Consumer Policy Research Centre

Level 6, 179 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

7 November 2022

Submission – Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Submitted via: https://www.aph.gov.au/Parliamentary_Business/Committees/OnlineSubmission

The Consumer Policy Research Centre (CPRC) generally supports the proposed amendments in *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*. Setting penalties at the right level will ensure that more businesses will seriously consider effective strategies to reduce the risk of data breaches. We are also pleased to note that the explanatory statement recognises the emotional harm that people can experience due to loss of their personal information.

However, the proposed legislation is still limited in its scope and remains far from the privacy protections that Australians deserve and that consumers in other comparative jurisdictions have enjoyed for several years. In particular, CPRC asks the Federal Government to:

- amend the legislation so the regulator can consider penalties for all data breaches, not just when incidents are serious or repeated
- commission an independent review of the regulator to ensure it is adequately resourced to enforce these penalties, including undertaking proactive surveillance
- ensure the ongoing review of the Privacy Act includes safeguards on how data is collected, shared, and used by businesses.

Failure to protect consumers will mean Australians will continue to navigate a digital economy that:

- collects, shares, and uses data to make predictions about consumers in ways that can leave them worse off
- uses and aggregates data to unfairly exclude consumers from accessing certain products and services
- targets consumers to expose their vulnerabilities for commercially beneficial outcomes
- fosters little transparency on what consumers are presented, what they consume and at what price
- lacks adequate support for consumers seeking redress from data-related harms.

CPRC is an independent, not-for-profit consumer research organisation. Our mission is to improve the lives and welfare of consumers by producing evidence-based research that drives policy and practice change. Digital issues are a research focus for CPRC, including emerging risks and harms and opportunities to better use data and technology to improve consumer wellbeing.

We would welcome the opportunity to work with the Federal Government and share further insights from our consumer research.

Yours sincerely

Chandni Gupta
Digital Policy Director
Consumer Policy Research Centre

Limiting penalties to repeated breaches limits protections for Australians

CPRC recommends that the Privacy Act be amended to remove the reference to "serious and repeated interferences" in the legislation (*Clause 13G of PARTIII*). Any data breach can lead to significant loss of personal information and consumer harm may be cumulative over time. As the Optus, Medibank and now Harcourts data breach have shown, Australians whose data has been hacked have had to bear the significant inconvenience and negative consequences of these incidences. Applying penalties to only serious or repeated breaches creates a regulatory loophole for businesses to evade accountability.

In our research into international laws on unfair business practices, our discussions with consumer advocates from both Europe and the United States noted the harms that come from the lack of breaches that result in penalties.[1] One of the key reasons is how the application of penalties is outlined in legislation. For example, in the United States, the Federal Trade Commission is unable to seek penalties for "first-time" breaches on unfair business practices. This means that there is little incentive for businesses to 'get things right first time, every time'. We have an opportunity to learn from other jurisdictions and ensure businesses are held accountable for data that Australians have entrusted them to keep safe.

Increased penalties must be backed by proactive enforcement and practical redress

Increasing penalties is one step, ensuring they can be adequately enforced is another. The regulator must be empowered to undertake proactive investigations before widespread harm has taken place. The Federal Government must ensure that the regulator – the Office of the Australian Information Commissioner (OAIC) – is adequately resourced to monitor and enforce privacy breaches. CPRC urges the Federal Government to conduct an independent review of the regulator, comparing its resourcing with that of other Australian regulators and comparative international regulators. The aim of the review should be to ensure the regulator is well-supported by Government and has the capacity and capability to enforce privacy protections in our current and future, fast-paced digital economy.

Currently, regulators largely rely on reports from consumers, identifying harm after it takes place. This is not sustainable in a digital environment where harms are difficult for individual consumers to identify and harm often occurs at a community or collective level. Instead, regulators need to proactively uncover harm that is currently obfuscated. Regulators should have the ability to push businesses to be radically more transparent about how they use consumer data.

Monitoring and surveillance of the market needs a diverse workforce that understands the technology used by businesses. Experts such as data scientists, artificial intelligence engineers, information security analysts and other technical professionals need to be in the mix to support upstream regulation and mitigate current and foreseeable risks to consumers.

In terms of effective redress, the Federal Government must consider a holistic approach to dispute resolution. This could be via the establishment of a Digital Ombudsman – a one-stop-shop where consumers can access support across all facets of a digital experience.[2]

Penalties are only the beginning – Australians deserve better privacy protections

Unlike other jurisdictions where privacy laws are being regularly updated, Australian laws pre-date not only the current digital economy but digital technology itself. Issues of safety and fairness cannot be regulated using consumer choice. Instead, consumers need the privacy law to:

- stop harmful business practices, allowing regulators to ban or restrict data practices that cause direct and clear consumer harms
- modernise the definition of "identifiable data" to recognise how data can now be used to target people

[1] CPRC, "How Australia can stop unfair business practices", (September 2022), https://cprc.org.au/stopping-unfair-practices/.
[2] See section on 'Ensuring redress' in CPRC's Digital Checkout report available at: https://cprc.org.au/the-digital-checkout/.

- require more effort on the part of businesses to assess whether how they collect and use data results in fair outcomes for their customers.

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 but bear the consequences potentially for the remainder of their life is not a fair trade. At minimum, any reform to the Privacy Act should prioritise protections that go beyond notifying consumers how data will be used or seeking individual consent.

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.[3]

Too often consumers are asked to consent to data collection in ways that involve no meaningful explanation of what is being done with their data and no meaningful way to control how data is used. The Privacy Act must be updated to make sure notification and consent works for consumers and is used appropriately by businesses.

Only 12% of consumers feel that they have a clear understanding on how their personal information is collected and shared in a digital economy.[4] Consumers are expected to read and understand terms and conditions that no reasonable person can easily navigate. The responsibility for translating and explaining needs to be placed back onto the businesses that have benefited from the information asymmetry that currently exists, especially online.

Any notification and consent framework must also be built on pro-privacy defaults. For example, consent to accept cookies should be defaulted to the minimum required for essential website navigation rather than the current situation where people are asked to accept all by default.[5]

[3] Findings from CPRC's 2020 Data and Technology Consumer Survey is available at: https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/.
[4] *Ibid*.
[5] CPRC's research on dark patterns revealed examples where consumers are simply being notified that by using the website and therefore were consenting to all cookies by default: https://cprc.org.au/dupedbydesign/.