Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

3 October 2019

ACCC

By email: loyaltyschemes@accc.gov.au

RE: Draft Report – Customer loyalty schemes

This submission from the Australian Privacy Foundation (the "APF") responds to the ACCC Draft Report on Customer loyalty schemes. The APF welcomes the decision by the ACCC to review the operation on customer loyalty schemes, and we strongly support reform in this area.

This submission will focus mainly on the data practices issues outlined in the Draft Report.

General comments

Privacy is about the control of one's personal information. Customer loyalty schemes take that control away. They deprive people of fundamental privacy rights with the use of very unfair practices. Businesses with customer loyalty schemes do this by:

- Burying unfair terms in fine print
- Misleading people about the actual nature of the agreement they are making – where the valuable commodity involved is their personal information, not their 'loyalty'
- Selling information to third parties
- Linking information and profiling people, even when those people do not want to be tracked
- Using the data for a range of secondary purposes that the person never understands and has not consented to
- Obtaining ostensible contractual consent by burying it in incomprehensible terms and conditions
- Refusing to delete or change personal information or provide information on request

The Draft Report covers many of the above issues, and we strongly support urgent reform.

Prohibition against unfair contract terms and certain unfair trading practices

The APF supports the proposed prohibition on unfair terms and certain unfair trading practices. We also support the move to prohibit unfair terms, instead of making those terms voidable.

When a person decided to enter into an agreement, they should not be faced with trying to find what terms are unfair. Instead those terms should have been removed already by the business.

The APF also stresses that privacy policies are part of the agreement for a customer loyalty scheme. Often the privacy policy is buried elsewhere on a website, and is not even incorporated into the terms and conditions. For example, the Flybuys terms and conditions refer to the privacy policy which is a separate document. In this case the person who wanted to read the terms and conditions for Flybuys would not even know that Flybuys can exchange information with service providers (and it is completely unclear who these entities are) at section 5.

In this case, the unfair practice is to hide the important information about data practices in a completely different document, and then rely on the multiple documents to indicate consent to everything, even though it is highly likely the person will not have appreciated the extent and implication of the fragmented terms. This is unfair. This is not an 'unfair term' per se, but instead it is the practice itself that is structurally unfair. It is a deliberate attempt to make it difficult to understand the nature of the agreement being entered.

We strongly urge the ACCC to use the *Australian Consumer Law* to review, investigate and take action against unfair terms and practices in relation to privacy policies. When considering unfair terms that investigation must cover privacy policies that are part of the terms and conditions for customer loyalty schemes. The ACCC should consult the Office of the Australian Information Commissioner (OAIC), but the fact that there are multiple regulators must not stop action on this point by ACCC.

Recommendations

The Australian Consumer Law must be amended to prohibit unfair terms and certain unfair trading practices.

The ACCC must work with the OAIC to identify and remove unfair terms in privacy policies.

The value of consumer data and the nature of the agreement

The collected data from customer loyalty schemes is incredibly valuable, both as an asset and a resource. The Draft Report confirms this extensively. Our concern is that the value of the data is such a key part of the agreement that the failure to disclose that fact is actually misleading.

When people enter into an agreement it should be a meeting of minds and in good faith. It should not be based on trickery where the person hands over something incredibly valuable for little or no reward. This is one of the fundamental problems with customer loyalty schemes, people do not understand that it is a very poor and very one-sided bargain.

It is also important to emphasize (both in terms of policy and in the communication to the person being invited to consent) that this great value to collectors, and to the rest of the 'commercial surveillance' industry participants who may be in a position to exploit it in some way, comes intimately linked with substantial risk projected onto the person who is the subject of the information. This is a potential long term, invisible risk that in Australia at present is not adequately shared by the collector and those other entities, is difficult to assess and understand,

and is not properly appreciated by most ordinary people, especially going into the future as data security threats proliferate and opportunities for misuse expand with new technologies.

Disclosure will not work

There is a lot of evidence that disclosure does not work. A review of the terms and conditions for customer loyalty schemes reveals very poorly drafted inaccessible agreements. As mentioned above, you may have to read two or more documents to find out the full extent of what has been agreed, and even then, the potential range and duration of risks are typically omitted or underplayed. And in any case, most ordinary people do not read the fine print, even if it is in a bigger font size. The Australian Securities and Investments Commission summarised this issue as follows:

> *Economic research in behavioural economics, as well as the experience of regulating retail financial markets, indicates that investors and consumers are prone to behavioural biases that mean decision making is often not instrumentally rational. This undermines the effectiveness of disclosure as a regulatory tool. Importantly, these behavioural biases are significant and systematic, rather than random and trivial.*[1]

Even if people understood that it was a manifestly unfair and poor value agreement, they would still be unable to change the deal, one whose terms are unilaterally developed by one party. The business can and will just say these are the standard terms. Behavioural biases will still lead people to enter the schemes. If people are unable to negotiate a fairer deal, and unlikely to appreciate the implications of what the full deal actually involves, then it follows that consumer protection is required.

