CPRC WORKING PAPER

Consumer Policy Research Centre

In whose interest?
Why businesses need to keep consumers safe and treat their data with care

cprc.org.au

CPRC

The Consumer Policy Research Centre (CPRC) is an independent, not-for-profit, consumer think-tank.
Our work is possible thanks to funding from the Victorian Government.

CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates.

Acknowledgements

Report author: Chandni Gupta

CPRC would like to thank the following people and organisations for their input, time and advice:

- Dr Jeannie Paterson (UoM)
- Dr Katharine Kemp (UNSW)
- Dr Kayleen Manwaring (UNSW)
- Dr Ron Ben-David (CPRC Board Member)
- Australian Communications Consumer Action Network
- CHOICE
- Consumer Action Law Centre
- Digital Rights Watch
- Financial Rights Legal Centre
- Foundation of Alcohol and Research Education

The views expressed in this report should not be attributed to them. CPRC is responsible for the views in this report, including any errors or omissions.

Statement of Recognition

CPRC acknowledges the Traditional Custodians of the lands and waters throughout Australia. We pay our respect to Elders, past, present and emerging, acknowledging their continuing relationship to land and the ongoing living cultures of Aboriginal and Torres Strait Islander Peoples across Australia.

Published by Consumer Policy Research Centre

Suggested citation: Consumer Policy Research Centre, In whose interest: Why businesses need to keep consumers safe and treat their data with care, March 2023

cprc.org.au

Table of contents

Introduction – moving beyond notification and consent

Issues of safety and fairness can no longer be regulated using consumer choice as the primary protection. Instead, consumers need a privacy law that stops harmful business practices before they cause significant harm.

As Australia and the world propel forward with more data and digital innovation than ever before, the onus continues to be placed on consumers to "choose" – choose accordingly, choose carefully, choose thoughtfully. Choice is touted as the antidote for navigating the complex digital economy. Yet, we now know through a myriad of behavioural studies that the market economy and governments at large have overestimated the extent that consumers can make informed and rational decisions with little market intervention to stop harm, especially in a fast-paced digital economy.[1]

Our privacy law still relies on notification and consent as the primary means of protecting consumers. By forcing consumers into a situation where they "decide once" about whether to share their data with a business but bear the consequences potentially for the remainder of their life is not a fair trade.

CPRC's previous research has confirmed that consumers consider the following common data practices to be unfair:

- Using personal information to make predictions about consumers.
- Collecting information about consumers from other companies.
- Sharing personal information consumers have provided with other companies.
- Selling personal information consumers have provided to other companies.
- Requiring more personal information than necessary to deliver products/services.

These are just the unfair data practices that the community is currently aware of. As data and digital innovation continue to grow in scope and velocity, new unfair practices and harms are likely to emerge. How do we create a digital experience that is fair, safe and inclusive to facilitate consumer trust in the growing digital economy? Many experts and organisations, including CPRC, have called for Australia's privacy law to go beyond consent. This paper looks deeply at what "beyond consent" options are available to protect consumers from harmful data practices.

Two concepts are explored in this working paper to address both current and emerging data harms:

- **Duty of care or best-interests duty**: operating similar to fiduciary duties in the finance sector to hold businesses accountable for how they collect, share, and use consumer data.
- **Privacy Safety Regime**: borrowing concepts from product intervention powers and product safety interventions, we propose options that would allow governments and regulators to stop or limit obviously harmful uses of data as well as a process for regulators to proactively restrict and test new harmful practices as they evolve.

The law needs to require more effort on the part of businesses to assess whether how they collect, share, and use data that results in fair outcomes for their customers. This burden can no longer remain on the shoulders of Australian consumers.

Methodology

The development of this paper has involved a combination of desktop and analytical research to identify how best-interest and duty of care obligations work across Australian and international legal frameworks. Research also involved analysis of different frameworks that are used to introduce temporary and permanent interventions when harm or the likelihood of harm is identified by regulators or governments.

This working paper benefited from advice and guidance from a variety of consumer and privacy experts, including academics (all are noted as experts when referenced in the working paper). CPRC collaborated with experts via one-to-one meetings and facilitated a roundtable held in December 2022. The roundtable also included a sketch artist from the Sketch Group agency who live illustrated the key discussion points. The imagery in this working paper is from those illustrations.

The aim of the discussions and the roundtable was to test the concepts outlined in an initial draft working paper. This published working paper takes into account the advice and guidance provided by the experts, for which CPRC is very grateful.

