Financial Rights
LEGAL CENTRE

**Submission by the**

**Financial Rights Legal Centre**

# Australian Competition and Consumer Commission

# Digital Platforms Inquiry, December 2018

February 2019

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. Financial Rights took close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to
www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

## Introduction

Thank you for the opportunity to comment on the Australian Competition and Consumer Commission's (**ACCC's**) Digital Platforms Inquiry Preliminary Report (**Preliminary Report**).

The Financial Rights Legal Centre's (**Financial Rights'**) interest in the Digital Platform Inquiry is centred on the need for a strengthened privacy regime arising out of the data use and collection practices as identified in the Preliminary report. This is an important finding that has broader implications for the digital economy and, more specifically, the implementation of the Consumer Data Right (**CDR**) and its first application in open banking.

Financial Rights has raised significant concerns with the development of the CDR and its impact upon the safety and privacy of financial services consumers. We have been vocal advocates for the need to review the *Privacy Act* and the Australian Privacy Principles in order to mitigate a number of the risks identified in the design of the CDR regime.

Our concerns have been submitted in detail to both Treasury – who have worked on the establishing legislation for the CDR – and to the ACCC, in its role of establishing the CDR Rules.[1] Many of the specific concerns have been at least temporarily ameliorated under the first iteration of the ACCC rules – including the removal of minors from the CDR regime, ensuring that non-accredited parties are not able to access CDR data and neither direct marketing nor on-selling of data is possible.

Financial Rights however remains concerned that these consumer-friendly CDR Rules are simply the first iteration and able to, and likely will be, amended in the future to better serve business interests under the guise of innovation – innovation that has seen the development of the types of exploitative data collection models described in this Preliminary Report in other sectors. Under the current design of the CDR, there remains no guarantee that strong consumer protections regarding privacy will continue to be protected moving into the future. What is required is a wholesale review of the *Privacy Act* and Australian Privacy Principles to embed strong protections across the board and better prepare the nation for the move to a data-based economy.

---

[1] Submission to the Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation https://financialrights.org.au/wp-content/uploads/2018/10/181012_CDR-Second-Round_submission_FINAL.pdf; Consumer Data Right (CDR) Rules Framework, Sept. 2018 https://financialrights.org.au/wp-content/uploads/2018/10/181003_ACCC_CDRRULES_Submission_FINAL.pdf; Submission to the Treasury Laws Amendment (Consumer Data Right) Bill 2018; https://financialrights.org.au/wp-content/uploads/2018/09/180907_CDRLegislation_Submission_FINAL.pdf; Joint consumer submission on the Open Banking: customers, choice, convenience, confidence Final Report; https://financialrights.org.au/wp-content/uploads/2018/03/180323_OpenBanking_FinalReport_Sub_FINAL.pdf; Joint consumer supplementary submission to Treasury's Open Banking Review – Issues Paper https://financialrights.org.au/wp-content/uploads/2017/10/171025-Open-Banking-Supplementary-Submission-FINAL.pdf Submission to Treasury on Open Banking, https://financialrights.org.au/wp-content/uploads/2017/09/170922-FINAL-submission-open-banking-issues-paper.pdf

We note that many of the proposals arising out of the ACCC's consideration of consumers of digital platforms, data collection and privacy, significantly align with the consumer movement's view that the privacy laws require significant strengthening. We wish to support these recommendations and provide specific comment in the context of the establishment of the CDR.

This submission will firstly provide details as to why the Digital Platforms Inquiry must consider the development and implementation of the CDR in finalising its report and recommendations.

The submission recommends the ACCC reconsider its decision not to recommend a comprehensive review and overhaul of the *Privacy Act* and Australian Privacy Principles.

The submission will then provide comments on the specific recommendations made under Chapter 5 with respect to Digital Platforms and Consumers.

## Digital Platforms, the Consumer Data Right and Open Banking

We note that there is no reference to the CDR in the Preliminary Report. It is critical that the ACCC takes into account the legislative changes currently occurring under the CDR and integrate these developments into the recommendations arising out of the Digital Platforms Inquiry.

