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

# Submission to the ACCC on the Digital Platform Services Inquiry on social media services – Issues Paper

15 September 2022

Kate Reader and Morag Bond
General Managers
Digital Platforms Branch
Australian Competition and Consumer Commission

**By email:** digitalmonitoring@accc.gov.au

Dear Ms Reader and Ms Bond

The Consumer Policy Research Centre (CPRC) is pleased to see the ACCC consider the impacts of social media services on Australian consumers as part of its digital platform services inquiry.

Entities that profit from social media need to have adequate obligations and expectations placed on them, given the significant use of social media by Australian consumers. Our research into dark patterns (also known as deceptive and manipulative designs) identified **social media platforms as one of the top five sectors where consumers experience dark patterns** (Attachment 1).[1]

Our research found 83% of Australians have experienced negative consequences as a result of dark patterns that are aimed at influencing their behaviour. Australians have lost money, lost control of their data or have been manipulated by a business to make a choice that was not in their interest. Social media is a sector that is attributing to these harms.

CPRC is a not-for-profit consumer policy think tank. Our role is to investigate the impacts that markets and policies have on Australian consumers and advise on best practice solutions. Consumer protections in the digital world is a current research focus for CPRC.

Our submission uses insights from our research and considers the questions raised in the issues paper using three key principles – fairness, safety and inclusivity for consumers engaging in the digital economy.

We would welcome the opportunity to work with the ACCC and share further insights from our consumer research projects. For further discussion regarding our research and the contents of this submission, please contact chandni.gupta@cprc.org.au.

Yours sincerely

Chandni Gupta
Digital Policy Director
**Consumer Policy Research Centre**

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

Question 26: Are consumers spending less or more time engaging with social media platforms? Has the COVID-19 pandemic and associated lockdowns had an impact on consumer engagement? Are any trends in consumer engagement on social media that emerged during the COVID-19 pandemic likely to continue?

Our research more generally on the rise of the 'Digital Checkout' identified the continued increase in consumers participating in the digital economy. This substantially increased in scale and scope during the COVID-19 restrictions.[2]

As part of our recent research into dark patterns, released in June 2022, we identified that **90% of Australians use social media** with **71% using it at least once a day**. When it comes to younger cohorts, 89% of young Australians aged between 18 and 28 years use social media at least once a day. In our research, younger consumers were identified to be more negatively impacted by dark patterns (Figure 1). As an example, younger consumers were 65% more likely than the national average to spend more than they intended and 34% more likely to accidentally sign up to something.[3]


Figure 1: Impact of dark patterns on younger consumers aged 18-28 years | Source: Duped by Design, CPRC: https://cprc.org.au/dupedbydesign

Given the frequent use of social media by younger Australians and dark patterns being highly prevalent on social media, the likelihood of harm to these consumers is significantly high.

Question 29: Are consumers faced with potentially misleading and/or deceptive claims through advertising on social media (including sponsored advertising or posts featuring influencers)? If so, has the incidence of potentially misleading and/or deceptive claims increased or decreased over time?

It is highly likely that consumers see misleading and deceptive claims through social media, some of which would be through disguised and hyper-personalised advertising.

**Disguised advertising**

Disguised advertising is when format, wording and design of the content mirrors regular content on a website or app with insufficient disclosure for consumers to distinguish it as an advertisement. Our survey into dark patterns revealed that 85% of Australians had recalled seeing online content they

[2] CPRC, "The Digital Checkout", (December 2021), https://cprc.org.au/the-digital-checkout/.
[3] CPRC, "Duped by Design – Manipulative online design: Dark patterns in Australia", (June 2022), https://cprc.org.au/dupedbydesign.

found difficult to determine if it was content that was part of the site or an advertisement. Close to half (45%) found it annoying while one in three (33%) found it deceptive. More than one in four (28%) found that advertisements disguised as content made the website or app more confusing.[4]

The prevalence of disguised advertising in social media is likely to be significant as there are no clear markers for declaring partnerships. While some social media platforms require branded content to be signified with "paid partnership" labels, the scope of how that applies is limited to what is being marketed in a specific social media post.[5] The nature of social media posts further blurs the line between content that is organic and content that an influencer may be benefitting from directly or indirectly. As an example, a social media influencer can showcase a variety of products from a particular brand or store that they may have purchased themselves. However, it is likely that they are also promoting other products (not mentioned in the posts) sold by the same brand or store (Figures 2 and 3). In this scenario, it is unlikely that a paid partnership label would be required by the platform, even though the influencer is benefitting more generally from promoting products from a specific brand or store.