Duty of care or best-interests duty

Imagining businesses acting in the interests of consumers

Other laws that require businesses to act in consumer interests

The obligation to act in the interests of others is not new or even unique. The financial sector requires that many professions act in the best interests of customers via fiduciary duties. In sectors such as disability, medical and aged care there is an obligation to act in the interests of others via common law duty of care. It is also a concept that is being explored by academics in the energy sector.[2]

Within the digital economy, this concept currently has been implemented through the New York Privacy Act's (NYPA) Data Fiduciary Obligation[3] and via a duty of care for large technology platforms in the European Union.[4] In the United Kingdom, the proposed Online Safety Bill proposes a statutory duty of care for social media companies to keep their users safe and tackle illegal and harmful content on their platforms.[5] The duty of care sits within UK's broader negligence law framework which requires businesses to a duty of care to *"…the general public who use the facilities they create and enable*".[6] However, this concept within consumer data is relatively new and unexplored in the Australian context.

A fiduciary duty traditionally is simply an expectation that an entity in a position of trust will act in good faith.

Within a traditional construct, a fiduciary duty is often set between individuals. The fiduciary is responsible for making decisions that are ethically and legally in the best interest of the trustee (often referred to as a client).[7] While a duty of care may be seen as a broader concept, in some jurisdictions, such as the United States, a duty of care is embedded within a fiduciary duty framework which also includes a duty of loyalty (i.e. there are to be no conflicts with the interests of the client).[8]

In other settings, such as superannuation, the fiduciary duty operates less in a binary model as it expects the fund to act in the collective interests of its members.[9]

The 2023 Privacy Act Review Report has already proposed a type of best-interest duty that is specific to children, noting that the law should "*require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances*".[10] The opportunity here is for the Federal Government to expand such a proposal to apply to the best interests of all Australians, and not just a subset.

Shifting the burden

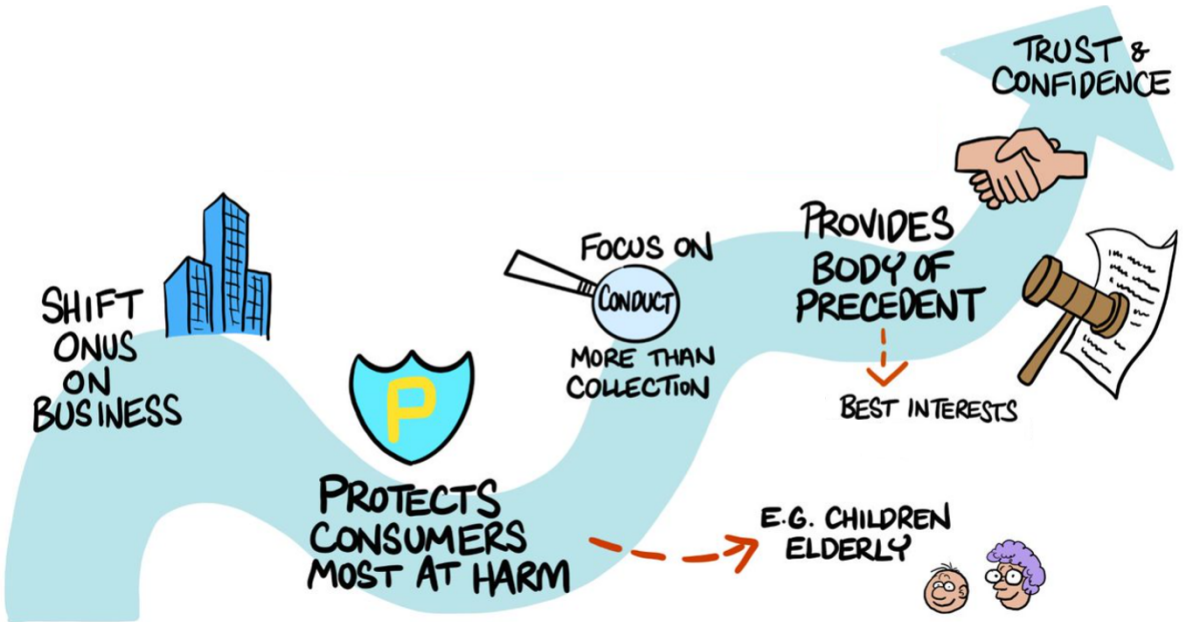
A best-interest or duty of care obligation shifts the onus onto businesses instead of holding consumers accountable to search for their best interests in a market economy that hasn't been developed with their interests in mind.

As an example, duty of care in an energy setting is being explored as imposing a "*positive responsibility on service providers… ensure compatibility between the provider's service offerings and customer's best interests"*.[11]

When it comes to how consumer data is treated and how choice architecture (the way a website or app is designed to influence how and what people choose) is presented and implemented on digital platforms, a best-interests duty or a duty of care model has the potential to provide a strengthened consumer protection framework. These concepts can help add a level of accountability on digital platforms that could significantly reduce the likelihood of consumer harm. It could also lead to pro-business benefits by increasing consumer trust that businesses will look after them.

