Article 13(2)(c)

[23] Article 13(2)(d)

- whether the provision of personal data is a statutory or contractual requirement[24]
- the existence of automated decision-making, including profiling[25]

All these should be included in any notification.

There should be no exemption where personal information is collected for non-commercial purposes and in the public interest. Full transparency should be required in *all* cases. While non-commercial cases may entail less risk of commercial exploitation, the collection of consumer data still involves significant risks including hacking and use for activities that they may not feel comfortable with or with to be a part, eg political, religious or other campaigning uses. A consumer should have a comprehensive right to know what data is being collected and how it is potentially going to be used, handled and stored.

It is important to reiterate that while notification is important, disclosure should not be relied upon to solve the problems raised by the ACCC report: outlined at Question 27 Third party collections

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

An individual should always be provided with notice when their personal information is collected, regardless of whether the collection is direct or indirect.

Specific information should be provided to alert the consumer to the fact that a third party is involved, that the third party have the same obligations and that the consumer has the same privacy rights.

If an entity does not have an individual's contact information a question arises as to whether the entity should be collecting the information at all. Further, if a third party, for any reason, cannot provide consumers with this information then the personal information should not be collected.

Limiting information burden

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

Limiting information overload requires a radical re-think in the nature and limits of disclosure; greater standardisation; consumer testing and a more prescriptive approach to permitted and prohibited uses and disclosures is necessary.

[24] Article 13(2)(e)

[25] Article 13(2)(f)

25. **Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?**

Yes – as outlined above.

Consent to collection and use and disclosure of personal information

Consent to collection, use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?

In theory consent is an important means of controlling personal information, and more broadly to express one's dignity and autonomy – that is each consumer should be free to decide how much or how little of their information they wish to share in exchange for a benefit.

However *in practice* the effectiveness of consent in a data context – particularly fully informed or meaningful consent – is limited. This is because:

- consent relies on disclosure as a tool to inform, a tool that has been acknowledged as a failure;
- consumers do not know what they are consenting to: there is substantial information asymmetry borne of the complexities of privacy agreements and terms and conditions the data market. Even if privacy statements are made clearer asymmetry will always exist because there is a structural incentive to "structuring the deal so that more financially valuable assets are procured from consumers than consumers would prefer."[26]
- consumers can not know what they are consenting to: the complex uses to which data will be put are not knowable to the user at the time of consent, in many cases precisely because the businesses company do not know themselves what the use will be.
- privacy preferences are difficult to institute: trying to put into effect one's privacy preferences is difficult if not impossible given the complexities involved in navigating this process in multiple, inconsistent, ever-changing ways across a large number of services and goods.
- declining to participate in data driven technologies is increasingly not an option for many consumers: Given the ubiquity of data driven services and collection - the choice to use or not use a service is simply not a free one to make, lest consumers drop out of society altogether.
- in many cases, sharing one's personal information is also sharing other people's information found within that information – information that these other people have not and cannot consent to sharing. For example, genetic information provided holds information about relatives, financial and banking data includes significant amounts of information about those with whom you transact (be it directly attributable or easily inferred information).

[26] Hoofnagle & Whittington, 2014 in Gordon Hull, Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data, Ethics and Information Technology 17:2 (2015), 89-101

- trade in personal data and businesses claiming behavioural data wherever it lays whenever they can get away with it, means that in many situations personal information is being collected without consent in the first place. For example the Google Street View photo-mapping public spaces, the use of trackers and Ad-Tech on websites, the development of shadow profiles on Facebook are all examples of companies laying claim to behavioural data and personal information bypassing the consent process entirely.

Consumers experiencing vulnerabilities are even more subject to the drawbacks of consent since they often have more limited literacy, even less experience with modern uses of data, and less ability to negotiate, object or seek redress.[27]

Reliance on the fiction of "informed" consent as it is currently framed can therefore only go so.

The solution is not necessarily to do away with the concept of consent altogether but to explicitly acknowledge the limited nature of "informed" consent, and use a full range of regulatory tools to ensure that the right to privacy and the consumer interest is protected.

The strategies must focus on both:

- improving the process of consent itself; and
- combatting and avoiding consumer harm via other regulatory means.

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

Ensuring that consent is freely given and informed is a difficult, if not impossible task. No particular design can ever guarantee this outcome. However, there are simple reforms to the APPs that can take place to at least improve the process in line with some of the improvements under the Consumer Data Right.

- consent needs to be more fully defined under the APPs. Meaningful consent should require:
    - a clear affirmative/express act;
    - that is freely given/voluntary (acknowledging that imbalance of power is sometimes present);
    - is specific as to purpose;
    - unbundled;
    - unambiguous;
    - time limited;
    - easily withdrawn;[28] and

[27] Dr. Katherine Kemp, Big Data, Financial Inclusion and Privacy for the Poor, Responsible Finance Forum, https://responsiblefinanceforum.org/big-data-financial-inclusion-privacy-poor/

[28] See Questions 38-39

    - informed
- entities should be required to obtain consent in relation to any and all:
    - collection;
    - use; or
    - disclosure

  unless the personal information is necessary for:
    - the performance of a contract to which the individual is party,
    - is required by law, or
    - an overriding public interest reason applies as recommended by the ACCC;
- all consent settings for data practices relying on consent to be pre-selected to 'off' ie. in favour of the consumer not consenting;
- introducing and requiring consistent consent processes including the use of standardised icons or phrases to facilitate comprehension and aid decision-making: see our response to Question 30;
- stop the unnecessary collection of personal information through introduction of the data minimisation principle: see our response to Question 29;
- introduce specific consent rules for children: see Question 33.

However, as outlined above, strengthening consent requirements will not necessarily solve all the shortcomings of consent as a tool to protect the right to privacy and prevent consumer harm. These changes need to be supplemented with a series of further reforms to the *Privacy Act*. They include introducing:

- Higher privacy standards embedded into the *Privacy Act* including
    - changing the objectives of the Act (Question 1);
    - broadening the definition of personal information (Questions 2-4);
    - removing exemptions (Question 7);
    - preventing the unnecessary collection of personal information in line with the data minimization principle (Question 29)
    - acknowledge the limitation of consent for things like the Internet of Things and introduce specific restrictions (Question 34);
    - restrict inferred data practices that are not in the best interests of the consumer (Question 35)
    - banning screen-scraping (Question 35);
    - prohibiting the secondary use and sale of personal data for targeted advertising purposes (Question 37);

- requiring higher security standards including a mandatory deletion obligation (Questions 43-44);
- strengthening the right to access one's personal data and information about its use and disclosure (Question 45);
- improving personal information correction rights (Question 45);
- introducing a right of erasure (Questions 46-47);
- strengthening consumer protection for overseas data flows (Questions 48-52);
- introducing a direct right of action, a statutory tort and unfair trade practices laws (Questions 56-62, 66);
- prohibiting the use of dark patterns – tricks to force a user to consent to something that they didn't mean to - via the introduction of a unfair trading practices law (see Question 67).

