CHOICE

PRIVACY ACT REVIEW

Response to Issues Paper, December 2020

ABOUT US

Set up by consumers for consumers, CHOICE is the consumer advocate that provides Australians with information and advice, free from commercial bias. By mobilising Australia's largest and loudest consumer movement, CHOICE fights to hold industry and government accountable and achieve real change on the issues that matter most.

To find out more about CHOICE's campaign work visit www.choice.com.au/campaigns

57 Carrington Road Marrickville NSW 2204

Phone 02 9577 3333 | Fax 02 9577 3377 | Email campaigns@choice.com.au | www.choice.com.au

The Australian Consumers' Association is a not-for-profit company limited by guarantee. ABN 72 000 281 925 ACN 000 281 925

For consumers, there are two important questions about personal data:

1. Who has my data?
2. What can they do with it?

This response to the *Privacy Act Review: Issues Paper* (the issues paper) focuses on matters most relevant to the interactions between people in their role as consumers and businesses that hold and use their data.

The reforms explored in the issues paper are largely answers to the first question - who has access to someone's data, how did they get it, store it, pass it on and what are the remedies if they do the wrong thing. Protections about access to personal information can be strengthened and the proposals in this paper are a positive step forward. CHOICE is particularly supportive of measures to improve how privacy complaints operate including a direct right of action.

But the second question - what is done with data that companies or other parties hold - must be better dealt with. This issue can only be partly solved with notification, consent and transparency measures. **Rather than requiring a consumer to understand how a product or service may be harmful for them, it is far better to stop the harm.** With this in mind, we suggest that the Federal Government strengthens consumer protections by implementing a ban on unfair trading which would limit the most harmful practices in markets. A fiduciary duty for data holders will also address this issue by requiring companies to use data in their customers' best interests.

Finally, we ask that this inquiry consider the outcomes it hopes to achieve with any notification, consent or disclosure measures. We know from our experience across markets, especially the energy and financial services markets, that specific requirements for disclosure will fail if the company implementing them has a commercial interest that clashes with the intent of the disclosure. A company controls how information is presented and framed. Specific legal or regulatory requirements for disclosure are risky for this reason. It is much better practice to require that a company meet an outcome like showing that its customers understood what information was collected and why. As a next step, we suggest that the inquiry explore how performance-based regulation could be applied in a privacy context.

1. Limits of information-based protections

Notice, consent and disclosure can sometimes work when helping people to engage with certain up-front and clear decisions, like which specific parties should have access to their data.

However, current industry practice falls well below what consumers need. Privacy policies and terms and conditions that consumers are regularly asked to agree to online are absurdly long.[1] They are often written in dense jargon that nobody other than a highly-qualified privacy expert could understand. Within this dense jargon, disclosures or requests for consent can be infuriatingly vague. For example, consumers are informed that data may be shared with "trusted third parties" for marketing purposes with no meaningful information about who these third parties are or what they're selling.

Disclosure, consent and notification are not always appropriate protections. This is best outlined in ASIC's report, "*Disclosure: why it shouldn't be the default*".[2] Its findings about the limits of disclosure are equally applicable to consent and notification. The report found that:

- Simplifying language in disclosures does not help people understand a company practice that is inherently complex.
- Disclosure has to compete for consumer attention. Businesses have great power to attract, distract and influence consumer attention in ways that can reduce the effectiveness of mandatory disclosures.
- Disclosure can have the opposite effect than regulators intend by, for example, increasing trust in a business with a slick sign-up experience even when the practices they are informing people about are harmful.

[1] For example, in 2017 CHOICE hired an actor to read aloud the terms and conditions for the Amazon Kindle. It took him nine hours. You can listen to all nine hours at https://www.youtube.com/watch?v=6QZml7sPbVU&feature=youtu.be

[2] ASIC (2019) *REP 632 Disclosure: Why it shouldn't be the default,* https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/ accessed 1 December 2020.

- When disclosure is used poorly it places an "unrealistic and onerous burden on consumers."[3]

Disclosure can still be useful in some instances:

- Disclosure has a role in enhancing market transparency, integrity and efficiency. It is particularly important as a tool to help media, competitors and intermediaries to understand other practices. Third parties decoding or comparing company practices can lead to enhanced competition.
- Disclosure can provide a reference point for a consumer when they make a complaint.

In short, notification, consent and disclosure should be seen as tools with limited effectiveness. They cannot be used alone. They should be relied upon to increase transparency, competition and to help people engage with simple decisions that are relevant to them in the moment they are being asked.

2. Notification, consent and disclosure should focus on outcomes

Where this inquiry does make recommendations about increased notification, consent and disclosure, it should focus on mandating outcomes rather than specific processes for companies to follow.