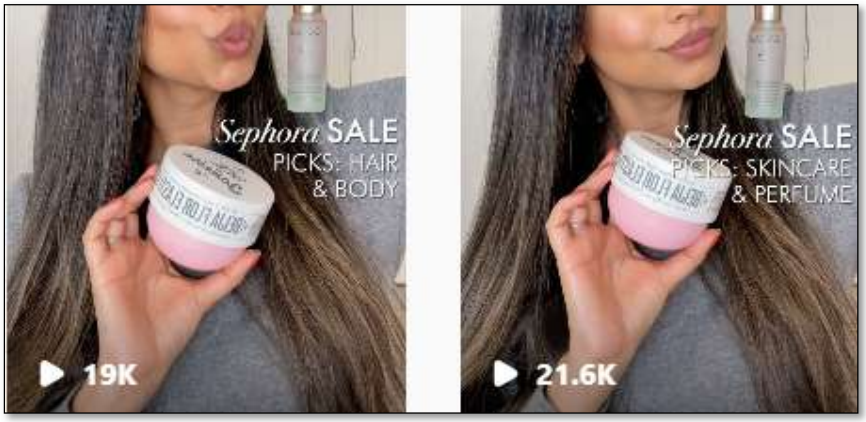



Figure 2: Influencer's reels on Instagram on specific products to purchase during a Sephora sale – no mention of any affiliation with Sephora (Screenshots captured on 14 September 2022 at 11 AM)


Figure 3: Ability to purchase a range of products (many available at Sephora exclusively) via the same influencer's website with direct affiliated links to Sephora (Screenshots captured on 14 September 2022 at 11:10 AM)

While the Australian Consumer Law covers misleading and deceptive conduct, including false and misleading claims, how that applies to social media influencers is unclear. Also, Australians are not just consuming content from Australian influencers but also overseas influencers, including the example

[4] *Ibid.*
[5] Instagram, "How to use the paid partnership label to tag branded content on Instagram", (Accessed 13 September 2022), https://help.instagram.com/1109894795810258.

above. There are inherent challenges in enforcing Australian laws on overseas entities. Currently there are only high-level guidelines by the International Consumer Protection and Enforcement Network (ICPEN) which encourage digital influencers to, "*be open about other commercial relationship that might be relevant to the content*".[6]

**Hyper-personalised advertising**

Another aspect to social media is its capacity to implement hyper-personalised advertising using personal information that is collected, shared and used by these platforms. Hyper-personalised advertising lacks transparency and has a greater ability for discrimination with harms obfuscated from consumers, researchers and regulators.

CPRC's 2020 Data and Technology Consumer Survey revealed that 94% of Australian consumers do not feel comfortable with how their personal information is collected and shared online. The research further reveals consumer discontent with tactics such as ad targeting, personalised price discrimination and exclusion from products and services:

- 92% agree that companies should only collect information they need for providing their product / service.
- 60% of Australians consider it very or somewhat unacceptable for their online behaviour to be monitored for targeted ads and offers.
- 90% believed it is unacceptable to charge people different prices based on past purchase, online browsing, and payment behaviours.[7]

While in Australia, traditional media such as radio and television have strict rules for ensuring there is a clear delineation between content and advertisements, in the online world the line between ads and content is blurred. Online presence of entities should be in line with the same obligations as they would be expected to meet across other mediums. Advertising content online should not be treated differently to other mediums.

Question 31: What is the process for consumers and business users to report potentially misleading and/or deceptive claims in advertising on social media, and what role do social media platforms play in these processes? How effective are these processes?