- More prescription regarding permitted and prohibited uses and disclosures to avoid harm altogether:

  See our response to Question 40;

- Improved and standardised notification requirements:

  See our response to Questions 21 and 22.

- Shift the onus of privacy protection on to entities by Introduce a legal framework that creates fiduciary obligations on trustees to manage and exercise data privacy rights on behalf of and in the best interests of consumers. This would require entities to only collect and process data in the interests of, and not in ways detrimental to, the subjects of the data.[29]

  The benefits of such an approach include:

  - limiting the information asymmetry where entities have much greater knowledge than their customers about how customers' data is used;
  - financially vulnerable people will not be required to give up their data protection rights to use digital services; and
  - establishing trust and confidence in consumers that their data are being used in a fair, safe and response ways.[30]

- Introduce an accountability regime in the form of post-purchase/post-service surveys to ascertain the effectiveness of consent processes:

[29] David Medine and Gayatri Murthy, *Making Data Work for the Poor: New Approaches to Data Protection and Privacy*, January 2020, https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf

[30] See Pages 14-15, David Medine and Gayatri Murthy, Making Data Work for the Poor

Performance or outcomes based regulation regulates the end result which a regulated entity must achieve. Its sets a measurable standard related to the regulator's goal and allows the regulated entity itself to choose how to meet that standard. It is largely used in the regulation environmental sector. An example in the environmental space is that an entity must achieve a specific level of emissions. An approach that should be considered in the consent regime could be to conduct testing and consumer surveys. Post-purchase/post-service surveys have the potential to ascertain the effectiveness of the consent process by testing consumer's understanding of the uses versus the actual uses of their data. It could potentially ascertain whether the consent was freely given. Requiring regulated entities to meet certain threshold standards for consent could ensure that business are incentivised to achieve certain levels of informed and freely given consent.

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

Yes. Businesses engage in what Kemp and Nicholls call 'concealed data practices' which refers to "a combination of overbroad use of consumer data and lack of transparency and choice for consumer.[31]" Practices can include:

- collecting a broad range of consumers' personal data and using that data for a wide range of broadly defined purposes;
- collecting, using and/or disclosing personal data well beyond that which is necessary to provide the user with the service they have sought;
- privacy policies that are too lengthy, broadly worded and/or confusing for the average consumer to read, understand and compare with other services
- hiding uses in the fine print of terms and conditions or privacy policies
- not identifying precise uses or identifying third parties and their uses.[32]

Without specificity uses or privacy practices will be obscured or concealed from the consumer undermining the meaningfulness of informed consent.

Consent should not be an 'all or nothing' proposition, which allows firms to impose unnecessary or unwanted data uses on consumers as a condition of using the core service.

Consent should be designed to ensure that it is:

- simple to understand; and
- does not lead to any surprises for the consumer down the track.

[31] Page 2, Kemp, Nicholls https://www.accc.gov.au/system/files/Katharine%20Kemp%20%26%20Rob%20Nicholls%20%28March%202019%29.pdf

[32] Page 2 Kemp Nicholls

As detailed above at Question 27 for meaningful consent to take place it must – along with other elements detailed - be

- unbundled; and
- specific as to purpose.

Unless otherwise prohibited, consent should specifically be required:

- for all uses of data that are not necessary for the provision of the service;
- where the consumer's personal information is used or disclosed for a purpose that is not in accordance with the consumer's own interests.[33]

Concepts of consent fatigue, burden or friction should not be used as an excuse to water down a strong consent scheme: see further details at Question 30.

29. Are the existing protections effective to stop the unnecessary collection of personal information?

a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?

No. The APPs currently permits firms to interpret the meaning of collection necessity (APP 3.1-3.2) and use or disclosure for related, secondary purposes (APP 6.2(a)) to their own advantage, potentially taking a broad view of what collection is 'necessary' for its primary purpose or when a secondary purpose can be said to be 'related' to the primary purpose for which the data was collected.[34]

The refusal of consent to a use that is not necessary should not be grounds to deny access to that product or service. The freemium model (upon which the digital sector is basing its business models) perpetuates poor consumer and social outcomes since the consumer becomes the product.

The Data Minimisation principle in Article 5 of the GPDR states:

> *(1)(c) Personal data shall be …adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*

The current formulation of this principle in the APPs under 3.1 and 3.2 is inadequate:

> *the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.*

This wording has allowed entities to define their activities in an overly broad manner. Combined with APP 6.2(a) which allows the use or disclosure of information that is in some way "related"

[33] Page 465 ACCC DPI

[34] Page 6 Kemp, Nicholls.

to the primary purpose has allowed – the intent to minimise data collection has in practice been a failure.[35]

The data minimisation principle should be made more effective in the *Privacy Act* to ensure that entities genuinely do not seek to collect more data than is specifically needed to fulfil their service to the consumer.

30. What requirements should be considered to manage 'consent fatigue' of individuals?

Concepts of consent fatigue, burden or friction should not be used as an excuse to water down a strong consent scheme.

Friction in the consent process –minor impediments slowing the process such as multiple screens – is not necessarily a bad thing. Yes, consumers generally seek convenience and speed over security and suitable products. However there are many cases where they do so to their own detriment. Frictionless transactions, for example, are already causing significant consumer harm in the online consumer space, for example the ease of accessing payday loans via mobile applications. We have also seen an increase in advice sought regarding the new PayID platform, due to the instant nature of transactions.

Some friction needs to be embedded into the data environment to enable better consumer decision making.

We support the strategies outlined in the DPI to address the consent fatigue including:

- the use of standardised icons or phrases to denote categories of personal information or categories of purposes
- seeking consent when they are intending to collect personal information other than in accordance with a contract to which the consumer is a party
- seeking consent when the purpose is not in accordance with the consumer's own interests;
- consumer testing the design of effective and meaningful consent processes;
- implementing post-purchase surveys to ascertain the effectiveness of consent processes;
- prohibiting certain uses, disclosures and practices: see Question 40.

[35] See the OAIC's response to Centrelink debt recovery system for an example: https://www.oaic.gov.au/updates/news-and-media/centrelink-debt-recovery-system/

Exceptions to the requirement to obtain consent

31. Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?

No comment.

Pro-consumer defaults

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Yes. Too often defaults are used to the advantage of the business over the interests of the consumer. Pro-consumer defaults should be used, noting that there are some uses and circumstances where pro-consumer defaults may not be effective enough to avoid harm. These practices should be prohibited.

Dark patterns and other unfair trading practices should be prohibited: see Question 67.

Obtaining consent from children

33. Should specific requirements be introduced in relation to how entities seek consent from children?

Yes. An appropriate framework upon which to design specific requirements under an updated *Privacy Act*, should include:

- an age limit for the concept of consent
- parental consent where the person is younger than this age, and
- age verification requirements.