Feedback from many consumer and privacy experts confirmed that a broader duty of care or best-interests framework would naturally shift the onus of responsibility from consumers to businesses. Such an initiative could:

- help move away from individual level of consent and shift the focus to system set-up and embedding safety by design
- protect people that may have the inability to consent such as children, people living with a disability or other consumers who are unable to participate in the consent model regardless of how well it may be set-up
- align interests of organisations and consumers as taking on new data will mean taking on new responsibilities and this can encourage a culture of data minimisation (collect only what you need not what you think you might need), and
- address issues of trust and confidence in both government and industry.



The tech neutrality of a broader framework that applies market-wide also makes it flexible to use across different technologies and tech industry. It moves away from the notion of regulating the consumer data aspect of specific technologies individually (e.g., artificial intelligence, facial recognition).

With the balance of responsibility tilting more towards the business in these models, an objection that can surface from industry is whether regulation in the data and privacy space will thwart innovation and limit the potential of the data at hand. However, the focus will need to shift to innovating for good, instead of innovating for the sake of profit. As Professor Jeannie Paterson of University of Melbourne noted in CPRC's webinar on unfair trading practices, "*Fairness doesn't stifle innovation, it just channels us to the right kind of innovation*".

What could a duty of care or best-interests duty look like?

A duty to individuals or to care for the collective?

While it appears to be a clearer and more familiar remit, in the data and privacy space, a one-to-one model may pose limitations to protections. It is now well-understood that individual data points and insights in aggregate can impact the products, services, and experiences of collective sets of individuals or communities. Also, given the significantly large number of users across many of the businesses that collect data, an effective system would need to expect a business to operate in good faith for large groups or the public as a whole.[12]

A broader framework that considers fairness and safety brings the opportunity to incorporate elements that may not have yet been considered in competition and consumer protection frameworks for digital settings.

A duty of care can be embedded within a fiduciary duty, but its focus is two-fold – avoiding practices that cause harm and putting in measures to ensure beneficiaries of the duty are protected from harms.[13]

For any new protection, Government must focus on limiting harms when businesses collect, share, and use consumer data. Often harm is obfuscated, and consumers are unable to assess the risk of current or future data harms, on themselves and on others.[14]

Even if consumers are given adequate information about how their data will be used, there still remains an asymmetry in power because, "*one party controls the design of applications and the other must operate within that design*".[15] CPRC's own research into dark patterns confirms that the prevalence of manipulative and deceptive design causes consumer harm. Australians have lost money, lost control of their data or have been manipulated by businesses to make choices that are not in their interests.[16]

Principle or prescriptive?

When considering a duty of care or a best-interests duty one element to explore is how it should be enshrined in law. Laws could be drafted to deliver:

- a general duty of care or best-interests statement that is broad to cover current, emerging, and future harms
- a prescriptive best-interests duty with specific bans and restrictions where the regulator is given authority to evolve the prohibitions over time, or
- a mixture of the two options with a flexibility for the regulator to impose new bans and restrictions.

How can businesses commit to fairness and safety?

A high-level principled approach could be enshrined into legislation. It could be as simple as the following statement:

> *A business must only collect, share, or use data in a manner that is in the consumer's best interest and avoids causing consumer harm*

The New York Privacy Act's data fiduciary obligation goes one step further by noting that it must be in the best interests of the state's citizens, "*regardless of how that impacts the interests of the business*". It captures the essence of fiduciary duties so when they come in conflict with the shareholders of a business, the duty to the consumer is given priority.[17]

In Europe, the Digital Services Act (DSA) calls for a duty of care but only for Very Large Online Platforms and Service Engines (VLOP and VLSE). While broad in its obligation, the DSA does outline the requirement of undertaking risk assessment, having a pathway to mitigate risks and conducting independent audits at their own expense.[18] There are mixed views on this duty of care, with some suggesting it as "ground-breaking" with its effectiveness becoming clearer with the introduction of specific legislation and guidelines,[19], while others claim that it is vague and lacks legal certainty.[20]

The above proposed statement could be also expressed inversely by outlining that a business cannot collect, share, or use data that is not in the consumers' best interests. This may limit the scope of what's expected but a broader duty can raise enforcement challenges. A broader framework could impose a positive duty on a business's data-based practices so they are implemented having both the individual's and the community's best interests in mind.

Whose data is it anyway?

Developing such a duty will require exploration of how to construct such a principle within regulatory measures relating to privacy. One particular issue to explore is how ownership of data is defined. Currently, there is a sense that the businesses who collect consumer data are in fact owners of that data. However, if data points (including direct and those related to) are all considered personal information, which they should be, then ownership and therefore duty of care can be effectively developed with the consumer being at the heart of that care.