The APF contends that one important way to 'level the playing field' and introduce fairness back into the agreement is to change the way that data can be used. When people hand over their data, they expect it will only be used by the primary company, and for the benefit of the customer, not as a way to make money surreptitiously. It is unfair to allow any other use of the data without specific and separate (in time) consent. With this amendment, the agreement becomes a fairer and more transparent agreement.

Recommendation

Personal information data should not be shared with any third party, and this term should be prohibited as an unfair term.

Sharing with third parties should only be permitted if separate and informed consent is obtained on a different day to the making of the agreement.

Creepy conduct and the need for audits

As acknowledged in the Draft Report, people have no real control of their personal information when in a customer loyalty scheme. People do not know where their information is or how it is

[1] ASIC, Financial System Inquiry: Submission by the Australian Securities and Investments Commission, April 2014, para 40.

being used. The personal information is likely in many places all over the world including in multiple places all over Australia.

We strongly believe that the ACCC and the OAIC need to work together to ascertain where and how all this information goes and is used. The Draft Report provides a general overview but there is no real detail. People need to know where their personal information has gone in detail. More importantly, if they want to delete that personal information, any shared information also needs to be deleted.

It is genuinely creepy to consider detailed personal information being shared all over the world and in Australia. Privacy policies provide almost no detail, and even when disclosure does work this is usually no disclosure at all about this important feature.

As stated above, the use of the data to send anywhere should be prohibited as an unfair term. However, if this recommendation is not adopted there must be the following further changes:

1. The privacy policy must contain specific detail on how the data will be shared.
2. This should include an easy way to track exactly who a person's information is going to be shared, and who actually received or accessed it, including by several removes not just the first 'hop' from the collector. Contact, corporate and other identifying details of each such entity should be easily accessible from the initial information or terms offered.
3. Any consent must be separately obtained and meaningful.
4. The disclosure should include details of the value of the data so the customer knows that this value is a key part of the benefit for the business.
5. The ACCC and the OAIC should regularly and randomly audit the sharing of data and monetisation.

Recommendations

As stated above, data should not be shared with third parties.

If data is to be shared, the privacy policy must set out exactly how data is shared, with who and where in specific detail. People should be given the ability to make a preference on what data is shared.

The ACCC and the OAIC must be regularly auditing the conduct of businesses to monitor how data is shared and monetised.

Draft Recommendation 3

The APF strongly supports the recommendation to improve the data practices of loyalty schemes. As we have outlined above, we believe that these measures need to go further and we have made specific recommendations on what further action is required.

The recommendation lacks detail so we expect that details of how those changes will work in practice will be provided by the ACCC.

Recommendation

The APF supports Draft Recommendation 3.

We expect further detail on how this recommendation would be implemented in practice. The ACCC needs to set standards on how these changes would be achieved.

Draft Recommendation 4

The APF strongly supports draft recommendation 4. We have outlined our position on these recommendations in our submission to the Digital Platforms Inquiry[2]. That position is set out again below with some extra detail.

Update 'personal information' definition

APF supports the above recommendation, but notes that special care must be taken to ensure that any definitional changes clearly overcome the difficulties and uncertainty created by the decision of the Federal Court in *Telstra v Privacy Commissioner*.[3] This was based on a now-obsolete and ambiguous definition in the former version of the Act, and accordingly its reasoning deliberately ignored the implications of later explicit statutory recognition of device and other technical and telecommunications metadata as personal information. Such a change would involve making it clear that information is 'about an individual' if it can (given current technologies), contribute to the identification of an individual. Such a clarification of the definition of 'personal information' is important to the ACCC's concerns, because IP addresses, device and network connector identifiers, telecommunication geolocation data points, URLs and similar data are among the types of data most commonly correlated by Google, Facebook and others in order to identify data that is about an individual. The EU's General Data Protection Regulation (GDPR)[4] now explicitly includes online identifiers and location data within its definition of 'personal data', and a similar approach is highly desirable in Australia.

APF further submits that the definition of 'personal information' in the *Privacy Act* ought to be amended to clarify that it encompasses data drawn from the profiling or tracking of behaviours or movements such that an individual can be singled out (i.e. disambiguated from a crowd or cohort) and thus can be subjected to targeting or intervention, even if an individual cannot be 'identified', in the conventional sense, from the data or related data on its own at the point of collection. The Government should consider such an amendment, which would place Australia's *Privacy Act* on a par with the best laws dealing effectively with the harms which the ACCC has identified.