We note that the EU's GDPR restricts the ability to consent to those 16 years (or potentially 13 years and above) depending on the State. Article 8 states:

Art. 8 GDPR Conditions applicable to child's consent in relation to information society services

1. *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*
2. *The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*

Children are particularly vulnerable to the allure of new technology and new apps and may not fully understand the consequences of any consents required nor the full range of contractual obligations. The current consent regime does little to account for children's use of digital technology and must be addressed urgently.

Minors are therefore highly vulnerable to exploitation and the risks versus potential benefits are high. For example, the Dollarmites program run by Commonwealth Bank in schools received a SHONKY Award in 2018 from CHOICE. The Dollarmites program works by offering commissions to primary schools in exchange for running the school banking scheme. The commissions include a one-off payment of $200 when the first student makes their initial deposit as well as annual rewards of up to $600 per year.[36] Recent investigations from Fairfax found that Commonwealth Bank staff fraudulently activated Dollarmite accounts for personal gain.[37]

YouTube was previously fined $170m by the US Federal Trade Commission (FTC) and New York State to settle allegations it collected children's personal data without their parents' consent. They found that the children's version of YouTube tracked information about what kids are watching in order to recommend videos and collected personally identifying device information.

The misuse of children's data and a lack of consent is particularly a concern since technologies provide the ability for individual consumers to retreat into private, hidden, digital spaces to transact. Given the ease, speed and inherently private nature of using these technologies, the usual social cues and hurdles that would work to potentially stop someone from accessing harmful or unsafe digital products and services are simply no longer there. These issues are a problem for adults but the situation is exacerbated when we consider the use of phones by minors and a willingness to hide activities from guardians and parents.[38]

Digital platforms should be required to demonstrate that they have verified someone's age and identity before acquiring consent to share and or CDR data.

The role of consent for IoT devices and emerging technologies

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

The nature of the interaction between consumers and Internet of Things (IoT) devices is such that current privacy protection approaches in relation to consent are incompatible and inappropriate. Restrictions on certain practices will be key to address the issues raised with IoT.

---

[36] https://www.commbank.com.au/personal/kids/school-banking/information-for-schools.html?ei=bld2-btn-information-for-schools

[37] https://www.smh.com.au/business/banking-and-finance/dollarmites-bites-the-scandal-behind-the-commonwealth-bank-s-junior-savings-program-20180517-p4zfyr.html

[38] Just as one example, Madhumita Murgia The secret lives of children and their phones, October 6, 2017 https://www.ft.com/content/7c972e2e-a88f-11e7-ab55-27219df83c97

Inferred sensitive information

35. Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?

No. The ability of businesses to infer information – and in fact build business models around such an ability - should be constrained.

There are situations where analysis of personal data held by an entity could assist the consumer. For example, analysing consumer financial data to identify that they are either a perpetrator or victim of financial or other abuse could be used to benefit the victim to provide actions or services that will assist that person. Lenders could also identify those who are experiencing financial hardship and provide appropriate support measures including offering to move people into basic bank accounts – as now required under the Banking Code of Practice.

More often though inferred information is used for reasons that do not serve their best interests such as for direct marketing purposes or political profiling, or could be used to identify information about an individual's health, religious beliefs, political affiliations, financial stress, their location etc, or re-identify a de-identified person or and subsequently mis-used or breached.

The Australian privacy law therefore must to establish consumer protections to prevent harms arising from inferred data that may be particularly sensitive or carry particular risks of harm.

The GDPR is clear that sensitive information (ie "special category data") includes not only personal data that specifies relevant details, but also personal data revealing or concerning these details. The *Privacy Act* must extend the definition of personal information and sensitive information to capture inferred data.

Any inferring of data that is not in accordance with the consumer's own interests should be prohibited.

Screen-scraping should also be prohibited (as it is in the EU and UK) since it:

- Promotes unsafe online practices actively deterred by government and industry;
- breaches bank terms and/or conditions, whereby losing E-payments Code protection;
- undermines the potential success of the safer Consumer Data Right environment;
- leads to errors and mistakes.[39]

Case study Annabel's story - C196186

[39] For a full description of the problems with screen-scraping see Pages 10-18, Financial Rights Legal Centre and the Consumer Action Law Centre submission to the Senate Select Committee on Financial Technology and Regulatory Technology https://financialrights.org.au/wp-content/uploads/2020/02/191223_FinTechInquiry_Sub_FINAL-1.pdf

About 2 years ago, Annabel got a loan a payday lender for $1,500. The lender uses a data aggregator with screen scraping technology to obtain required information for responsible lending checks.

In the 90 days before this loan was obtained, Annabel had entered into 2 other Small Amount Credit Contracts (**SACC's**) with the payday lender and was a debtor on 6 SACC's in total. This fact was noted in the loan application.

Annabel borrowed a further $700 in 2018.

Last September, Annabel's Centrelink benefit changed from DSP to Newstart, and Annabel was unable to afford repayments at the fortnightly rate of approximately $150.

In examining Annabel's situation, Financial Rights obtained documentation from the payday lender which was based on the use of a data aggregator's screen scraping tool.

The report was riddled with inaccuracies including:

1. Incorrect calculations with respect to her net monthly income which inappropriately took into account lump sum cash advance payments she received from Centrelink and assumed they were additional regular income.
2. Missing information with respect to EFTPOS payments.

Source: Financial Rights Legal Centre

Case study Gavin's story - C196186

Gavin has payday loans totaling $4,000. In December last year he applied for loans with a payday lender where he was declined on two applications but accepted into two other loans.

Gavin has struggled to pay the loans as he has Child Support of $400 per fortnight and rent. Gavin pays $400 a fortnight to the payday lender with fees of $80 for each loan per fortnight.

Financial Rights has begun representing Gavin but upon looking at the data aggregation provided for responsible lending purposes, it was riddled with errors – including categorizing his café payments for coffee as rent.

Source: Financial Rights Legal Centre

36. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

Yes.

Direct marketing

37. Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

No. The current APP7 is manifestly inadequate.

> **Case study –Directing marketing complaint against Acquire**
>
> In 2015 Consumer Action Law Centre lodged a representative complaint against Acquire Learning and Careers Pty Ltd and related entities (Acquire) on behalf of job seekers who provided their personal details in the hope of getting a job, only to receive calls from telemarketers selling vocational education courses. The Privacy Commissioner was asked to investigate whether, among other things, Acquire complied with its obligations under the Australian Privacy Principles (APPs) when carrying out direct marketing calls to Australians who had provided their details when applying for jobs. The complaint regarding direct marketing was not upheld by Privacy Commissioner, even though a few years later ACCC took enforcement action in relation to unconscionable conduct & misleading conduct for similar conduct.
>
> *Source: Consumer Action Law Centre*

At a minimum consumer should provide their express consent before a business can provide a service that includes as a primary purpose direct marketing. For example, a comparison or switching service.