One option is to consider if data could be defined as it is currently in the Consumer Data Right[21] (CDR) framework. Within CDR, there are clear parameters between data ownership and data access. It is understood that consumers are data owners and businesses who collect consumer data are data holders and other intermediaries that may have access to the data are accredited data recipients. Such a model, if implemented thoughtfully, can further shift the focus towards 'doing right by the consumer'.

One factor that the CDR framework does not address is the ownership of insights gained from collection of data. By default, it can be implied that in the current ecosystem, insights belong to the business. Within a best-interests or duty of care model, some aspects relating to insights could be dealt via the responsibilities linked with the use of data. A duty could expect that insights curated from data points, in particular those that lead to decisions on products and services offered should not leave consumers worse off.

The insights gained should be used to create a more positive and safe experience that is more meaningful for consumers. Currently, some of the harms that can take place due to ill-informed insights often originate from the lack of human oversight over algorithmic decision-making, often set up to identify and act on insights.[22] That lack of oversight can make it difficult to assess whether insights from specific data points accurately pinpoint a causation or whether it is simply coincidental correlation.[23] In the report by Human Technology Institute on facial recognition, the authors highlight a range of issues that could also be applied to use of data settings. Two in particular are the problems noted as "system error" or "abuse". System error is where the facial-recognition technology (FRT) accurately identifies an individual but aggregates other data incorrectly to produce inaccurate and potentially harmful decisions. Abuse relates to "deliberate misuse" of the FRT such as racial profiling.[24] These concepts could be embedded into a data duty to help create limitations on how insights are curated and utilised.

Practical options to make a duty a reality

Clear no-go zones

CPRC's previous research into exploring an unfair trading prohibition considered 'blacklists' as an approach to provide a clear expectation on what businesses can and cannot do. The same could be imagined within a duty of care setting. A more prescriptive form of accountability may make enforcement more clearcut, but rogue businesses are also likely to find loopholes that sit outside the 'no-go zones' that may still not be in the best-interests of the consumer.

Blacklists are used in legislation such as the Unfair Commercial Practices Directive in Europe and Consumer Protection (Fair Trading) Act in Singapore, both of which include adjunct documentation outlining specific business practices that are deemed unfair under their laws.[25]

Blacklists of harmful practices can be applied to specific types of data such as de-identified data which may need to be defined given that a broad framework may still be limited in its scope for such form of data. One example that was shared included a gambling platform purchasing de-identified data from a bank. A blacklist could ensure that such practices could be identified as a clear no-go zone enshrined into law under a broader framework. De-identified data may not necessarily impact an individual, but its aggregation and use may impact a group or community.[26] Experts highlighted that de-identified data can still be rich and valuable with the potential to be used against others that might fit a similar description but aren't part of the original data set.

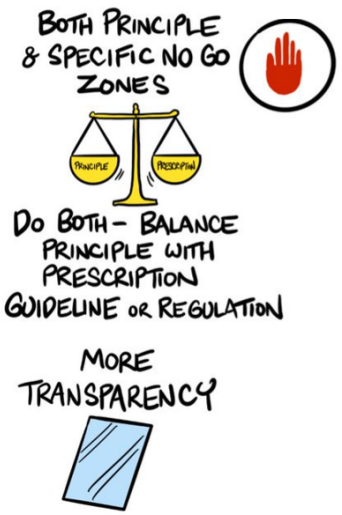
High-level principle with evolving guidance

It is likely that a more practical option is a framework that is broad but is supported by clear guidance and rules on data practices, including 'no-go zones' that evolves over time, noting that enforcement would not be limited to just these. Also, to ensure rules and the 'no-go zones' are fit for purpose in the current and emerging data-enabled environment, ideally it would be a measure that the regulator could have power to regularly review and update, instead of being enshrined in legislation.

An example of a broad approach to a duty of care that is supported via specific rules is the Financial Conduct Authority's (FCA) Consumer Duty in the United Kingdom which will come into effect from July 2023 onwards. This principles-based Consumer Duty requires businesses to "*act to deliver good outcomes for retail customers*".[27] The broad Consumer Duty is split across three key requirements.

> *"The cross-cutting rules require firms to:*
> - *act in good faith*
> - *avoid causing foreseeable harm*
> - *enable and support retail customers to pursue their financial objectives."*[28]

The guidance supporting the Consumer Duty and each of its three requirements outline conduct that businesses should and should not be engaging in. As an example, under the requirement 'Avoid causing foreseeable harm', there is a specific list of examples of foreseeable harms which includes conduct relating to the inability to cancel a product or service or incurring high fees due to lack of appropriately tailored information disclosures.[29]