We acknowledge the Digital Platforms Inquiry and the CDR are dealing with two different areas. The Digital Platforms Inquiry is examining digital search engines, social media platforms and digital content aggregators. The CDR is being established to allow consumers to ask for data to be safely shared with trusted recipients in specific sectors such as banking, energy and telecommunication services, and eventually for other services across the economy.[2] Despite this there is significant crossover in their impact upon consumers, their data and privacy (and other consumer) protections.

Firstly, the somewhat dubious data collection and use practices of the key digital platforms described in the Preliminary Report are not solely confined to digital search engines, social media platforms and digital content aggregators. These data collection and use practices are undertaken by major financial services companies in the financial services sector, FinTech sectors and other sectors. These sectors are also the direct beneficiary of many of these practices as both advertiser and recipient of data gathered by digital platforms.

Secondly, the Preliminary Report identifies major flaws in the regulatory framework over the collection, use and disclosure of user data and personal information. Many of these flaws have similar been identified by the Open Banking Report[3] and sought to be addressed under the CDR but not the wider economy.

Third, the Preliminary Report makes a number of recommendations in ensuring that consumers are better protected. Most of these recommendations align with consumer recommendations with respect to data collection and use practices in the financial services and FinTech sectors that will be subject to the CDR and Open Banking.

Strengthening the *Australian Privacy Law* and Australian Privacy Principle in its application to all consumers across the economy will assist in solving many of the problems Financial Rights has identified with the CDR legislation and design. More specifically, many of the Preliminary recommendations have the potential to provide strengthened privacy protections to consumers whose CDR data leave the accredited CDR regime and falls into the hands of non-accredited parties. While non-accredited parties currently will not have access to CDR data under the ACCC CDR Rules, it is highly likely that they will at some point available to non-accredited parties, be it through future iterations of the ACCC CDR Rules, some form of

[2] https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-handout.pdf

[3] https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

regulatory arbitrage or it may simply be accessed by non-accredited parties through other means such as screen-scraping.

Bolstering general privacy protections applying to all Australians to levels that match or even exceed the privacy protections under the CDR in its application to accredited CDR participants has the potential to address many of the concerns consumer representatives have with the leaking of such data outside of the CDR system.

Furthermore, consumer data held by financial institutions which has the potential to become CDR data, should in our view be subject to strengthened privacy protections and data collection and use rules, similar to those being recommended under the Preliminary Report.

It is therefore critical that if it has not yet done so, the ACCC's Digital Platforms Inquiry engage directly with the ACCC CDR team to discuss the implications of each other's work and integrate their respective recommendations.

We note that the ACCC's preliminary recommendation is not to review or amend the *Privacy Act* to adopt identical terms to those found in the EU's General Data Protection Regulation (**GDPR**). It is, rather proposed that some of the underlying principles of several provisions of the GDPR should be incorporated into the law and make up a part of the proposed recommendations to strengthen notification requirements, introduce certification schemes, strengthen consent requirements, and enable the erasure of personal information respectively.

While we support many of the recommendations and these will go some way to dealing with many of the concerns of consumer representatives, we believe the ACCC needs to reconsider their position to recommend a comprehensive review and overhaul of the *Privacy Act* and Australian Privacy Principles given the:

- the limited scope of the current inquiry to digital search engines, social media platforms and digital content aggregators;
- the broadly applicable nature of the issues identified in data collection and use practices to other sectors;
- the major flaws identified in the current regulatory environment; and
- the limited scope to address broader data use and collection practices under the CDR and potential abuse by non-accredited parties

An economy wide review of the *Australian Privacy Act* and Australian Privacy Principles is more than justified.

The last time privacy laws in Australia were comprehensively reviewed was ten years ago when the Australian Law Reform Commission wrote its report on Australian Privacy Law and

Practice.[4] The way Australians use and supply data has changed dramatically in the last decade as is obvious from the Preliminary Report.

We are not arguing for a delay in implementing the positive recommendations put forward in in the Preliminary Report. However we do wish to ensure that Australia does not introduce much needed reform in a piecemeal manner that leads to the country falling behind fast paced developments in a modern digital economy and being implemented across the world.