The secondary use of data for targeted/personalised marketing and the sale of personal data in any form for the same purpose should be prohibited. This is because:

- tracking and surveillance of consumers has introduced too many privacy risks for consumers and broadening the potential attack surface of the consumer's personal information;[40]

[40] "Behavioural advertising relies on far greater collection, use and storage of personal data than contextual or traditional advertising, since it depends on profiling and targeting consumers based on data about their past behaviour and not merely their immediate interaction with the publisher, Page 6, Kemp, Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper

- there is growing evidence that personalized ads are ineffective[41]
- personalized advertising can be more manipulative[42]
- behavioural analysis and inferring personal information leads to inappropriate discriminatory practices. Data analysis can allow advertisers to select the very specific segments of the population they think are most likely to want their products. This can have benign impacts such as the sale of women's shoes to those with an interest in online women's fashion or it lead to abuses such as the exclusion of minorities;
- lack of transparency about the practices and the inability to attain fully informed consent;[43]
- The negative impact personalized and behavioural advertising has on social and democratic process.[44]

If prohibition is not accepted the following protections must be introduced as a minimum:

- Consumers should have the right to know exactly who their data is being shared with – the use of terms such as "third party" or "affiliate"
- The right to erasure needs to be introduced.
- A right to bring actions for a breach
- Any direct marketing that occurs that is reliant in part or in whole by the use of personal data should
    - clearly identify the original source of the consent chain – ie if a consumer has agreed that a neo-Bank can data to a direct marketers to direct market on behalf of a credit union – the advertising must identify the source of the data – ie the neo Bank.
    - what it is being used for;
    - provide easy ability to withdraw consent and erasure.

https://www.accc.gov.au/system/files/Dr%20Katharine%20Kemp%20%2826%20April%202020%29.pdf"

[41] Arwa Mahdawi, Targeted ads are one of the world's most destructive trends. Here's why, The Guardian, 6 November 2019, https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy and Page 6, Kemp, Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper https://www.accc.gov.au/system/files/Dr%20Katharine%20Kemp%20%2826%20April%202020%29.pdf

[42] See Page 6, Kemp, Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper

[43] See Page 7, Kemp, Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper

[44] Arwa Mahdawi, Targeted ads are one of the world's most destructive trends. Here's why, The Guardian, y

Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

Yes – regular reminders should provide the opportunity to consumers to engage with the services and prompt people to consider their consents.

39. Should entities be required to expressly provide individuals with the option of withdrawing consent?

Yes. The ACCC has pointed out that consumer cannot currently withdraw their consent for personal information to be collected and held by an APP entity.[45]

Withdrawing consent should be as easy as providing consent in the first place and be made available at any time. As with the CDR rules consumer should be provided with

- a statement that, at any time, the consent can be withdrawn;
- instructions for how the consent can be withdrawn;
- a statement indicating the consequences (if any) to the CDR consumer if they withdraw the consent;
- a receipt or record of that withdrawal.

Consumers will have the reasonable expectation that once a consumer withdraws consent or their consent is expired, that their information will be deleted or destroyed in order to protect their privacy: see Right to erasure.

40. Should there be some acts or practices that are prohibited regardless of consent?

Yes. While consumers have received some benefits from digital services including:

- online search
- social networks
- fast and convenient connections with relevant products, news and entertainment,
- real-time information on healthier lifestyle choices[46]

there are significant detriments that have arisen from concealed data practices. These include:

- risks of hacking, accidental disclosure and illegal use of personal information
- disclosure of personal information that consumers do not wish to disclose

[45] Page 471 ACCC DPI

[46] Concealed Data Practices And Competition Law: Why Privacy Matters Katharine Kemp [2019] UNSWLRS 53 https://ssrn.com/abstract=3432769

- discrimination, manipulation and exclusion
- inappropriate price optimization and other unfair and disadvantageous economic practices and
- increase ability to exploit vulnerable cohorts.

Serious consideration needs to be given to prohibiting certain acts by businesses in collecting, handling, using personal data. Possibilities include the prohibition of:

- the processing of data about minors (as occurs under the GPDR and in Canada);
- the collection of genetic test results as a requirement for providing goods and services or entering into a contract including life insurance;
- automated decision-making about individuals such as that found under the GPDR where individuals have the right not to be subject to a decision based solely on automated processing, including profiling.
- the use methods of tracking that individuals cannot control, for example, device fingerprinting
- the offering of incentives to consent to the commercial exploitation of personal data - in anonymized, pseudonomised, identified or de-identified form - unrelated to the primary use such as the offering of vouchers, goods and/or cash (such as that proposed in California with the Own Your Own Data Act). This is because it fundamentally undermines the concept of meaningful consent and incentivizes "people to give up their fundamental right to privacy and exacerbate inequality by specifically encouraging vulnerable lower-income people to pour more personal information into an industry that exploits and discriminates against them."[47]
- screen-scraping practices;[48]
- concealed data practices;[49]
- the secondary use of data for targeted/personalised marketing and the sale of personal data in any form for the same purpose (See Question 37);
- online tracking for targeted/personalised marketing purposes;
- the for-profit trade in personal data through data brokers: some property rights are restricted by law because society has recognised the potential of exploitation such as the trade in organs. Consumer harms and exploitation borne of trade in personal data on

[47] ACLU quoted in Selling Your Private Information Is a Terrible Idea https://www.nytimes.com/2019/07/05/opinion/health-data-property-privacy.html

[48] For a full description of the problems with screen-scraping see Pages 10-18, Financial Rights Legal Centre and the Consumer Action Law Centre submission to the Senate Select Committee on Financial Technology and Regulatory Technology https://financialrights.org.au/wp-content/uploads/2020/02/191223_FinTechInquiry_Sub_FINAL-1.pdf

[49] as outlined in Page 2, Kemp, Nicholls https://www.accc.gov.au/system/files/Katharine%20Kemp%20%26%20Rob%20Nicholls%20%28March%202019%29.pdf

an individual and societal level potentially outweigh the benefits of such a trade. There is also the risk of undermining competition and entrenching market power. The establishment of a data broking sector is creating a market with entrenched players that have control of outcomes because they have means of access to data which others can't access;

- inappropriate data practices to purposes that a reasonable person would consider appropriate in the circumstances such as that occurs in Canada under the Personal Information Protection and Electronic Documents Act (**PIPEDA**) subsection 5(3)[50] including
    - Collection, use or disclosure that is otherwise unlawful
    - Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law;
    - Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual;
    - Publishing personal information with the intended purpose of charging individuals for its removal;
    - Requiring passwords to social media accounts for the purpose of employee screening
    - Surveillance by an organisation through audio or video functionality of the individual's own device;
- unfair trade practices such as dark patterns (see Question 67);
- the collection of location data unconnected to the fulfillment of a service.

Emergency declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?

No comment

[50] Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/

Regulating use and disclosure

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

Yes. For a complete list of reforms see Question 40.

Any uses or disclosures that are not in accordance with the consumer's own interests should be subject to restriction or outright prohibition.