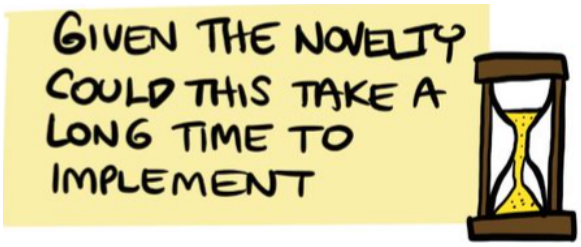


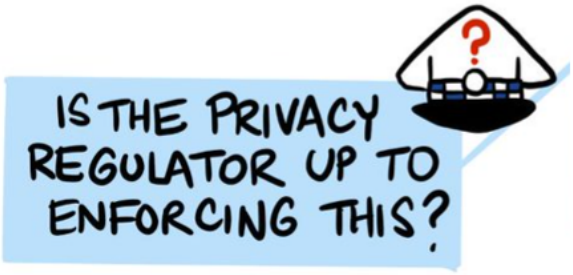
Such a model can provide the regulator with a broader remit if the regulator is adequately resourced to undertake more proactive enforcement. While we are yet to see the implementation of FCA's Consumer Duty, it is a model that has potential to be replicated in a data and privacy setting.

Embedding a fair and safe framework in law

There is, as in any broad framework, the possibility that a best-interests or duty of care obligation will create regulatory loopholes, especially in identifying which entities a broad duty applies to when the data supply chain is not a linear one-to-one process. A duty may be difficult to enforce given it also requires different enforcement skills and a different regulatory culture – one that is proactive, well-resourced and can identify and enforce issues before widespread harm occurs. Two options were explored by experts:

1. Framing the duty as an obligation.
2. Implementing a tiered approach to best-interests.

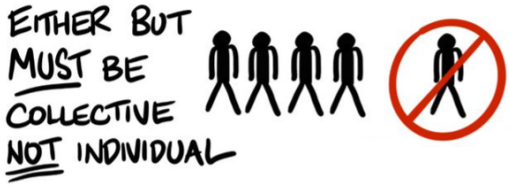




Framing the duty as an obligation

One option is to frame the duty as an obligation to not harm those who will be impacted by the decisions based on the data used. This would also help broaden the scope to the analysis of de-identified data which was raised earlier in this paper. This would be a collective approach which experts noted would likely be a better way to proceed but could face arguments within a law and economics space.

A collective duty could be seen by some as vague, and rogue organisations may take advantage of this to undermine a duty to the individual. Experts also noted that a collective "interests" duty is less commonly used in legislation. Most interest duties



place obligations on individuals to protect individuals (e.g., financial advisers and their clients or doctors and their patients).

There are limited examples of broad duties (e.g., in superannuation). To counter this, another option would be to place a positive obligation on businesses to 'do good' and use data to create opportunities for a better world.

Tiered approach to introducing fairness and safety as a business obligation

One approach could be to consider leading with implementation of specific best-interest or duty of care obligations to help reform how businesses think about how and what data they are collecting rather than litigating after a harm as occurred.

A tiered approach may help Government to change business conduct over time, first starting with a shift in mindset. This could be implemented in many ways:

- Limit the initial application of a best-interest framework or duty of care obligations towards their customers (i.e., individuals not businesses who may also be their customers) followed by introducing a broader framework of fairness and safety that embeds a collective duty.
- Limit the initial application to larger platforms, similar to how the duty in the Digital Services Act in the EU will only apply to Very Large Online Platforms (VLOP) and then broaden the scope to more businesses over time with support to implement the new mindset.
- Expand the current Australian Privacy Principles (APPs) to include best interest – with a clear indication of how this duty interacts with directors' duties.
- Incorporate best interest duty as part of a tort.
- Develop clear 'Guidance' or examples which are binding (i.e., when new conduct is identified, there needs to be a clear and effective way to add to an evolving blacklist). Any guidance, including a blacklist with examples will need to be carefully drafted to ensure best interests can still be broadly interpreted and enforced by the regulator.

One limitation with a tiered approach is the disparity it can create in the market. Creating a tiered approach or excluding specific types of businesses can continue to create loopholes for poor online practices to thrive. It also places the onus on consumers to navigate a complex market to determine which businesses are obligated to act in their best interest and which ones do not. This adds further burden on consumers who already feel overwhelmed when it comes to engaging online.[30]

A way to mitigate this issue, is to outline a detailed timeframe and process to how a tiered approach would be implemented, building in expectations upfront that the ultimate goal is for the entire market to eventually comply with the obligations. This form of a tiered approach is not new and can help a market to progressively reach a desired outcome for consumers. As an example, in 2019, the new mandatory product safety standard for quad bikes was introduced in two stages where the initial stage involved meeting specific standards, testing and labelling requirements. The second stage (effective one year later) then introduced obligations for protection devices and minimum stability requirements.[31] The transition to the mandatory standard was supported by various guidance for both dealers and manufacturers.[32]

Privacy safety regime

Safety at the heart of privacy

The privacy regulator needs new powers to keep consumers safe

We need our regulators to stop obviously harmful behaviour and practices before widespread harm occurs and to have the power to restrict likely harmful practices while investigations take place.