We are concerned that some recommendations for increased privacy protections for consumers can be very process-based. They step out specifically how disclosure should occur, in what form and when. Businesses are easily able to circumvent prescribed disclosures by framing the decision with other information.[4] They often have commercial interests in doing so. This allows a business

[3] Ibid, p. 4
[4] Willis, Lauren E. (2013) "When Nudges Fail: Slippery Defaults," *University of Chicago Law Review:* Vol. 80 : Iss. 3 , Article 4. Available at: https://chicagounbound.uchicago.edu/uclrev/vol80/iss3/4

to comply with the letter of the law but not the spirit of it. Overly prescriptive requirements also contribute to “consent fatigue”.

Prescription is useful when the goal is transparency for public interest reasons - where the audience being served is an expert, researcher or intermediary serving to translate the information, especially when consistent standards are needed for data sharing. Prescriptive disclosures have a place, but are rarely the right approach where consumers are the primary intended target of the disclosure, notification or consent.

We encourage the inquiry to explore the work of Professor Lauren Willis who has put forward the idea of “performance-based consumer law”.[5] Her ideas could translate well in the privacy context. Prescriptive obligations require that a business must take certain action - they must post a notice, ask a question or have a tick-box someone must engage with. Performance-based obligations instead demand that an outcome must be achieved. A business must demonstrate that their customers engage with and largely understand what has been presented. They can demonstrate compliance through auditing, consumer surveys or other testing methods.

A performance-based model allows companies to innovate - they can experiment with how information is presented to achieve the best outcome. This model encourages businesses to use the user experience, marketing and copywriting skills they have for a positive consumer outcome.

An ideal approach would be to require businesses to disclose details for transparency reasons in a prescribed, clear form for experts and those consumers wanting a greater level of detail. How a company explains these details, for the purposes of notification, disclosure or consent, could be governed by performance-based measures.

[5] Willis, Lauren E. (2015) "Performance-Based Consumer Law," *University of Chicago Law Review*: Vol. 82 : Iss. 3 , Article 4. Available at: https://chicagounbound.uchicago.edu/uclrev/vol82/iss3/4

3. Protections beyond disclosure: unfair trading

Companies can cause acute harm to consumers when they use personal information or aggregated data in ways that target, discriminate or exploit. This is why protections are needed that restrict what companies can do with personal information and other sensitive data, regardless of how they sourced it or what permissions were given.

Currently there is no specific legal protection against a company using unfair practices, especially towards vulnerable groups of consumers.[6]

CHOICE has found examples where companies are using data against their own customers. In an investigation into Tinder's pricing practices for its premium dating service we found that:

- Tinder charges some people up to five times more than others for the same service.
- Prices varied by age.
- Tinder is using other factors to set prices.
- Tinder could potentially be using data on sexuality, gender, location or interests to set prices.
- Tinder doesn't clearly say that customers may pay a different price to someone else or that their data will be used to set prices.[7]

We strongly recommend that a law against unfair trading is implemented alongside any reforms to privacy protections. This would implement recommendation 21 of the ACCC's Digital Platforms Inquiry.

[6] See https://consumeraction.org.au/wp-content/uploads/2019/02/Unfair-trading-AltLJ.pdf
[7] https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/tinder-plus-op-ed

4. Protections beyond disclosure: fiduciary duty for data holders

Currently large businesses have significant power and resources to use data but few tangible responsibilities to customers. In the current environment, the material value of personal data justifies organisations using the same mechanisms to manage it as they use to manage money.

Fiduciary duties or obligations to act in a party's best interests have been effective protections for consumers using legal, health and financial services. They can be constructed to require that a business consider a specific individual's best interests - like we see with duties for financial advisers, lawyers and most recently mortgage brokers. Or, the obligation can require a company to act in the best interest of a cohort, like we see in the superannuation sector.[8]

A fiduciary duty would rebalance the dynamic between large businesses and consumers when it comes to privacy and data use.[9] Such a duty is particularly well suited to privacy and data management as it requires data holders to constantly monitor and assess their own decisions and actions, rather than place the burden of assessment on individual consumers. It recognises that consumers place their trust in companies when sharing their data but have little ability to confirm if their trust is being abused. The duty is flexible and adaptive in a way that prescriptive laws cannot be for fast moving developments.

Companies holding and using consumer data should have an obligation beyond simply telling people what they are doing. They should be required to meet a minimum ethical standard for action, best expressed as a requirement to act in the best interests of the people whose data they hold. We strongly encourage this inquiry to explore a fiduciary duty for data holders to ensure that businesses that hold someone's data have to use it in their interests.

---

[8] https://www.apra.gov.au/sites/default/files/spg_516_outcomes_assessment_december_2018_v3.pdf p.6

[9] Balkin, Jack M.,(November 2020). *The Fiduciary Model of Privacy* Harvard Law Review Forum, Vol. 134, No. 1 , Available at SSRN: https://ssrn.com/abstract=3700087