A fiduciary duty should be placed on those collecting data (see Question 27)

We support consideration of the "no go zone" model in Canada to restrict certain uses and disclosures as listed in answer to Question 40.

Control and security of personal information

Security and retention

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

Stronger requirements are required to be imposed on businesses to maintain adequate information security management systems in accordance with accepted international standards.

Currently APP 11 leaves it to industry to "take steps as are reasonable in the circumstances" to protect personal information from misuse, interference, loss unauthorised access, modification or disclosure. This is the wrong way of approaching the matter.

APP entities handling personal information should be required to maintain adequate information security management systems in accordance with accepted international standards. Higher security requirements should be required for specific classes of information.

There are currently no specific requirements under APP 11 as to how specific types or class of information should be protected.

This is important given the recent proposal by the ACCC to expand the CDR rules to allow non-accredited parties to obtain highly sensitive CDR data via the Open Banking regime. This is a problem since the data held by accredited parties must be protected under higher levels of security than currently exists for APP entitities and non-APP entitities. It creates two standards of security and consumer protections for CDR data.

At a minimum, all business (APP entities or otherwise) should meet higher security standards as required under the CDR for obtaining and holding CDR data. Otherwise the CDR merely facilitates the movement of highly sensitive financial data from a secure and environment to one that is likely to lead to breaches as currently take place. There is already a steady stream of high

profile data breaches from those in the financial services sector including RI Advice Group[51] Visa Europe Ltd and isignthis[52], PayID, [53] to Equifax,[54] MYOB,[55] NAB,[56] the list goes on and on and on.[57]

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

Yes. Holding on to data that is no longer needed increases the "attack surface" of the consumer's personal information – that is

> *The more personal information is collected and stored, the more broadly it is disclosed, and the longer it is stored, the more likely it will be hacked, accidentally disclosed or used for illegal purposes. … These risks are greatly increased by the fact that this personal information may later be controlled by a subsequent purchaser of the supplier's business, or data brokers, aggregators or associates, who are not contractually obliged to protect the consumer's information. The extent of data collected, the duration of its storage and the extent of its disclosure are all factors which, in themselves, increase the vulnerability of the data.[58]*

We note that the DPI did not recommend the introduction of a mandatory deletion obligation once the data is no longer necessary since it could create a significant regulatory burden. We disagree. Given technological developments, the automatic deletion of personal information once unnecessary is not a complicated or onerous process. The obligation of businesses to respect consumer's right to privacy should not cease once they have provided the good and/or service. If collecting and using personal information is required to obtain the good or service there should be an obligation to deal with the data in an appropriate manner that protects consumer' right to privacy. An automatic mandatory deletion obligation should be built into the business model – no matter how small.

---

[51] IT News ASIC sues financial services company for repeated hacks, August 2020 https://www.itnews.com.au/news/asic-sues-financial-services-company-for-repeated-hacks-552124

[52] iSignthis Ltd (ASX:ISX) Visa Europe Ltd -Breach of Personal Data, Yahoofinance, 17 August 2020, https://au.finance.yahoo.com/news/isignthis-ltd-asx-isx-visa-202100430.html

[53] PayID breach sees customers' banking information hacked, https://www.news.com.au/finance/business/banking/westpacs-payid-breach-sees-customers-banking-information-hacked/news-story/08c3fb5bad5ee01463233ed669b33013

[54] Equifax hit with major pay out for data breach settlement, Techradar, 23 July 2019,Prohttps://www.techradar.com/au/news/equifax-to-pay-dollar700m-in-data-breach-settlement

[55] Australian workers' salaries exposed after MYOB glitch, Yahoo!finance, 8 July 2019 https://au.finance.yahoo.com/news/peoples-salaries-exposed-after-myob-glitch-005414328.html

[56] NAB reveals 13,000-person data breach at 6PM Friday, itnews 26 July 2019 https://www.itnews.com.au/news/nab-data-breach-hits-13000-customers-528757

[57] For a large list of data breaches in Australia see: https://www.webberinsurance.com.au/data-breaches-list

[58] Page 19 Concealed Data Practices And Competition Law: Why Privacy Matters Katharine Kemp [2019] UNSWLRS 53 https://ssrn.com/abstract=3432769

Consumers have the reasonable expectation that once a consumer withdraws consent or their consent is expired, that their information will be deleted or destroyed in order to protect their privacy.

Consumers do not want the situation where their data has been used by a company – with or without consent – and that company holds on to that data to use for secondary purposes, either in aggregated or de-identified form where there is any possibility of re-identification.

This expectation is also increasing as consumers become more and more aware of and literate regarding the extent their own personal data is being used and misused by companies, as outlined in the Preliminary Report.

Consumers will remain highly cynical of any regime that allows APP entities to hold on to their data after they leave a service.

Automatic deletion after a set period of time should be introduced in line with standards set by GDPR Article 17(1)(b) where the:

> *the relevant storage period has expired and the data holder doesn't need to legally keep it (such as banking records for a seven year time period).*

An automatic deletion requirement will also help overcome the behavioural biases that prevent people from taking the necessary and sometimes cumbersome steps to delete.

We note that the ACCC has recommended this obligation be set out in the Digital Platforms Privacy Code of Practice. This however will only apply to those entities covered by or signatories to a DP Privacy Code. Similar automated deletion and retention periods will need to be applied to every other sector across the economy. This could be done so in piecemeal by the Consumer Data Right. However we believe that it is more appropriate to apply this right to all holders of data as a part of the Australian Privacy Principles and the *Privacy Act*.

Access, quality and correction

45. Should amendments be made to the Act to enhance:

a. transparency to individuals about what personal information is being collected and used by entities?

The right to access one's personal information needs to be expanded beyond mere provision of the information. It needs to align itself with the EU Article 15 Right of Access to include the right not just to access the personal data but to also access the following information:

- the purposes of the processing (Art15.1(a));
- the categories of personal data concerned (Art15.1(b));
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations (Art15.1(c));
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period (Art15.1(d));

- the existence of the right to request a correction or erasure of personal data or restriction of processing of personal data or to object to such processing (Art15.1(e));
- the right to lodge a complaint with EDR or a regulator (Art15.1(f));
- where the personal data are not collected from the data subject, any available information as to their source (Art15.1(g));
- the existence of automated decision-making, including profiling and, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Art15.1(h));

APP 12 needs to be updated in a number of further ways:

- the time frame for accessing to personal information – ie reasonable period after the request is made – is far too subjective and a short hard time frame needs to be introduced. Given technological advances timeframes should be reducing to zero/instantaneity.
- charging for accessing one's own personal information should be removed. Currently APP 12 states that an organisation may charge an individual but that it must not be excessive and must not apply to the making of the request.