Across several research pieces and submissions, CPRC has continued to raise issues with the lack of accessible dispute resolution for consumers across markets within the digital economy. When consumers are unable to resolve issues directly with an essential service like an energy provider or telecommunications company, they have access to independent support for redress through an ombudsman. However, in the case of redress relating to an online experience, this support is out of reach. Consumers are frequently left to navigate any form of recourse themselves or simply give-up.[8]

There must be effective dispute resolution pathways to enable consumers to seek redress for when things go wrong in the online space. CPRC strongly recommends that Government finalise and release a scoping study as a matter of priority to identify the types of online disputes consumers are raising along with options for establishing more effective external dispute resolution pathways that not only address digital issues today but also complex matters that are likely to arise in the future. As mentioned in previous CPRC submissions, we believe there may be merit in a more holistic approach to dispute resolution, such as via the establishment of a Digital Ombudsman that can provide support on all facets of a digital experience, beyond digital platforms.

[6] ICPEN, "Online Reviews and Endorsements – ICPEN Guidelines for Digital Influencers", (June 2016), https://icpen.org/sites/default/files/2017-06/ICPEN-ORE-Guidelines%20for%20Digital%20Influencers-JUN2016.pdf.
[7] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey.
[8] *Ibid*.

## Attachment 1

**CPRC Report**

# Duped by Design – Manipulative online design: Dark patterns in Australia

# DUPED BY DESIGN

## Manipulative online design: Dark patterns in Australia

Consumer Policy Research Centre

The Consumer Policy Research Centre (CPRC) is an independent, non-profit, consumer think-tank established by the Victorian Government in 2016.

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

**Acknowledgements**
Data collection was conducted by CPRC, using Ipsos' Digital Platform. Terms and Conditions of Ipsos' Digital Platform can be found here: www.ipsos.digital/terms-and-conditions

**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
Level 14, 10-16 Queen Street
Melbourne Victoria 3000
cprc.org.au

Consumer Policy Research Centre, *Duped by design - Manipulative online design: Dark patterns in Australia*, June 2022.

Images: Facu Montanaro - Unsplash, Jeremy Bezanger - Unsplash
Design: Erin Farrugia

# Contents

# Introduction

Whole industries now exist to "hack" marketing funnels. Teams of experts experiment to get that extra person to subscribe or to add one more thing to the cart. We need to step back and ask, at what point is this push in web design misleading or manipulative to the user?

This report looks at what current trends in web and app design mean for consumers. We have found that Australian consumers are having their choices and experience manipulated through online designs known as dark patterns.

Dark patterns are design features and functionalities built into the user interface of websites and apps that purely exist to influence consumer behaviour – often not in the consumer's best interest.

This report looks closely at ten dark patterns common in Australia today, ranging from those that are ubiquitous and frustrating for consumers to those that are possibly misleading and deceptive and can lead to significant consumer harm.

This report will:

- provide an overview of the ten dark patterns that are prevalent for Australian consumers
- present the Australian consumer experience of dark patterns
- outline what next steps could look like, including actions businesses, regulators and government can take in addressing and mitigating consumer harm.

Some of the deceptive designs we found are so misleading that CPRC will be referring them to the relevant regulator for investigation for breaches of the Australian Consumer Law. The report includes examples of highly misleading designs such as extra services being added automatically into the cart (e.g. service plans for whitegoods) and convoluted app navigation that make the unsubscribing process long and confusing for consumers.

These deceptive techniques deteriorate a consumer's experience in the digital economy. Our survey found that 83% of Australians experienced one or more negative consequences, like financial harm or a feeling of being manipulated, as a result of a website or app using design features aimed at influencing their behaviour. Dark patterns have led one in four Australians to share more personal information than they wanted to and one in five to spend more than they intended.

For many of the dark patterns covered in this report, Australia's consumer protection laws do not go far enough to protect consumers. The onus must be put back on businesses to mitigate harm by presenting choices that are meaningful for and in the interest of consumers.

Jurisdictions worldwide are taking action on dark patterns. The introduction of the General Data Protection Regulation (GDPR) in 2018, while not perfect, provided European consumers with privacy protections far superior to those available for Australian consumers. Also, the European Union recently updated its directive on unfair commercial practices to include obligations relating to data-driven personalisation and dark patterns. In the United States, the state of California strengthened its Privacy Act by introducing a ban on specific dark patterns.

The Australian Government must fast-track a review of the *Competition and Consumer Act*, including the Australian Consumer Law (ACL) to make sure that consumer problems in the digital era are adequately captured by our laws.

