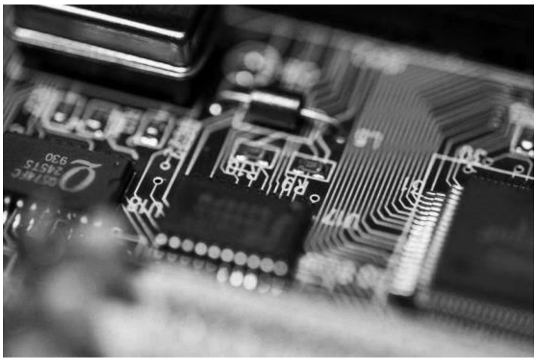
Submission by Salinger Privacy

ACCC's Draft Report on Customer Loyalty Schemes

30 September 2019



SalingerPrivacy

We know privacy inside out.

Covering letter

SalingerPrivacy

We know privacy inside out.

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655

30 September 2019

Mr Rod Sims
Chair
Australian Competition and Consumer Commission
VIA EMAIL: loyaltyschemes@accc.gov.au

Dear Mr Sims,

I am writing to submit the attached comments by way of a submission to the ACCC's Draft Report into Customer Loyalty Schemes.

I have no objection to the publication of this submission.

Please do not hesitate to contact me on (02) 9043 2632 if you would like clarification of any of these comments.

Anna Johnston
Director | Salinger Privacy

Introduction

This submission makes the following arguments:

- The ACCC's Draft Report on Customer Loyalty Schemes (the Draft Report) has under-estimated the degree of harm to consumers which can flow from participation in customer loyalty schemes;

- The Draft Report has under-estimated the degree of harm to consumers *even if they do not join* customer loyalty schemes; and

- Our legal system is not currently equipped to regulate the harms to consumers from individuation, which arises from practices of market segmentation and targeted advertising.

The harm to participants in customer loyalty schemes

The Draft Report discusses the potential impacts for consumers of their participation in customer loyalty schemes in fairly benign ways, such as "targeted advertising and personalised marketing". We submit that this under-estimates the potential negative impacts on consumers.

Consumers may not be aware that if personalised discounts can be offered, then so too can price rises, or access to a market in the first place, be 'personalised'.

When we read about companies 'tailoring their offers' for us, it is not only discounts they could be offering. It can mean the price I see is higher than that offered to another customer; or I might not know that the product or service exists at all.

The objective of customer loyalty schemes is to collect enough data that the retailer can predict their consumers' purchasing interests, and drive a purchase decision. In an online market, the implications for us as individual consumers are particularly acute.

In the hard copy world, advertisers will choose what ads to place in which newspaper or magazine, based on the target audience for that publication, and what they know about the demographics – in aggregate – of the readership. A retailer might place an ad for a luxury sedan in the *Australian Financial Review*, an ad for a family SUV in the *Australian Women's Weekly*, and an ad for a ute in *Fishing World*. Anyone can walk into a newsagent or library, and buy or flick through a newspaper or magazine. Everyone looking at that newspaper or magazine will see exactly the same ads as everyone else.

But in the digital world, advertisers use micro-targeting to find a class of individuals – for example, busy middle class mums if that's their target market for a family SUV – no matter what they read online, or how else they consumer advertising. Data brokers' promise to retailers is that they can find exactly who they want, and show those consumers the retailer's ad – and exclude everybody else. So two people reading the same newspaper story online, or looking at the same website at the same time, or receiving newsletters from the same retailer, will see two different ads.

Algorithms can lead to price discrimination, like surge pricing based on Uber knowing how much phone battery life you have left. Or market exclusion, like Woolworths only offering car insurance to customers it has decided are low risk, based on an assessment of the groceries they buy. Or predatory marketing; for example Australian Facebook executives were found to be touting to advertisers their ability to target psychologically vulnerable teenagers.

Once we move beyond straight-up advertising and into predictive analytics, the impact on individual autonomy becomes more acute. Big Data feeds machine learning, which finds patterns in the data, from which new rules (algorithms) are designed. Algorithms predict how a person will behave, and suggest how they should be treated.

Banks have been predicting the risk of a borrower defaulting on a loan for decades, but now algorithms are also used to determine who to hire, predict when a customer is pregnant, and deliver targeted search results to influence how you vote.

Further, by allowing exclusion, targeted advertising also allows discrimination. For example Facebook has been caught allowing advertisers to target – and exclude – people on the basis of their 'racial affinity', amongst other social, demographic, racial and religious characteristics. So a landlord with an ad for rental housing could prevent people profiled as 'single mothers' from ever seeing their ad. An employer could prevent people identifying as Jewish from seeing a job ad. A bank could prevent people categorised as 'liking African American content' from seeing an ad for a home loan.

Privacy of non-participants can be affected too

While offering consumers better education, transparency, choice and control over their participation in customer loyalty schemes is a positive step, that alone is not sufficient privacy protection.

Even leaving aside the power imbalance between an individual and a company, and leaving aside also the issue of digital literacy of consumers, there are some fundamental flaws in the idea of consumer control as a solution to privacy challenges.

This is because one person's privacy can be negatively affected by a *different* person making choices about their own personal information.

Targeted advertising is built on data about classes of people with shared characteristics. Let's say for example an algorithm has been built on data from people who have 'consented' to share their data, in a research project. That algorithm then makes predictions about people who share certain characteristics. For example: that indigenous students are more likely to fail first year Uni than non-indigenous students, or that people who buy lots of pasta are at higher risk of car accidents.