  Charging a fee to access your own personal information is a significant barrier to access. Telstra, in one case run by Consumer Action, requested a $70 per hour fee to access documents containing the client's personal information. When challenged, Telstra withdrew this request. Whether a fee is excessive or otherwise is in the eye of the beholder and for particularly vulnerable consumers experiencing significant financial hardship, any fee, no matter how small it seems to others, will be too much and act as a barrier to such access. APP12 in its current form is therefore embedding a class system for accessing private information. Even if a waiver were to be made available, this would be an additional hurdle to a cohort of consumers who, going on past experience, will simply not take the steps required.

  APP 12 must be amended to ensure that the process for gaining access to your own personal information should be free, easy and straightforward. It is a difficult task for an individual to request access to personal information as it is varied, generally hidden in terms and conditions or buried in the fine print somewhere on a website. Minimum standards need to be set.
- consumers should be able to access personal information – including inferred information held by them. This means removing the exception APP 12.3(j) re: "giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process." Consumers should have a right to access this information that is being used for commercial gain.

b. the ability for personal information to be kept up to date or corrected?

Consumer representatives can attest to a general ongoing failure to amend or correct personal information in a speedy or good faith manner. Seeking amendments to credit reports, as an example, is frustrating and difficult. And seeking corrections is important as inaccurate information can lead to say, losses and notices being sent to incorrect addresses and the consequent losses that arise from that.

Currently APP 13 states that organisation must "must take such steps (if any) as are reasonable in the circumstances." The EU GPDR Art 16 Right to Rectification states that rectification should take place "without undue delay." It is critical that APP 13 be amended to ensure that a data holder must take *immediate* steps to correct information once it becomes aware (by learning itself or being told by the consumer) that personal information they hold is inaccurate, out of date incomplete, irrelevant or misleading. If they do not they should be held liable for any reliance on this information that leads to a loss.

Right to erasure

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

Yes. The EU's GPDR Art 17 should act as a model for the right to erasure in Australia. GDPR Article 17 provides for the "Right to Erasure" where an individual will hold the right to request the erasure, *without undue delay*, of any links to, copy or replication of the data in question, under the circumstances where:

- the data is no longer necessary in relation to the purposes for which it was collected: Article 17(1)(a)
- the individual withdraws consent or the relevant storage period has expired and the data holder doesn't need to legally keep it (such as banking records for a seven time period): Article 17(1)(b)
- the individual objects to the processing of data – including direct marketing purposes and profiling: Article 17(1)(c) & Article 21
- the data was unlawfully processed: Article 17(1)(d)
- there is a legal requirement for the data to be erased: Article 17(1)(e)
- the consumer is a child at the time of collection: Article 17(1)(e) & Article 8

There are exceptions to this right, which include:

- exercising the right of freedom of expression and information: Article 17(3)(a)
- for compliance with a legal obligation, e.g. again as mentioned above a bank keeping data for seven years: Article 17(3)(b)
- for reasons of public interest in the area of public health: Article 17(3)(c)

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes: Article 17(3)(d)
- for the establishment, exercise or defence of legal claims: Article 17(3)(e)

It is important that the right to erasure should not be limited to those cases where personal information is provided by a consumer with 'consent' but should capture those circumstances where data was collected without their consent. This would ensure that the right captures a de-linking right.

47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

The exceptions under the GPDR are appropriate. It is important that these reasons align with public interest reasons not commercial or other self-interested business reasons. We think the proposed exception is broad enough to ensure that genuine and legitimate interests in retention are captured – in line with the GPDR

We disagree with the small business exemption (see above). We therefore disagree with the ACCC's view that the right to erasure should not apply to small businesses exempted under the current APP entity definition.

Overseas data flows and third party certification

48. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?

a. Are APP 8 and section 16C still appropriately framed?

49. What (if any) are the challenges of implementing the CBPR system in Australia?

50. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?

51. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

Meaningful consent must be sought and received before sending a consumer's data overseas. The obligation under APP 8 to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the data should be bolstered to make it so that the entity must ensure that this is the case and be held liable for any breaches.

Article 45 of the GPDR states:

> *A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified*

sectors within that third country, or the international organisation in question ensures an adequate level of protection.

Shifting the responsibility of ensuring adequate protections are in place from the entity to Government is an efficient process that will produce stronger consumer outcomes and not leave consumers liable to the inconsistent approaches taking by entities. The same approach needs to take place in Australia.

Sending data overseas is the biggest and most obvious chink in the safety and security regime in handling personal data. Firstly the data can become subject to the laws of the overseas jurisdiction, such as the United States, and be accessed under their laws. Secondly, if any breaches were to occur in an overseas jurisdiction it is always more difficult to access justice for somebody in Australia, particularly if that data is being on-sold to a fourth party based solely in another jurisdiction.

The refusal of consent should not be used to punish or penalize a customer, nor should it be used to refuse service to a customer. It should not be presented in such a way also that skews the consumer in favour of consenting.

Enforcement powers under the Privacy Act and role of the OAIC

52. Is the current enforcement framework for interferences with privacy working effectively?

53. Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?

54. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?

a. If so, what should these enforcement mechanisms look like?

Consumer representatives have had significant issues in the past with the OAIC's application of the privacy laws, which in our experience have erred against the consumer interest.

Financial Rights, for example, has had extensive experience in dealing with the OAIC's complaints process in a number of representative complaints. In general, the complaint handling process that we have experienced has been lengthy, haphazard and opaque. The following are some of the procedural deficiencies that we have experienced:

- *Lack of procedural clarity:* We have not been given an overall explanation of how complaints would proceed from the outset, nor have we been told what the steps toward a determination would be, or the estimated timeframes for the various stages of a complaint.

- *Non-transparency:* In one complaint, we were made aware of discussions that the Privacy Commissioner had with opposing parties regarding one of our complaints, including regulatory guidance that the Commissioner gave to representatives of the opposing party on issues of the complaint to which we were never made privy. We asked for transcripts of relevant meetings or at least a written summary of the issues discussed but we were never given anything.
- *Confidentiality:* Financial Rights has found that it has been unclear what parts of the complaints process were confidential and what parts were not confidential. A statement needs to be sent at the start of a complaint process by the OAIC to both parties to clarify this matter. The complaint process should be transparent.
- *Lack of timeliness:* Financial Rights has experienced significant delays between communications with the OAIC, had meetings cancelled with limited notice, and multiple deadlines given to opposing parties to respond to our complaints were ignored and unenforced. The opposing party in a series of complaints did not formally respond to any of them until eight months after Financial Rights lodged them with the OAIC. We have experienced delays of up to two years. We note that the Australian Privacy Foundation refers to a "six month delay before it even starts to investigate a complaint."[59]
- *Unreasonable conciliation:* We were also made to attend two separate conciliation meetings even though we made it clear in writing and verbally that we did not believe our complaints could be resolved in that manner, and we were unable to compromise on behalf of all the consumers that we represented in the proceedings.