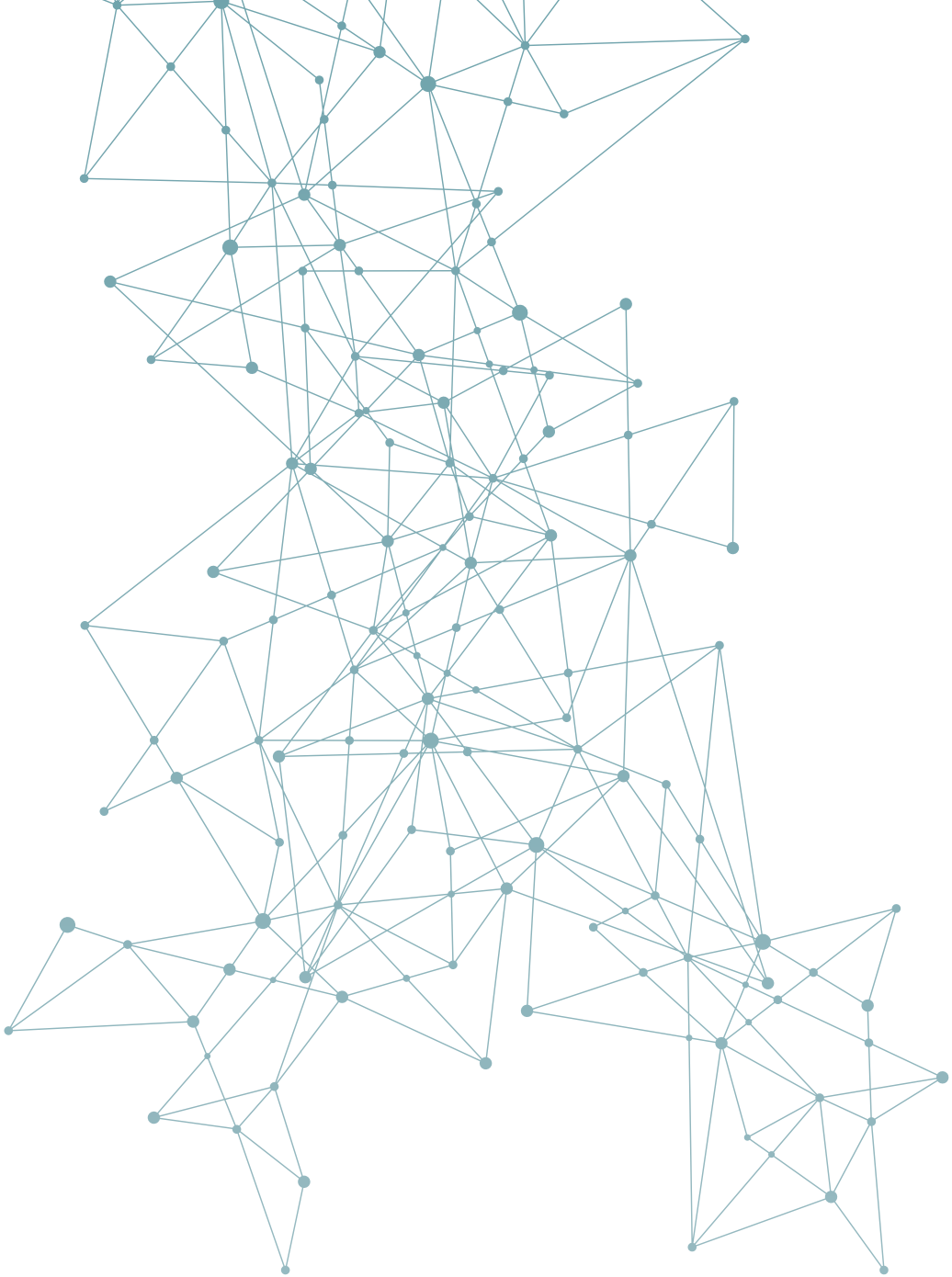
In addition, wider whole of economy reforms are needed to adequately protect consumers including:

- introducing an unfair trading prohibition
- strengthening unfair contract terms provisions
- reforming the Privacy Act to give consumers more control and agency over their data.