[4] ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 , 12 August 2008. Available at: https://www.alrc.gov.au/publications/report-108

## Preliminary recommendation 8 - Amendments to the Privacy Act

### a. strengthen notification requirements

Financial Rights supports strengthening the notification requirements under APP 5 to notify consumers of the collection of their data. It is currently left up to the APP entity to decide whether and how to provide notification under APP 5. This is unacceptable for a data-heavy economy.

Financial Rights supports the notification being:

- concise, transparent, intelligible and easily accessible, written in clear and plain language (particularly if addressed to a child), and provided free of charge.
- consumer tested; and

We also support APP 5 explicitly specifying the information that must be set out in the notification, including:

- the identity and contact details of the entity collecting data;
- the types of data collected and 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.

We wish to note a couple of issues.

The draft CDR legislation states that a participant "must take steps" rather than "must take reasonable steps." This is a simple solution to address the core problem.

Under the ACCC CDR Rules, notification must include "the data that has been requested."[5] 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[6]
- transfer personal data to a third country or international organisation[7]

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

[6] Article 13(1)(c)

- the period for which the personal data will be stored[8]
- the existence of the right to request from the controller access to and rectification or erasure of personal data[9]
- where the processing is based[10]
- the right to lodge a complaint[11]
- whether the provision of personal data is a statutory or contractual requirement[12]
- the existence of automated decision-making, including profiling[13]

All these should be included in any notification.

Finally, Financial Rights does not support an exemption to the proposed notification requirements, 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.

**b. introduce an independent third-party certification scheme**

Financial Rights supports the principle of an independent third-party certification scheme but notes that the scheme should be explicitly empowered to monitor and examine the use of algorithms.

We note that the ACCC's recommends[14] the creation of a regulatory authority to be tasked with monitoring, investigating and reporting on the criteria, commercial arrangements or other factors used by relevant digital platforms including the effects of algorithms or other policies on the production of news and journalistic content or competition in media markets.

However, this recommendation is limited in scope to only digital platforms which generate more than AU$100 million per annum from digital advertising in Australia. We believe regulators need to be keeping track of all use and misuse of algorithms.

---

[7] Article 13(1)(f)

[8] Article 13(2)(a)

[9] Article 13(2)(b)

[10] Article 13(2)(c)

[11] Article 13(2)(d)

[12] Article 13(2)(e)

[13] Article 13(2)(f)

[14] Recommendation 4

Algorithmic bias or discrimination is already well documented[15] and arises when an algorithm is used in a piece of technology that reflects the implicit or explicit values of those who are involved in coding, collecting, selecting, or using data to establish and develop an algorithm. The Preliminary Report details a number of poor consumer outcomes arising out of the misuse or algorithms by digital platforms including online profiling and exploitation, price discrimination and competition issues arising out of businesses favouring their own business interests.

The practices described in the Preliminary Report are however more widespread.

Closed proprietary algorithms used by entities such as FinTechs and InsurTechs to, for example automatically calculate say an individual's credit worthiness or the interest rate they are offered could potentially lead to situations where consumers are denied access to crucial products and services based on accurate or inaccurate data without the ability to determine why or to correct underlying assumptions.

Credit scoring, social scoring or e-scoring algorithms in the financial services space, for example can produce feedback loops where somebody from a particular suburb where a lot of people default can be given lower credit ratings due to that association. Statistical correlations used by actuaries between a person's postcode (here geographical information standing in for a particular race, ethnicity or culture); their language patterns on social media; their potential to pay back a loan; or, keep a job; can lead to significant discrimination being built into opaque black box algorithm technology.

RegTech could provide regulators with confidential and protected access to commercially sensitive algorithms and other black box technologies to examine automated decision making programs. This way they can interrogate such technologies more closely to identify price discrimination and discriminatory practices more generally.

While this should be the remit of the ACCC, the OAIC or some other regulator such as ASIC or APRA in the financial services space, it could also fit within the scope of the third part scheme envisioned under recommendation 8(b).

