Australian Government
The Treasury

DATA STANDARDS BODY

Consumer Experience Working Group

Noting Paper 359: Deceptive Patterns Health Check | Next Steps

Contact: *Michael Palmyre*

Publish Date: *1 November 2024*

Context

Deceptive patterns (AKA dark patterns)[1] have been raised as a risk to the Consumer Data Right (CDR) for several years. The Data Standards Chair engaged the Consumer Policy Research Centre (CPRC) to extend standards consultation into the community sector, which produced four reports from late 2020 to early 2022. This work identified that while implicitly discouraged, deceptive patterns are not explicitly prohibited in the CDR. A recommendation was made to explore the viability of specific consumer experience (CX) data standards to protect consumers against the risks of deceptive patterns.

In collaboration with the Treasury, the DSB conducted two consultations on deceptive patterns as part of the consent review, which included Noting Paper 273 in late 2022 and Design Paper 321 in late 2023. These consultations included examples of deceptive patterns and hypotheses considering how they might manifest in the CDR ecosystem. All submissions on deceptive patterns supported further work on the topic, with around 90% supporting deceptive pattern prohibitions through the CX standards. The prevailing view was that principles-based requirements should be supported by prescriptive detail, where stakeholders supported the use of CX guidelines to provide clear examples.

The recently concluded consultations on draft rules and data standards did not contain proposals on deceptive patterns. While the rules already provide scope for standards to be made on this topic, these proposals were omitted to allow further analysis to be conducted on the appropriateness and form of any such standards.

[1] Deceptive patterns can be defined as practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade users to engage in unwanted behaviours or into undesired decisions which have negative consequences for them. *(2022) Regulation (EU) 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)*

Deceptive Patterns Pressure Test

The DSB engaged the University of South Australia (UniSA) to progress this analysis, which has produced two reports: a landscape review of deceptive patterns (see: NP355), and the recently published *Deceptive Patterns Pressure Test*. The purpose of this engagement was to better understand deceptive patterns in use and how the CDR may be vulnerable to them.

UniSA's findings suggested that the CDR is protective against a range of deceptive patterns, particularly including the most nefarious patterns, but noted that many of these protections are optional guidelines that participants are not required to follow.

UniSA's analysis identified key areas of concern, including how:

- metadata acquired through the CDR may be used to target CDR consumers using deceptive patterns outside of the CDR
- subtle design choices may be CDR compliant but still manipulate consumer behaviour
- CDR participants may use knowledge of a consumer's CDR arrangements, such as when an authorisation is due to expire, to manipulate the consumer's decision to renew their consent to the ADR.

This work was focused on mapping written statements, as opposed to analysing visual manifestations of deceptive patterns in the context of live CDR participant flows.

Regulatory Landscape

A number of jurisdictions have progressed prohibitions against deceptive patterns, including the European Data Protection Board and a range of interventions in the United States, such as the California Consumer Privacy Act and the Biden Government's recent 'Time is Money' initiative. In Australia, work being progressed in response to the risks posed by deceptive patterns include the Treasury's consultation on unfair trading practices, the Attorney-General's Department's Privacy Act Review, the ACCC's Digital Platform Services Inquiry, and the OAIC's Global Privacy Enforcement Network (GPEN) Sweep. The work by the OAIC, for example, found that almost all of the >1000 websites and mobile applications they examined used a range of deceptive patterns.

However, UniSA and consumer advocates have suggested that existing and emerging regulations in Australia may still lack sufficient focus and enforcement capabilities to appropriately address the risk of deceptive patterns, including in the CDR. Further, it has been suggested that the timing and focus of any emerging regulations relating to deceptive patterns in Australia is unclear.

The Albanese Government's media release on Wednesday 16 October outlined key actions it will take to ban unfair trading practices under Australian Consumer Law. These actions will address practices that include deceptive and manipulative online practices, which the Treasury would consult on before legislating a general prohibition.

Next Steps

Following the publication of UniSA's second report, the DSB suggests further analysis is necessary to understand where compliant design patterns have the effect of subverting or impairing a genuine choice, such as to withdraw consent, authenticate, give an authorisation, or provide consent in an informed way.

This analysis is particularly important where further simplifications to the consent model may be considered in support of a 'CDR reset'. Such a focus will help the program understand where changes may introduce deceptive pattern risks, including those captured by any general prohibition on unfair trading practices to ensure alignment. The findings of this work can also be relayed beyond the CDR to inform broader regulatory direction.

To support this work, the DSB will conduct further analysis to understand where compliant design patterns may in practice undermine meaningful consumer choice, control, and consent management mechanisms. This will include activities to 'hack' the CDR, where a range of deceptive patterns will be designed in the context of the CDR consent model to assess where CDR protections do, or do not, prohibit them. These will draw from UniSA's typology input from consumer advocates and community members, and practices identified as part of the unfair trading practices analysis. The initial focus will be on patterns relating to information asymmetry and free choice repression in consent, authentication, authorisation, and dashboards.

Preliminary analysis by the DSB suggests that the CDR requirements which UniSA's findings identified as affording some protection may still allow a range of deceptive patterns to exist. The DSB will assess the risk and impact of any deceptive patterns that this work identifies, and if they are indeed prohibited by CDR protections and any general prohibition on unfair trading practices.