Regulators have an opportunity to reimagine their traditional enforcement models and move away from the “whack-a-mole” approach that places the onus on consumers to identify and report harms. Australian regulators need to be well-resourced for proactive surveillance and enforcement initiatives to deal with digital harms that are difficult for an individual consumer to identify.

While law and enforcement catch-up, businesses can make significant changes to their practices right now to ensure their online presence places the needs and experience of consumers above profit margins. Businesses can conduct regular audits of their website design, undertake regular consumer-centric user experience testing to test their designs and pivot towards design choices that enhance the consumer experience instead of deteriorate it. Our survey revealed that 30% of Australians stopped using the website/app (either temporarily or permanently) as a result of dark patterns and one in six Australians felt their trust in the organisation undermined. In the long-term it makes good business sense to give consumers an online experience that is in their best interest.

It will require a collective effort to turn the tide away from a digital economy that preys and profits on people’s vulnerabilities. However, it can be achieved if all involved in the ecosystem play their part in creating a digital economy that is fair, safe and inclusive for Australian consumers.



# Methodology

This report outlines key findings from a nationally representative survey of 2,000 Australians, exploring the prevalence and impact of dark patterns in Australia. It draws on consumer research conducted by UK consumer advocacy agency Which?.[1] We thank the Which? Team for their advice and support for this work.

CPRC's survey was conducted between 21 and 27 April 2022. Data collection was conducted by CPRC, using Ipsos' Digital Platform.[2] To achieve a nationally represented sample, quotas were set on each of the three demographic variables of age group, gender, state/territory.

In addition to the consumer survey, CPRC also conducted a randomised sweep of various websites and apps to identify specific dark patterns which Australian consumers are being exposed to. Various examples have been cited throughout this report. Where the practice is widespread in a sector or is likely built into the user interface of an off-the-shelf e-commerce solution, only de-identified examples are shown. However, this report identifies certain businesses where a:

- dark pattern has been identified as manipulative or deceptive in the consumer survey
- dark pattern was present on the website/app of a large business (i.e. not a small Australian business), and
- business was named by participants in the consumer survey as an entity that embeds dark patterns on its website/app.

# Key findings from CPRC's dark pattern research

**83%**

of Australians have experienced one or more negative consequences as a result of a website or app using design features aimed at influencing their behaviour

**58%**

of Australians are aware that organisations use specific types of design features to try and influence them to behave in a certain way

**18 to 28 years**

Younger consumers (aged 18 to 28 years) were more likely to be negatively impacted by dark patterns than any other age group

Younger consumers were

**65% more likely**

to spend more than they intended to as a result of dark patterns

"Manipulative" or "Deceptive" were in the top three responses to 9 out of the 10 dark patterns tested with Australian consumers

Dark patterns led to 1 in 4 Australians sharing more personal information than they wanted to

**30%**

of Australians stopped using the website or app (either temporarily or permanently) as a result of dark patterns used by the business