**c. strengthen consent requirements**

Financial Rights supports amending the *Privacy Act* to define 'consent' to include only *express* consent and that the current non-binding elements of the OAIC's guidance regarding consent be binding requirements under the APPs, to ensure that:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

[15] See Cathy O'Neil, Weapons of Math Destruction, 2017

The EU has finalised guidelines on consent.[16] These guidelines should provide the ACCC significant guidance as to the nature of consent including examining a multitude of situations and concepts to enable genuine consent to be effective.

The *Privacy Act* was drafted during a period where the use of digital terms and conditions that are bundled and lengthy were relatively new. Their use has led to a significant asymmetry of information and power, working against the interests of consumers. They are unfair and have led to lower levels of product, service and data literacy.

The APPs (including APP3, 7 and 8) must be modernised and future-proofed with clear requirements on all companies (not just digital platforms and financial services) to gain express, fully informed consent from a consumer.

With respect to the specific elements put forward by the ACCC, Financial Rights makes the following observations and recommendations.

***Adequately informed:*** It is important to ensure that the lack of consent for a particular use should not limit the ability to receive a service unless the data is fundamentally necessary for a particular product or service to work.

***Voluntariness:*** The EU guidance acknowledges that there are a number of situations where genuine consent cannot be freely given – for example in situations where there is a significant imbalance of power. This needs to be incorporated into any notion of voluntariness. To this end consent must be freely given, absent of any element of inappropriate pressure or influence upon the consumer preventing them from exercising their free will including:

- any imbalance of power;
- the presence of any conditions via for example, the bundling of consent of necessary and unnecessary uses;
- the conflation of several purposes without consent for each specific use; and/or
- detriment to the consumer if consent is withdrawn or refused;

***Current and specific consent:*** Consent should also be able to be constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data. Entities must be obliged to only collect the minimum amount of personal information that the business actually needs. This means not collecting extra information simply for marketing purposes at some later date for example. Consent must also be time limited and should not be ongoing in perpetuity. Like the CDR rules there must a period of time where consent must be renewed.

***Understanding and communicating consent:*** APP entities must explain in simple, clear, terms *why* information is being collected and for what it is being used.

**d. enable the erasure of personal information**

Financial Rights supports the amendment of the *Privacy Act* to enable the erasure of personal information.

16

Erasure should occur without undue delay as per Article 17 of the GDPR.

We note that the ACCC supports the exception to erasure being "overriding reasons for the APP entity to retain the information." It is important that these reasons align with public interest reasons not commercial or other self-interested business reasons.

Financial Rights supports the automation of deletion after a set period of time as proposed in Box 5.24. This would meet the standard 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).*

The following elements from Article 17 should also be included to ensure erasure where:

- 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

The following exceptions are also reasonable:

- exercising the right of freedom of expression and information: Article 17(3)(a)
- for compliance with a legal obligation, e.g. 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)

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

**e. increase the penalties for breach**

Financial Rights supports increasing penalties for a breach.

**f. introduce direct rights of action for individuals**

Financial Rights supports direct rights of action for individuals

**g. expanded resources for the OAIC to support further enforcement activities**

Financial Rights supports expanded resources for the OAIC to support further enforcement activities. However we would note that Financial Rights has had significant issues in the past with the OAIC's application of the privacy laws, which in our experience have erred on the side of against the consumer interest.

As we have submitted to the Open Banking consultations and consultations on the CDR legislation we have 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.
- *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.

Given this, we would hope that any increase in resources and capacity at the OAIC to undertake enforcement activities will empower the OAIC to take more of a pro-consumer approach than what they have to date.

**Further rights**

The ACCC should consider the inclusion of a number of strengthened and new rights under the *Privacy Act*.

*Corrections to consumer data*

Firstly, the rules regarding the correction of personal information under APP13 need improvement.

Financial Rights 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, notices being sent to incorrect addresses and the consequent losses that arise from that.

It is critical that APP 13 be amended to ensure that a APP entity 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.