It should also deal with the increased future potential for re-identifiability of records in those data sets which are based on unit data about the behavior of individuals but have then been subject to attempts to limit identifiability by using currently accepted de-identification methods. These methods, even if arguably effective enough now, are likely to become less successful over time, and this needs to be recognized in the core explanation of the scope of 'personal information'. (Only a subset of loyalty scheme data will be affected by this.)

[2] Available at https://privacy.org.au/publications/by-date/.
[3] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 ('Grubb Case')
[4] General Data Protection Regulation (EU) is now the key regulation in European Union law on data protection and privacy for all individual citizens of the European Union. It has both legal effect (for certain personal data) and persuasive influence globally, not just in Europe, and is the de facto benchmark of serious data protection.

ACCC R16(b) Strengthen notification requirements

APF supports these recommendations, but submits that the Government's legislation should be more specific, and should specify (as ACCC suggested in its draft Report, p. 227) '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'. It is essential that individuals be told the purposes for which their personal data is collected, so that they can insist that the collector should only use the data for that purpose (subject to legislative exceptions). Such informed consent and consequent control reaffirms individual autonomy and serves to build trust in online interactions across the public and private sectors, a trust weakened by public awareness of recurrent large-scale data breaches and other problems involving large organisations.

If there is third party collection there should also be a duty on the APP entity to require (by contract or otherwise) the third party to deliver the notice. A third-party collector may not itself be an APP entity, so the obligation needs to rest with the APP entity.

Strengthened consent requirements and pro-consumer defaults

APF support these recommendations, but submit that it should specifically state that the onus of proof of compliance with all consent conditions lies with the collector of the information. APF also submit that separate consents should be required for each separate purpose ('unbundling' of bundled consents as a means to ensure each consent is understood for what it is, and not given where there is no real consent for that practice); and that furthermore, information for which consent is required should be unbundled from any information for which consent is not required. As ACCC states, steps need to also be taken to minimize 'consent fatigue', and particularly to avoid requiring the same consent on multiple occasions.

However, the APF also submits that tightening up the meaning of 'consent' alone will not be sufficient. It is also necessary to tighten up the wording in relation to collection necessity (APP 3.1-3.2), and use/disclosure for 'related' secondary purposes (APP 6.2(a)), in order to require companies to rely on genuinely informed 'consent' as the legal basis for collecting, using or disclosing any personal information that is *not strictly necessary* to fulfil the original transaction. Otherwise Facebook, Google and other companies will simply sidestep any new/stricter consent rules, either by defining their primary purpose in an overly permissive manner, or by arguing that their handling of personal information is 'related' to the primary purpose in some way as outlined in their privacy policy.

The extraordinary breadth allowed under the 'related secondary purpose within reasonable expectations' test, given the OAIC's loose interpretation of APP 6.2(a) in dismissing a complaint about the deliberate release by Centrelink to the media[5] of the personal information of a welfare recipient, and particularly the personal information of her partner whose knowledge and implied consent were not established, demonstrates the inability of APP 6.2 to constrain even egregious behaviours under the current Australian regime.

A further concern that needs to be addressed is the tendency of APP entities to adopt a 'take it or leave it' approach, and require consent as a non-negotiable term of contract. APF contends that

[5] See https://www.oaic.gov.au/media-and-speeches/statements/centrelink-debt-recovery-system#concluding-statement-centrelink-release-of-personal-information (currently unavailable due to website changes)

consent to collection or use or disclosure of any item of personal information can only be a condition of use if the denial of consent can be demonstrated to undermine the provision of the service.

The government should ensure that the "take it or leave it" approach to consent and "bundled" consent are both clearly interpreted as unfair terms which the ACCC can take action to remove under the unfair terms provisions in the Australian Consumer Law.

Finally, the government should ensure that the effectiveness of consent is "consumer tested". Many consumers have been worn down and effectively trained to give consent as part of service provision, in part due to the difficulty or impossibility of understanding the implications of the terms offered. To ensure that consent is meaningful and not illusory it is necessary to independently test what consent is effective, and in particular how the knowledge of implications and risks can be effectively shared with the person involved.

When an effective method is designed, tested/evaluated and confirmed to work then that method should be made mandatory.

Enable the erasure of personal information

APF supports this recommendation, and gives particular strong support to the fact that the recommendation is not limited in its scope to information provided by the data subject on the grounds of 'consent' in the first place.

This broader erasure right is essential to a modern data privacy law. The European Union experience with the so-called 'right to be forgotten' pre-dates the 'erasure' right in GDPR art. 17, and originates in the *Gonzalez* decision of 2014.[6] In both pre- and post-GDPR, the right to 'de-linking' (and thus privacy through obscurity), or in some cases actual erasure, has been available to those whose personal data was collected without their consent, including under statutory authority. The overall experience in the EU has been positive, and data protection authorities and courts have been prudent in determining where use of the right is appropriate. APF submits that such a right, not limited to consent-based provision of data by data subjects, should also be adopted in Australia. Given the resistance of Australian courts to adopt any expansive interpretations of privacy protections (on the basis that law reform is a matter for legislatures informed by recommendations from a succession of law reform reports[7]), the Government needs to ensure that any erasure right is worded so as to expressly incorporate a de-linking right such as adopted by courts in the EU.