One way to achieve this could be via a concept CPRC has termed as a Privacy Safety Regime. Such a regime could mirror similar reforms introduced in the Australian financial markets such as the product intervention power and consider measures currently in Australia's product safety framework that are used to investigate emerging product safety hazards. Feedback from experts confirmed that a proactive approach to pause and assess data practices could effectively deal with new and emerging technologies and help drive positive change in business conduct to make safety a priority.

CPRC's research thus far has confirmed that Australian consumers strongly support further privacy protections. CPRC's 2020 research found that 74% of Australian consumers have safety concerns in relation to being targeted with particular products or services, 76% consider it to be unfair when their personal information is used to make predictions about them and 80% consider it is unfair for their personal information to impact what products they are eligible for.[33]

How do other regulators stop emerging harms?

Product intervention power

In 2018, the Federal Government introduced product intervention powers under the Australian Securities and Investment Commission's (ASIC) remit. This means that ASIC can place a temporary prohibition on a financial or credit product. It has enabled ASIC to make product intervention orders on financial products that are causing or at risk of causing consumer harm.[34]

As an example, in 2022, ASIC placed a product intervention order on short term credit and continuing credit contracts involving high fees to consumers for small amounts of credit.[35] This was an intervention that ASIC could implement independently to the Federal Government, meaning it could be brought into application within the market far sooner than it would have had it gone through the usual route of legislative review and change.

Unlike traditional enforcement where issues are investigated after harm has taken place, a product intervention power has meant ASIC can take a more proactive approach to market regulation. In its guidance documentation, ASIC notes the following powers that it now has as a regulator via the product intervention power:

> *"The power:*
>
> *(a) enables us to respond to problems in a flexible, targeted, effective and timely way*
>
> *(b) enables us to take action on a market-wide basis, and*
>
> *(c) is available without a demonstrated or suspected breach of the law, which enables us to take action before significant detriment, or further detriment, is done to consumers, so that we can better uphold community expectations on the conduct of firms that issue or distribute products".*[36]

A similar product intervention power also exists in the United Kingdom. The FCA has authority to make rules in the interest of "*consumer protection, competition and market integrity*".[37] Rules generally require public consultation before being introduced but in specific circumstances the FCA has power to make temporary product intervention rules (valid for up to 12 months) before undertaking consultation. FCA notes the following circumstances when a temporary product intervention rule can be made.

> *"Some of the instances in which the FCA might consider making temporary rules include:*
>
> - *where a product is in serious danger of being sold to the wrong customers, for instance where complex or niche products are sold to the mass market*
> - *where a non-essential feature of a product seems to be causing serious problems for consumers, and*
> - *where a product is inherently flawed".*[38]

In contrast, ASIC does not have the flexibility to impose product intervention orders of any kind without first undergoing public consultation.[39] While there may be perceived market risks when FCA introduces a temporary product intervention order without consultation, it does mean that a review of a product or service can be fast-tracked to limit consumer harm. It effectively pauses the conduct while the regulator conducts rigorous investigation and consultation ensuring that no further consumer harm takes place.

Interim and permanent product safety bans

Within the Australian Consumer Law under the *Competition and Consumer Act 2010*, the Commonwealth Minister and the respective state and territory fair trade or consumer protection Ministers can enforce an interim ban for products that have or are likely to cause injury.[40]

Unlike introducing a mandatory standard, which can involve a lengthy regulatory process, an interim ban can be imposed and be effective immediately for up to 60 days and extended to a further 60 days, if needed. Within this time period, the Australian Competition and Consumer Commission (ACCC) will assess the risk of consumer harm and, if required, it may recommend to the Commonwealth Minister to impose a permanent ban.[41] For example, in 2009, the Commonwealth Minister initially imposed an interim ban on sky lanterns due to these products posing a fire risk. Following the interim ban, the Commonwealth Minister issued a permanent ban on these products.

Sky lanterns, also known as flying paper lanterns, resemble miniature hot air balloons that lift into the atmosphere with the support of an open flame inside the lantern.[42] While no injuries or near-miss incidents had been reported in Australia, the imminent risk of fire due to Australia's drought-prone environment, was adequate to impose the ban.[43] Unlike a mandatory standard which involves significant evidence of harm either in Australia or overseas along with a detailed Regulatory Impact Statement, an interim ban can help bring safeguards to consumers immediately and help fast-track an assessment process towards more long-term measures.

One particular shortcoming of this framework that was explored by experts was its reliance on Ministerial intervention, even to introduce temporary restrictions. This can increase the likelihood of delay and can potentially politicise what would otherwise be an issue of consumer safety. If the Federal Government was to consider such a model for privacy, the regulator should have the independency to at least introduce an interim ban so measures to protect consumers can be implemented swiftly.