Privacy law as overseen by the OAIC should be proactive and protective, setting standards that serve to prevent harm. Consumers shouldn't need to rely on the Australian Consumer Law 'after the fact' to address harm already occurred – as occurred in the complaint outlined in the example presented at Question 37.

If the *Privacy Act* is strengthened and re-balanced in favour of the consumer and the right to privacy, and the OAIC is resourced and empowered to better serve the consumer interest in supporting that right, there is likely to be improved enforcement outcomes.

[59] Australian Privacy Foundation, Submission to the ACCC Digital Platforms Inquiry, February 2019 https://www.accc.gov.au/system/files/Australian%20Privacy%20Foundation%20%28February%202019%29.PDF

Direct right of action

55. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

We have had the opportunity to read the Public Interest Advocacy Centre' submission to this review and wish to endorse their views with respect to a direct right of action. In particular we support:

- the direct right of action being clear and simple – for the public to understand, for individuals to exercise, for entities to respond, and for courts to determine jurisdiction
- individuals ought to have a choice as to whether they apply directly to the courts, or to seek conciliation through the OAIC;
- allow the Commissioner to be heard in proceedings as amicus curiae

Further we do not support:

- a limitation of the right to 'serious breaches' of the Act, or
- making it a condition to go through a conciliation process before applying to the courts
- introducing a cap on the damages that may be awarded

We support individuals being given a direct right to bring actions and class actions against APP entities in court to seek compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for the financial and non-financial harm suffered as a result of an interference with their privacy under the Act.

Relying on the OAIC to solely enforce *Privacy Act*, given its limited resources and approach as described above means that the current constrained process to enforce rights is inadequate to protect consumers.

The AFCA model involving a combination of much of the above including to ensure access to justice is may also be helpful in guiding the development of the right model.

Some principles should be established to guide the development of the appropriate model:

- consumers should have access to a conciliatory approach before a tribunal or court;
- choosing a conciliatory approach should not prevent the consumer from taking their complaint to a tribunal or court;
- access to free and independent advice and representation is essential to an effective dispute resolution framework, particularly for consumers experiencing vulnerability and disadvantage.

Statutory tort

56. Is a statutory tort for invasion of privacy needed?

57. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

58. What types of invasions of privacy should be covered by a statutory tort?

59. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

60. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

61. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

As above, we have had the opportunity to read the Public Interest Advocacy Centre' submission to this review and wish to endorse their views with respect to a statutory tor. In particular we agree that:

- a cause of action for breach of privacy should not be left to incremental development of common law through the courts;
- there be two forms of invasion of privacy which form the first element of the tort, that is:
    - there has been an intrusion of their seclusion or private affairs;
    - there has been a misuse or disclosure of information about their information;
- the tort should be actionable where a person in the position would have a 'reasonable expectation' of privacy in the circumstances, measured by an objective standard;
- the tort should not be confined to intentional or reckless invasions of privacy, but should extend to negligent invasions of privacy;
- legal action should be actionable *per se* without the need to prove that any actual loss or damage;
- defences should be limited to:
    - conduct was authorised or required by law;
    - conduct was incidental to the lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm;

- meaningful consent specific to the conduct alleged to have breached the person's privacy;
- conduct was in the public interest, where public interest is a limited concept and not any matter that the public may be interested in; and
- a range of remedies should be made available to the court to order where a person has been aggrieved by an invasion of their privacy.

A statutory tort for serious invasions of privacy should be introduced. This recommendation has been around since the ALRC examination of the issue and its implementation is long overdue to bring Australia into line with other jurisdictions.

This will be a positive step in the financial services sector as it increasingly moves into business models that are based on the use of new data collection technologies and data analytics in FinTech[60] and InsurTech[61]. FinTech products and services' utility arises from a near total reliance on data – largely a consumer's personal financial data - their transactions history, credit history, etc. FinTechs are also integrating financial data with other data about individuals drawn from social media and other sources – information that people would consider have nothing to do with their financial status. InsurTech is also tracking people's every movement and drawing conclusions about a person's identity and their life derived from the use of their car.

This increased collection of data is feeding the creation of a "financial identity" – a concept increasingly used by financial institutions to get to know their customer more.

Financial institutions have for years stored and verified customer identities and attributes through "Know Your Customer" systems i.e. the process by which banks or other financial institutions identify their customers in order to evaluate the possible legal and other risks. They therefore have a commercial incentive to collect more and more accurate information about their individual customers. However the development of an increasingly accurate financial identity built by data has serious consequences and harms for consumers. A person's financial circumstance is highly sensitive since its use by financial institutions, or in other cases a breach causing a leak of this private information, opens them up to a range of significant problems.

A statutory tort will motivate current and emerging business models to not engage in harmful data collection and use practices and pay more regard to the consequences of the use and any potential breach of personal information.

---

[60] E.g. mobile and online banking; Open Banking; new personal financial management services; investment and wealth management services with automated or robo-advisers services; new lending and unsecured credit services based on data led credit-scoring and risk profiling; new payment services; encrypted digital wallets that stored bank, debit or credit card detailing for online payments; neo banks and FinTech savings banks; offline mobile payments; and credit scoring and social scoring

[61] Where connected devices and telematics technology (e.g. Fitbit), connected home technologies (e.g. Amazon Alexa) and what is known as the "Internet of Things" (e.g. connected smoke alarms, locks, fridges and light switches) are being put to specific use by the insurance sector. Insurers are using genetic testing technology in their underwriting provided to them under disclosure laws, an ability borne of increased computing processing power, new hardware and data analytics.

Non-digital serious invasions of privacy

However it should also be noted that the introduction of a statutory tort for serious invasions of privacy should be designed and implemented not solely with digital platforms in mind. There are current non-digital practices by financial services companies that would and should be captured by a statutory tort for serious invasions of privacy.

In insurance claims handling, assessment and investigation practices have a significant impact upon consumers – issues with investigation tactics and surveillance are one of the key issues complained about to the Insurance Law Service.

Without a statutory action for invasion of privacy any person can without your consent take photographs, still pictures and videography of you in a public place. In addition, any information that is publically available can be sourced. Insurers also will sometimes allow themselves the right to undertake surveillance of their insured's in the contract of insurance. This contractual right does not extend to non-parties to the insurance. But, as stated, there is no restriction on the practice of still photography, and filming or monitoring of third parties in public places, places of work and businesses.

Surveillance device laws theoretically provide a level of protection against the unwarranted, intrusive or inappropriate surveillance of Australians, including insurance claimants. While laws are in place in each state and territory to regulate the use of surveillance devices, their complexity, inconsistency and failure to keep up with technological progress provide irregular protection and little comfort to parties subject to intrusive and unwarranted surveillance. See further information in the Financial Rights' Report *Guilty Until Proven Innocent: Insurance Investigations* in Australia.[62] In the end though while much of the surveillance undertaken by life insurance investigators is legal, the conduct of the surveillance does veer into ethically murky territory.