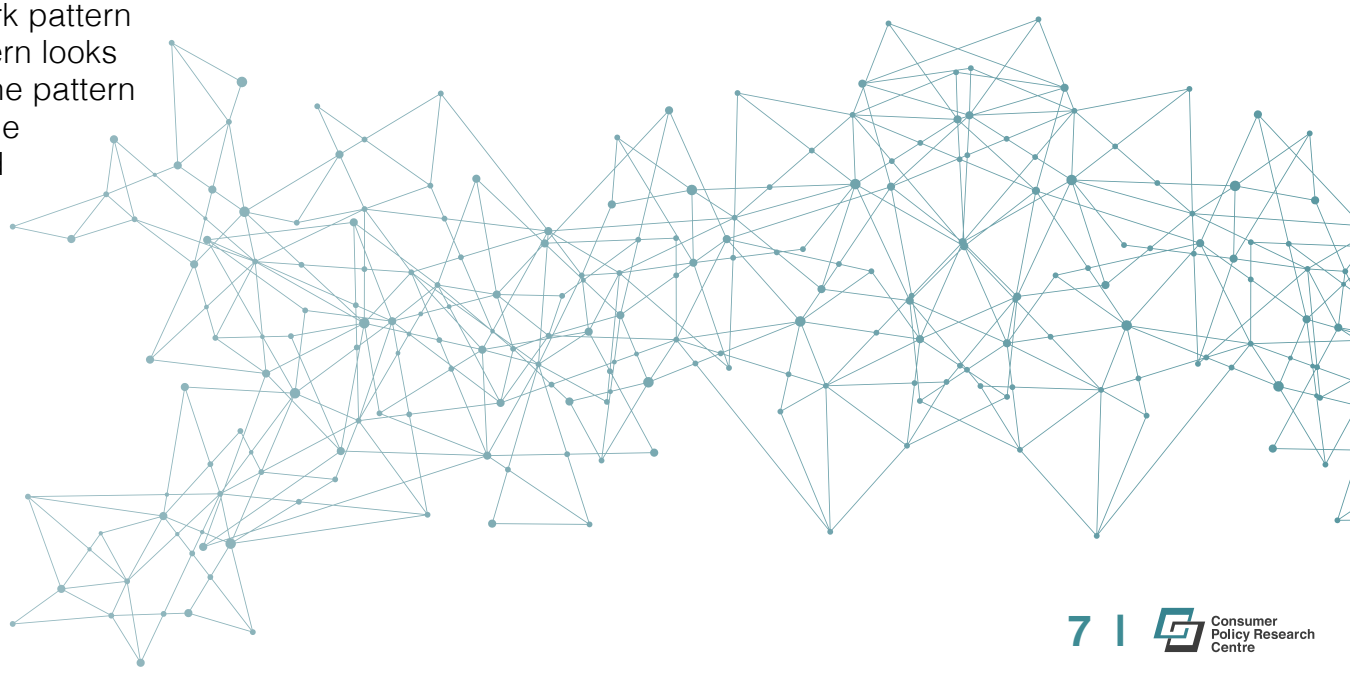
# What are dark patterns and where are they?

Up until the last decade, user interface design principles for websites and apps have largely hinged on providing a seamless and user-centric experience to consumers. A key objective of a user interface is to enable people to undertake the task they intended to do as efficiently as possible.[3] Dark patterns operate completely contrary to these principles by focusing on designs that deliver profit over user needs. A widely used practice now, dark patterns use a mix of cognitive biases and information asymmetry to influence consumers in making decisions that they otherwise would not have intended to make.[4] Dark patterns have now become increasingly prevalent across online platforms and shopping websites.[5]

This section first maps the possible spectrum of harm of dark patterns – identifying which patterns may breach current consumer protections and where our protections are not going far enough. The report then explores each dark pattern in detail, providing examples of what the pattern looks like in practice, the consumer experience of the pattern and nature of harms caused to consumers. The extent of harm indicates whether the threshold should be reviewed or reconsidered to provide adequate protection to consumers participating in the digital economy.

Ten dark patterns are explored in this report:

1. Hidden costs
2. Disguised advertisements
3. Trick question
4. Scarcity cues
5. Activity notifications
6. Confirmshaming
7. Hotel California (forced continuity)
8. False hierarchy
9. Redirection or nagging
10. Data grab



Our survey invited consumers to name businesses that they feel use dark patterns on their websites and apps. Over 1,200 eligible responses were received from 1,020 survey participants. Businesses from almost every sector were identified (Figures 1 and 2). The top five categories included:

1. clothing and accessories
2. online marketplaces
3. tech products and services
4. social media
5. department stores.


**Figure 1:** Sectors that utilise dark patterns as identified by business names provided by survey participants.

The top ten businesses that consumers identified as using dark patterns included:

- ebay
- Facebook
- The Iconic
- Catch.com.au
- Shein
- Instagram
- JB Hi-Fi
- Aliexpress
- Kogan.
- Amazon


**Figure 2:** Snapshot of businesses identified by survey participants as using dark patterns on their websites and/or apps.

## Spectrum of harm

At first glance, dark patterns can appear as innocuous annoyances that may just be our "way of life" online – a blip that consumers have to navigate as part of participating in the digital economy. However at the other end of the spectrum, dark patterns, can cause direct harm to consumers and breach consumer protections such as:

- misleading or deceptive conduct under the Australian Consumer Law (ACL) which aims to protect consumers from business practices that can create a misleading or deceptive impression about a product or service, including its price, value or quality[6]

- unfair contract terms under the ACL that aims to protect consumers where there is limited opportunity to negotiate with a business and where a term may pose significant imbalance, detriment or there is a lack of transparency[7]

- privacy protections under the Privacy Act 1988 which aims to protect the privacy of personal information of individuals.[8]

Many of the dark patterns we observed in our sweep of Australian websites involved credence claims: statements made by a company that cannot be easily verified by the customer.