When that algorithm is operationalised, it is going to result in decision-making affecting *everyone* with those characteristics (or who is believed to share those characteristics), never mind that they were not part of the original group who ‘consented’ to the use of their data for the research project.

To suggest that as consumers each of us must take individual responsibility for our own privacy, and therefore consumer education and control in relation to customer loyalty schemes is the solution to privacy challenges, misses the bigger picture.

If we think of managing privacy as private and transactional, then the ideas of notice and consent, choice and control sort of make sense. But that’s not actually the world we live in. As individuals, we have no control over the data ecosystem we find ourselves in, any more than as individuals we have control over the quality of the air we breathe or the water we drink. It is only as a public, enforcing our collective will though laws to regulate companies’ behaviour, that we can have any impact.

Privacy is a public good, which is why privacy protection cannot be left to the actions of individual consumers.

The gaps in our system of legal protection

There are two main weaknesses in our current system of privacy protection for individuals:

- An assumption that privacy harms can be avoided by a system of consumer choice, and
- An assumption that privacy harms can only occur if an individual is *identifiable*.

Privacy laws are predicted on an assumption that privacy harms can only occur if an individual is *identifiable*. Privacy statutes are therefore typically structured around a threshold definition of ‘personal information’, with the handling of data regulated only if individuals are *identifiable* from that data.

However it is my submission that trying to model all regulation of data handling practices based this type of ‘identifiable or not’ binary legal structure is not helpful. If our objective is to protect people’s privacy, our laws need to grapple with a broader view of the types of practices which can harm privacy – regardless of whether or not a person is identifiable.

The UN’s Special Rapporteur on Privacy, Joe Cannataci, has written about privacy as enabling the free, unhindered development of personality. You could think of privacy as related to the right to self-determination, or as an element of autonomy.

And if you think of the purpose of privacy laws as protecting individual autonomy, we should be ensuring that our laws regulate all types of activities which can impact on autonomy. Because it is *individuation*, rather than *identification*, which can trigger privacy harms.

In other words, companies can hurt someone without ever knowing who they are.

Individuation means a company or government can disambiguate the person in the crowd. This is the technique used in online behavioural advertising; advertisers don't necessarily know who an individual is, but they know that the user of a particular device has a certain collection of attributes, and they can target or address their message to the user of that device accordingly.

The Facebook / Cornell University 'research' project on emotional contagion offers another fine example of causing privacy harm, without 'personal information' being involved. Although the researchers argued that no personal information was at stake (and, thus in theory there were no privacy impacts) because they did not know who their research subjects were, they deliberately manipulated the news feeds of almost 700,000 Facebook users, in order to trigger emotional outcomes for people who had no idea they were even part of a 'research' project.

As with the examples of price discrimination and market exclusion mentioned above, these activities hold the potential to impact on individuals' autonomy, by narrowing or altering their market or life choices.

Philosophy professor Michael Lynch has said that "taking you out of the decision-making equation" matters because "autonomy enables us to shape our own decisions and make ones that are in line with our deepest preferences and convictions. Autonomy lies at the heart of our humanity".

Yet for now, our legal protections for privacy only start to apply when there is an 'identifiability' dimension to an activity.

We submit that the ACCC should consider the scope of our privacy laws, with the objective of consumer protection being to regulate practices of individuation, as well as identification, so as to protect individual consumers' autonomy in life and market choices.

Conclusion

Existing patterns of social exclusion, economic inequality, prejudice and discrimination can be further entrenched by micro-targeted advertising, which is hidden from public view and regulatory scrutiny.

These practices impact not only consumers who actively participate in customer loyalty schemes, but *all* consumers.

Fiddling with rules about transparency or fairness of terms and conditions for participants in customer loyalty schemes is not nearly enough. Improving controls set at the individual level will achieve almost nothing. Instead, we need collective, political and regulatory action.

Automated decision-making diminishes our autonomy, by narrowing or altering our market and life choices, in ways that are not clear to us, and over which we have no control or choice. People already in a position of economic or social disadvantage face the additional challenge of trying to disprove or beat an invisible algorithm.

In a predictive and pre-emptive world, individual dignity, autonomy and free will are programmed out of our society.

If we want our lives to be ruled by human values and individual dignity, and if we want to preserve consumers' autonomy over their life and market choices, we need robust, enforced and effective privacy laws, which are predicted in their scope and reach on the ability for an individual to suffer harm, rather than whether or not an individual was identifiable from a piece of data.

About the author

This submission has been prepared by Anna Johnston, Director, Salinger Privacy.

Anna has served as:

- Deputy Privacy Commissioner of NSW
- Chair of the Australian Privacy Foundation, and member of its International Committee
- a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
- a member of the Advisory Board for the EU's STAR project to develop training on behalf of European Data Protection Authorities
- a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
- a Member of the Asian Privacy Scholars Network
- a member of the Australian Law Reform Commission's Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
- an editorial board member of both the *Privacy Law Bulletin* and the *Privacy Law & Policy Reporter*.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the designation of Fellow of Information Privacy (FIP).

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).

About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy resources, training, and consulting services.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

We consult, train, publish, blog and tweet on all things privacy.

Find out more or sign up for our email newsletter at
www.salingerprivacy.com.au

SalingerPrivacy

We know privacy inside out.

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655