The APF has watched with concern that a key right to deletion or erasure was dropped from the Consumer Data Right (CDR) legislation (also marketed as 'open banking'). We understand there is some negotiation to reinstate that right. However, although concern remains that this fundamental right (one that is available in the EU, and under consideration in other jurisdictions) is not present in recently legislated 'data portability' legislation, its value is not in any way limited to the context of data portability, and it should be explicitly included in reforms based on the ACCC recommendations here.

Establishment of such a right is constitutionally permissible and would not be contrary to recurrent High Court judgments about the implied freedom of political communication. We emphasise,

[6] *Google v AEPD & Gonzalez* (2014) CJEU

[7] Despite the fact that the consistent key recommendations for the last three decades and five ALRC reviews, particularly that Australians should no longer be denied the right to sue for breach of privacy, have not been addressed by or put before the legislature.

consistent with EU jurisprudence, that consent should be substantive rather than merely formal, and we draw the Government's attention to exploration by the Department of the Treasury about technical mechanisms to facilitate meaningful informed consent in relation to the Australian Consumer Data Right.

Introduce direct rights of action for individuals

We give strong support to this Recommendation. It is crucial that individuals can seek access to justice when there has been an interference with their privacy. To provide meaningful access to justice there must be two paths available:

(i) access to Court to seek compensation and other orders; and
(ii) access to an alternative free dispute resolution scheme (which is the OAIC).

It is essential to have both options because many people cannot afford to go to Court, but must be able to seek compensation without needing to do so.

However, the investigation and enforcement functions of the Privacy Commissioner have operated in a very unsatisfactory manner for many reasons (some of which are discussed below), only some of which can be addressed by providing more resources to the OAIC. In particular, there have been long delays in even opening files to deal with complaints, an extremely limited number of actual determinations after a prolonged process where a file is opened, and no effective right to require a determination or to appeal its merits if the outcome is unsatisfactory. It is therefore of equal importance to allow direct access to the courts to those who wish to take that route to obtain compensation, and have the means to do so.

APF notes that the Law Reform Commissions of at least the Commonwealth, NSW and Victoria have published detailed analyses and Recommendations to this effect in 2008/2014, 2009 and 2010 respectively, alongside recommendations by parliamentary inquiries. Those recommendations are practical, the result of extensive and repeated consultation with all affected stakeholders, and have not been opposed by consensus bodies such as the Law Council of Australia.

Where individuals have sufficient resources to take a breach of the *Privacy Act* before the courts, without need to first complain to the OAIC, there are very good reasons to enable them to do so, including practical reasons such as:

(i) where plaintiffs are willing to fund their own litigation, with the risk of the award of costs against them, this is one indicator of the seriousness of a complaint; and
(ii) where cases go before the courts, this may reduce the costs to the OAIC of multiple repeated complaint investigation and enforcement actions.

However, the most important reason for supporting an alternative enforcement route is that it will mean that courts will have the opportunity to interpret the *Privacy Act*, and courts will through their judgments set standards for what are appropriate types and levels of penalties and compensation for privacy breaches. This has not occurred under the current 'no right to sue' model. It is common in most other subject areas of regulation and consumer protection in Australia, and operates without controversy in most other comparable jurisdictions in one form or another, including those in New Zealand, UK, US, Canada, EU and many Asia Pacific countries.

The APF also notes the importance of the transparency provided by both litigation and by the ACCC's engagement with professional and other communities. A key weakness of the OAIC regime under the *Privacy Act 1988* is that agency's ongoing emphasis on closed-door complaint resolution, and its

resistance to disclosure of how it makes decisions in response to complaints. Such resistance is ironic given the OAIC's role as the Commonwealth's freedom of information agency, and the strong desire across both industry and civil society for information that will enable stakeholders to understand how the OAIC is interpreting the *Privacy Act*. Litigation would provide the 'sunlight that is the best disinfectant' for administrative inefficiency, errors of law, and consumer exploitation. It would offset the growing disquiet among Australian consumers evident in empirical research about the timeliness and sufficiency of the OAIC's handling of complaints.[8] It would help provide the certainty that business expects in dealing with consumers, governments and other enterprises.

If you have any questions please do not hesitate to contact Kat Lane or APF chair David Vaile.

Yours sincerely

Kat Lane,
Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

About the Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems.

The APF makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters. Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance. When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

[8] See for example Jodie Siganto and Mark Burdon, 'The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going Through the Motions?' (2015) 38 (3) *University of New South Wales Law Journal* 1145.