Considerations for a privacy safety regime in Australia

One of the key benefits of both the product intervention powers and product safety interim bans is their timeliness to deal with emerging and potential consumer harm. It also enables the regulators and Government to impose a pause on a practice or product while they proactively assess the risk. This ability to proactively intervene to stop emerging harm is currently missing from Australia's privacy regulations.

As an example, if a privacy safety regime was in place today, it would have meant that some uses of facial recognition technology could have been restricted immediately as the Office of the Australian Information Commissioner investigated its use by Bunnings, The Good Guys and Kmart.[44] Instead, we are relying on the good faith of businesses to stop using this controversial technology, many of which are placing commercial benefits of data harvesting over the safety and wellbeing of Australians.

Effective resourcing

Adequate resourcing or lack thereof can impact how an intervention, or a ban is developed and enforced. Experts noted that either framework can be resource intensive for regulators. Regulation costs can be high requiring the regulator to have both the capacity and capability at any given point in time when an issue is raised. Building evidence of harm may also prove difficult as there is a risk of capturing positive uses cases. Interventions or bans need to be broad enough to apply market-wide but focused enough to restrict the specific practices that are causing or likely to cause harm.

One possibility explored with experts to mitigate the resource constraint likely to be faced by a regulator, is for the Federal Government to consider an industry payment model by introducing levy penalties based on how much data is held by a business. This could encourage data minimisation as much of the harm is often derived from hoarding and transferring data. Another option would be to resource consumer organisations to assess and raise issues in a format similar to a super-complaint.[45]

Conclusion

Australia is at the cusp of delivering privacy protections that Australians need and deserve. Considering privacy protections as an opportunity to provide both care and safety to consumers enables Australia to foster a digital economy where consumers can thrive. It can become a digital economy that supports instead of manipulates consumer choice, builds trust instead of embedding opaqueness.

The ideas outlined in this paper show that safety and care are standards that consumers need businesses to meet and that could be practically developed as legal obligations.

Endnotes

[1] Nadler, A. and McGuigan, L., "An impulse to exploit: the behavioral turn in data-driven marketing", (2018), Critical Studies in Media Communication, 35:2, 151-165, https://doi.org/10.1080/15295036.2017.1387279

[2] Ben-David, R., "Energy consumers deserve a best interest duty", (June 2022), https://www.linkedin.com/pulse/energy-consumers-deserve-best-interest-duty-ron-ben-david.

[3] Romano Law, "Ready or Not New York, Privacy Here We Come: The Impending New York Privacy Act", (April 2021), https://www.romanolaw.com/2021/04/30/ready-or-not-new-york-privacy-here-we-come-the-impending-new-york-privacy-act.

[4] European Union, "Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", (Accessed 5 November 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014#d1e2731-1-1.

[5] UK Parliament, "Parliamentary Bills – Online Safety Bill", (Accessed: 2 March 2023), https://bills.parliament.uk/bills/3137 .

[6] Gelber, K., "A better way to regulate online hate speech: require social media companies to bear a duty of care to users", (14 July 2021), The Conversation, https://theconversation.com/a-better-way-to-regulate-online-hate-speech-require-social-media-companies-to-bear-a-duty-of-care-to-users-163808.

[7] Corporate Finance Institute, "Fiduciary Duty", (October 2022), https://corporatefinanceinstitute.com/resources/wealth-management/fiduciary-duty/.

[8] Tretina, K., "How Fiduciary Duty Impacts Financial Advisors", (15 July 2022), Forbes Advisor, https://www.forbes.com/advisor/investing/financial-advisor/what-is-fiduciary-duty.

[9] Cormican, L., "Super funds' fiduciary duty to participate in class actions", (July 2022), Super Review, https://superreview.moneymanagement.com.au/news/superannuation/super-funds-fiduciary-duty-participate-class-actions.

[10] Attorney-General's Department, "Privacy Act Review Report", (16 February 2023), https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[11] Ben-David, R., "Minimising consumer harm for a successful energy transition", (November 2022), https://www.linkedin.com/posts/ron-ben-david-753a7940_minimising-consumer-harm-in-the-energy-transition-ugcPost-6999951284657102849-JxAl/.

[12] Balkin, J.M., "The fiduciary model of privacy", (2020), Harvard Law Review Forum, 134:1, https://doi.org/10.1080/15295036.2017.1387279.

[13] Arora, C., "Digital health fiduciaries: protecting user privacy when sharing health data", (2019), 21, 181-196, https://link.springer.com/article/10.1007/s10676-019-09499-x.

[14] Balkin, J.M., "The fiduciary model of privacy", (2020), Harvard Law Review Forum, 134:1, https://doi.org/10.1080/15295036.2017.1387279.