Claims like 'five people are looking at this right now' may be accurate but, depending on how they are determined, they could also be misleading. This is a category of dark patterns that needs regulatory attention to determine if falsehoods could be driving claims online – consumers cannot check these for themselves. In these cases regulators will need to use proactive surveillance to uncover and test credence claims.

Some dark patterns cause consumer harm but are not well-captured by current legal or regulatory protections. Many of the dark patterns we identified can be considered unfair: they involve a business taking advantage of its relative power to influence consumers. Some of these unfair practices have potential to cause financial or significant consumer harms. For example, "Hotel California" or forced continuity designs likely lead to fewer people cancelling subscription services they wish to end. Many of these practices could be captured by an "unfair practices prohibition" that CPRC and other consumer advocates have argued is a necessary addition to the ACL.[9]

While experiences within some of these categories may not be adequately addressed under the current consumer protection framework, the ubiquitous presence of such dark patterns has the potential to erode consumer trust and impede consumer's experience on digital platforms, specifically for people who may be experiencing vulnerability.[10] Figure 3 maps the ten dark patterns across a spectrum of harm.

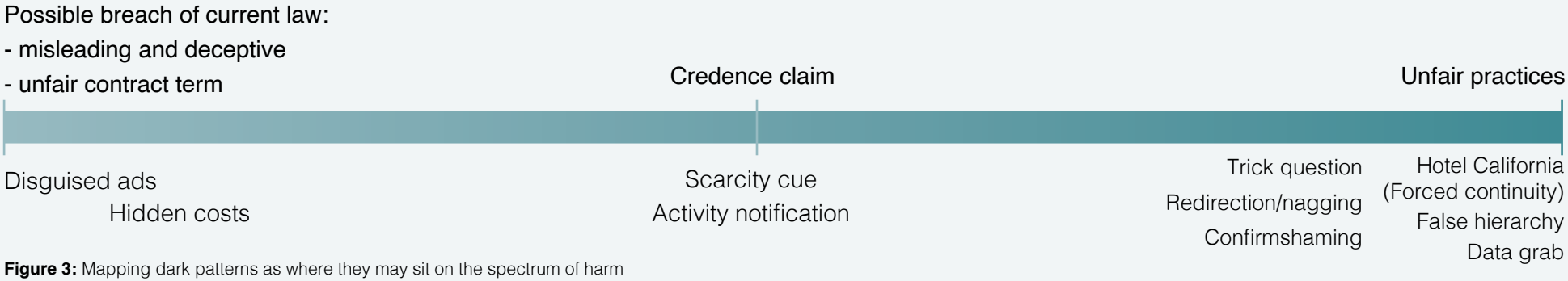



**Figure 3:** Mapping dark patterns as where they may sit on the spectrum of harm

## Hidden costs

This occurs when consumers are unaware of additional costs or are forced to pay more for a product or service than they initially perceived. Often this occurs via pre-selected add-ons that are embedded close to or at the final stage payment. This can include shipping and other costs that are not made clear upfront. It can also include pre-selected add-ons such as insurance or service plans that are either automatically added to a shopping cart by default or presented in a way that heavily implies the need to purchase. Consumers have to actively "untick", "opt-out" or navigate through a variety of options to avoid the extra cost.

This dark pattern is one that is most likely to cause direct financial harm to consumers and result in a company breaching the ACL.

### What does it look like?

Figure 4 shows an example from Appliances Online, an online home appliances retailer, which automatically adds a three-year care plan into the cart upon adding a product to a shopping cart. To further disguise the inclusion of this additional cost, the number of items displayed next to the cart icon equates only to the number of products added by the customer and the addition of the service plan is only visible once the shopping cart page is open, just prior to a customer making payment. The onus is on its customers to "opt-out" of the plan by actively removing it from their cart prior to finalising payment.