*Opting out of data processing*

Further consideration should be given to implementing a number of other GDPR rights including:

- The right to object to processing of personal data and
- The right to not to be subjected to automated individual decision-making, including profiling

*Standardisation of terms and definitions*

A key problem identified by the Preliminary Report is the lack of consistency with respect to terms:

> *Many digital platforms' privacy policies are long, complex, vague, and difficult to navigate. They also use different descriptions for fundamental concepts such as 'personal information', which is likely to cause significant confusion for consumers.*

This confusion must be reigned in. There are however no recommendations made to address this key issue.

Financial Rights regularly sees poor consumer outcomes arising out of the use of confusing, vague, incomparable and inconsistent terminology in financial services – in particular insurance disclosure. Just as the multitude of terms, phrases and interpretations in insurance fail to serve the interests of consumers and actively work against their interest, the same can be said of privacy terms and conditions.

Following a recommendation by the Senate Economics References Committee Treasury is currently developing and implementing standardised definitions of key terms for general

insurance.[17] The ACCC should consider recommending a framework to standardise key terms used in privacy notifications, for example addressing the issue in the proposed Code of Practice.

## Preliminary recommendation 9 – OAIC Code of Practice for digital platforms

Financial Rights in principle supports the development of effective and enforceable Codes of Practice to improve consumer outcomes in areas where legislation fails to provide specific details. They are also, generally speaking, more easily reviewable and updated, in a dynamic industry – more so than changing legislation.

Financial Rights notes that the proposal has similarities to the current OAIC administered *Privacy (Credit Reporting) Code 2014*.

It is important that a Code of Practice for digital platforms be monitored by an independent administrative body.

The current governance structure for the Credit Reporting Code is not sufficiently robust to enable stakeholders to have confidence in the credit reporting system. Nor does it sufficiently deal with conflicts of interest.

Consequently, the establishment of an OAIC Code of Practice for digital platforms should be monitored by an independent Code Compliance Committee, established under the Code. This Committee should:

- be independent of the digital platforms sector (with a balance of industry representatives, consumer representatives, and an independent chair); and
- be provided with adequate resources to fulfil the relevant functions and to ensure that code objectives are not compromised

The current governance structure of the Credit Reporting Code relies almost entirely on Credit Reporting Bureaus monitoring Credit Providers' compliance with their Part IIIA obligations, incorporated in their agreements with the Credit Reporting Bureaus. This structure presents an unacceptable conflict of interest.[18] A similar mistake should not be made in an OAIC Code of Practice for digital platforms.

Financial Rights points to the Codes of Practice in Banking and Insurance as examples of ways to structure oversight.

Finally the Code of Practice provides an opportunity to address many of the issues raised in the Preliminary Report namely:

- the inconsistency and vague terminology used in privacy terms and conditions

[17] https://treasury.gov.au/consultation/c2019-t354736/

[18] CPs are the paying clients of CRBs, and CRBs will necessarily be dis-incentivised to report their incidents of non-compliance under the Code. Even if each CRB establishes a documented, risk based program to monitor CPs' compliance, there will inevitably be less thorough reporting of all non-compliant activity than there would be under an independent administrative body. Less thorough reporting means that systemic problems will either not be identified or will continue for longer.

- the difficulty in navigating terms and conditions
- the difficulties in accessing and finding privacy statements on websites;
- the use of vague and ambiguous language;
- the use of online tracking technologies;
- the difficulties in switching off location tracking

Other commitments can also be included in the Code of Practice including adhering to 'Privacy by Design' Principles, implementation of ethical data management principles and human design standards.

### Preliminary recommendation 10 – serious invasions of privacy

Financial Rights supports the introduction of a statutory cause of action for serious invasions of privacy

### Preliminary recommendation 11 – unfair contract terms

Financial Rights supports the recommendation that unfair contract terms should be illegal (not just voidable) under the ACL, and that civil pecuniary penalties should apply to their use, to more effectively deter digital platforms from leveraging their bargaining power over consumers by using unfair contract terms in their terms of use or privacy policies.

## 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 Financial Rights on (02) 9212 4216.

Kind Regards,

Karen Cox
Coordinator
Financial Rights Legal Centre
Direct: (02) 8204 1340
E-mail: Karen.Cox@financialrights.org.au