[15] *Ibid.*

[16] CPRC, "Duped by Design – Manipulative online design: Dark patterns in Australia", (June 2022), https://cprc.org.au/dupedbydesign.

[17] Véliz, C., "The ethical case for data fiduciaries", (November 2020), Ada Lovelace Institute, https://www.adalovelaceinstitute.org/blog/ethical-case-for-data-fiduciaries/.

[18] European Union, "Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", (Accessed 5 November 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014#d1e2731-1-1.

[19] Pirkova, E., "The Digital Services Act: your guide to the EU's new content moderation rules", (July 2022), Access Now, https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/.

[20] Article 19, "EU: Due diligence obligations in the proposed Digital Services Act", (May 2021), https://www.article19.org/resources/eu-due-diligence-obligations-in-the-proposed-digital-services-act.

[21] Consumer Data Right, "What is CDR?" (Accessed 1 April 2022), https://www.cdr.gov.au/what-is-cdr.

[22] Australian Human Rights Commission, "Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias" (2020), https://tech.humanrights.gov.au/downloads.

[23] Broad, E., "Made by Humans", (2018), Melbourne University Press, Melbourne Australia.

[24] Davis, N., Perry, L. & Santow, E., "Facial Recognition Technology: Towards a model law", (2022), Human Technology Institute, The University of Technology Sydney, https://www.uts.edu.au/human-technology-institute/explore-our-work/facial-recognition-technology-towards-model-law.

[25] CPRC, "How Australia can stop unfair business practices", (September 2022), https://cprc.org.au/stopping-unfair-practices.

[26] Kemp, K., "Concealed data practices and competition law: why privacy matters", (5 November 2020), European Competition Journal, Volume 16, 2020 – Issue 2-3, https://doi.org/10.1080/17441056.2020.1839228.

[27] Financial Conduct Authority (UK), "A new Consumer Duty – Feedback to CP21/36 and final rules", (July 2022), https://www.fca.org.uk/publication/policy/ps22-9.pdf.

[28] *Ibid.*

[29] Financial Conduct Authority (UK), "Finalised Guidance - FG22/5 Final non-Handbook Guidance for firms on the Consumer Duty", (July 2022), https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf.

[30] CPRC, "The Digital Checkout", (December 2021), https://cprc.org.au/the-digital-checkout.

[31] ACCC, "Quad bikes", (Accessed 28 February 2023), Product Safety Australia, https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans/mandatory-standards/quad-bikes.

[32] ACCC, "Quad bikes", (Accessed 28 February 2023), Product Safety Australia, https://www.productsafety.gov.au/products/transport/quad-bikes#toc-related-publications.

[33] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.

[34] ASIC, "RG 272 Product intervention power", (June 2020), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-272-product-intervention-power/.

[35] ASIC, "19-250MR ASIC makes product intervention order banning short term lending model to protect consumers from predatory lending", (12 September 2019), https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-250mr-asic-makes-product-intervention-order-banning-short-term-lending-model-to-protect-consumers-from-predatory-lending.

[36] ASIC, "RG 272 Product intervention power", (June 2020), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-272-product-intervention-power/.

[37] Mathieson, M. and McLennan, M. "What do the product intervention powers of the UK financial conduct regulator look like?", (September 2014), Allens, https://www.allens.com.au/insights-news/insights/2014/09/unravelled-what-do-the-product-intervention-powers-of-the-uk.

[38] Financial Conduct Authority (UK), "FSA confirms approach to using temporary product intervention rules that will be used by the FCA", (25 March 2013), https://www.fca.org.uk/news/press-releases/fsa-confirms-approach-using-temporary-product-intervention-rules-will-be-used.

[39] ASIC, "RG 272 Product intervention power", (June 2020), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-272-product-intervention-power/.

[40] ACCC, "About product bans", (Accessed 10 November 2022), Product Safety Australia website, https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans/product-bans/about-product-bans.

[41] *Ibid.*

[42] ACCC, "Product bans – Sky lanterns" (Accessed 10 November 2022), Product Safety Australia website, https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans/product-bans/sky-lanterns.

[43] Australian Government, "Explanatory Statement – Consumer Protection Notice No. 17 of 2011 – Permanent ban on sky lanterns" (Accessed 10 November 2022), https://www.legislation.gov.au/Details/F2011L00227/Explanatory%20Statement/Text.

[44] Pereira, A., "Complaint to OAIC on use of facial recognition in retail stores", (June 2022), CHOICE, https://www.choice.com.au/consumer-advocacy/policy-submissions/2022/june/complaint-oaic-on-use-of-facial-recognition.

[45] Office of Fair Trading (United Kingdom), "Super-complaints – Guidance for designated consumer bodies", (July 2003), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/284441/oft514.pdf.