We note that the ALRC considered the need for a specific defence to protect investigations into potential fraud or misrepresentation. It stated that:

> *It is in the interests of all policy holders that insurers have safeguards against fraudulent claims. Where they have reasonable grounds for suspecting fraudulent conduct, they or others on their behalf may often carry out investigations that could be viewed as invasions of privacy. The defence that the conduct was required or authorised by law is wide enough to cover these circumstances. … The ALRC considers that individuals or organisations that engage in such conduct may be protected from liability under the public interest balancing test.*

We supports the reasons here but believe that insurers have not acted in ways that either demonstrated reasonable grounds for suspecting fraudulent conductor acted in ways that met expectations of privacy.

ASIC's recent report into car insurance investigations found that:

> *Fraud is a real and serious issue and insurers need to investigate, identify and deny fraudulent claims. But our data shows that of all the claims that insurers decided to investigate, only 4%*

[62] https://financialrights.org.au/wp-content/uploads/2016/03/Guilty-until-proven-innocent.pdf

were declined for fraud, and only 10% were declined for some other reason. Over 70% of the claims that insurers investigated were paid.

This clearly demonstrates that while there is a public interest in preventing fraud the grounds upon which insurers are undertaking investigations (that can involve serious invasions of privacy) are not as robust or as reasonable as they claim.

> *Consumers expect a fair process to be followed when a claim is investigated. Consumers in our research whose claims were investigated and eventually paid felt angry, frustrated, confused, overwhelmed and helpless during investigations*

In developing the statutory tort, it is critical that it is designed in a way to ensure that defences are not used as carte blanche get-out-of-gaol-card-free cards to act in unreasonable ways that invade people's privacy.

Notifiable Data Breaches scheme – impact and effectiveness

62. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?

63. Has the NDB Scheme raised awareness about the importance of effective data security?

64. Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

We note the recommendations made by the Consumer Policy Research Cetnre regarding Notifiable Breaches a support:

- Reducing the 30 day timeline for reporting a breach to the OAIC to 3 days as set by the EU's GPDR;
- Require reporting of all breaches – serious and less serious – that indicate systemic data-handling and securities issues within an entity.

Interaction between the Act and other regulatory schemes

65. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

66. Is there a need for greater harmonisation of privacy protections under Commonwealth law?

a. If so, is this need specific to certain types of personal information?

67. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?

The multiplicity of legislative, regulatory and self-regulatory regimes related in part of in whole to privacy has led to a complex web of consumer protections with varying standards, rights and safeguards. This includes everything from the Consumer Data Right, Artificial Intelligence Ethics Framework, Data Availability and Transparency laws to the Digital Economy Strategy, eSafety Strategy, telecommunications laws, and an endless array of other laws that impact upon Australians' right to privacy.

Consideration needs to be given to how the *Privacy Act* can drive a holistic, harmonised, principled, regulatory framework to protect our right to privacy. We touch on the following key areas where the interaction needs to be dealt with urgently to ensure improved consumer outcomes.

Privacy Act and the CDR

The introduction of the Consumer Data Right (**CDR**) regime has created multiple levels of privacy standards for different people that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

- CDR Privacy Safeguards– essentially strengthened versions of the Australian Privacy Principles (**APPs**);
- the *Privacy Act* safeguards as detailed under the APPs; and
- general consumer protections and law applying to those holders of consumer data that are *not* "APP entities" as defined under the APPs, i.e. all private sector and not-for-profit organisations with an annual turnover of less than $3 million.

If non-accredited parties are ultimately able to access CDR data, this will lead to the following two situations that provide lower standards of consumer protection:

1. CDR data accessed and held by non-accredited parties who are "APP entities"[63] will be subject to the APPs, not the CDR privacy safeguards.
2. CDR data accessed and held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

It is therefore critical that this review examine the fracturing of the privacy regime and look at ways protect the right to privacy across the economy with a principles-based governance framework.

Greater harmonisation between the *Privacy Act* and the *Consumer Data Right* is required. The development of strengthened consumer protections under the CDR should be instructive for the development of a stronger Privacy regime more generally.

If the CDR regime is not a closed scheme – stronger privacy protections and standards are required in the handling of consumer data in the broader economy.[64]

Privacy Act and unfair contract terms

The *Competition and Consumer Act 2010* needs to be amended to ensure that unfair contract terms (**UCT**) are prohibited and not just voidable, with civil penalties applying. We note that the recent communique from the Meeting of Ministers for Consumer Affairs where Ministers have agreed to strengthening and enhance the UCT regime.[65] Currently without civil penalties financial firms are able to include unfair terms that serve their interests, with individual consumers and their representatives forced to identifying these terms and argued for them to be declared void. This is incredibly difficult in an environment with long, overly complex terms and conditions. This also has very little impact on a firm where there is no money exchanged in the digital economy.

Privacy Act and unfair trading practices

We note that work is underway through Consumer Affairs Australia and New Zealand on exploring how an unfair trading prohibition could be adopted in Australia to address potentially unfair business practices. This work needs to be prioritised to capture an increasing number of unfair practices relating to the collection, use, handling and disclosure of data.

---

[63] Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses

[64] For further outlining of our concerns with respect to the provision of CDR data to non-accredited parties see Financial Rights' Submission to ACCC re: CDR rules expansion amendments, Consultation Paper. https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf

[65] Meeting of Ministers for Consumer Affairs, Friday 6 November 2020 https://consumerlaw.gov.au/index.php/consumer-affairs-forum/communiques/meeting-12-0 and Treasury, Enhancements to Unfair Contract Term Protections - Regulation Impact Statement for Decision, 9 November 2020, https://treasury.gov.au/publication/p2020-125938

We therefore support the ACCC's recommendation[66] to prohibit unfair trade practices through a simple, principles-based, outcomes-focused new provision in the Australian Consumer Law prohibiting unfair trade practices, including practices that are likely to have an unfair outcome.

The scope of the provision should not be limited, but regulatory guidance can be provided to help businesses understand what is meant by unfair conduct or practices, including in the areas of:

- Marketing and sales, particularly addressing harm associated with consumer manipulation;
- Product or service design and pricing, drawing on the concepts of a legitimate business purpose and fitness for purpose;
- The use of dark patterns - tricks used in apps that force consumers to unwittingly buy, sign up or consent to things that they didn't mean to and
- Customer service and complaints processes, ensuring service is responsive to customer vulnerability.[67]

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Drew MacRae, Financial Rights' Policy and Advocacy Officer at drew.macrae@financialrights.org.au or on (02) 8204 1386.

[66] Recommendation 21, ACCC Digital Platforms Inquiry Report.

[67] For a full description of the problems that an unfair trading practice prohibition will address see Pages 29-32, Financial Rights Legal Centre and the Consumer Action Law Centre submission to the Senate Select Committee on Financial Technology and Regulatory Technology https://financialrights.org.au/wp-content/uploads/2020/02/191223_FinTechInquiry_Sub_FINAL-1.pdf