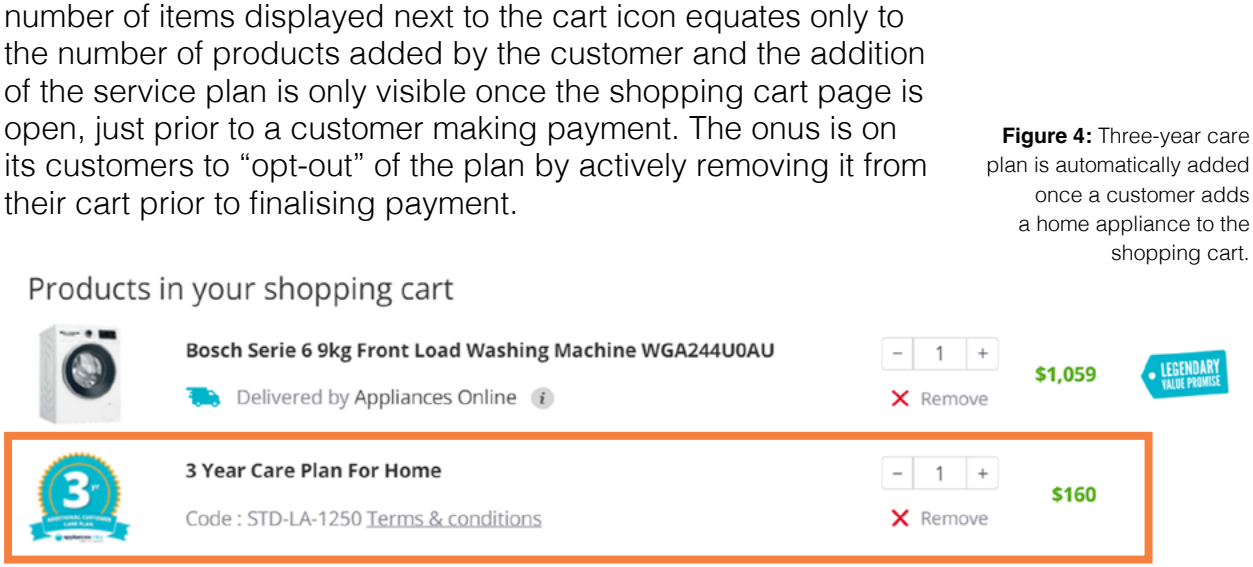
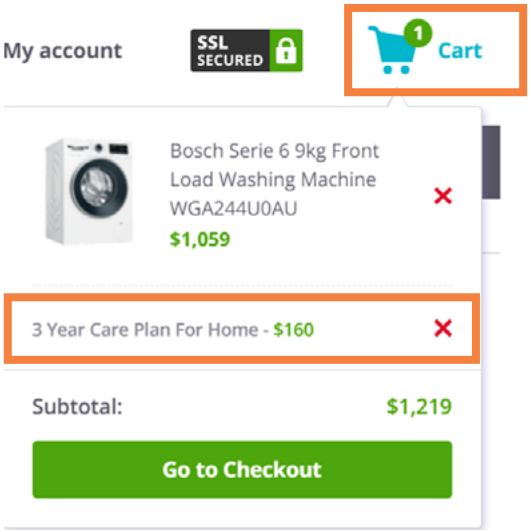



**Figure 4:** Three-year care plan is automatically added once a customer adds a home appliance to the shopping cart.

This design choice by Appliances Online strongly implies that a consumer requires a 3-year care plan in order to have a product repaired if something goes wrong. This hidden cost is particularly harmful because it likely adds an unnecessary product for the consumer. The "3-year care plan for home", like many extended warranties, adds very little extra value for a consumer when compared to the rights all consumers have for free under the consumer guarantees in the ACL.

Not all hidden costs are so blatantly added to an online shopping cart. Some are presented as part of a natural progression to finalising a purchase or are highly encouraged by the business (sometimes via a free trial) and can imply to a consumer that the additional purchase is necessary. Harvey Norman, Good Guys and Kogan use this technique where the product care plan is presented at several points of the checkout process. Again, this design approach risks implying that an extended warranty or product care plan is required when most faults or problems are adequately covered by the consumer guarantees. Kogan also opts-in the customer (via a pre-ticked option) for a free 14-day trial to its membership program which will automatically renew for an ongoing $59 annual fee after the trial ends (Figure 5).



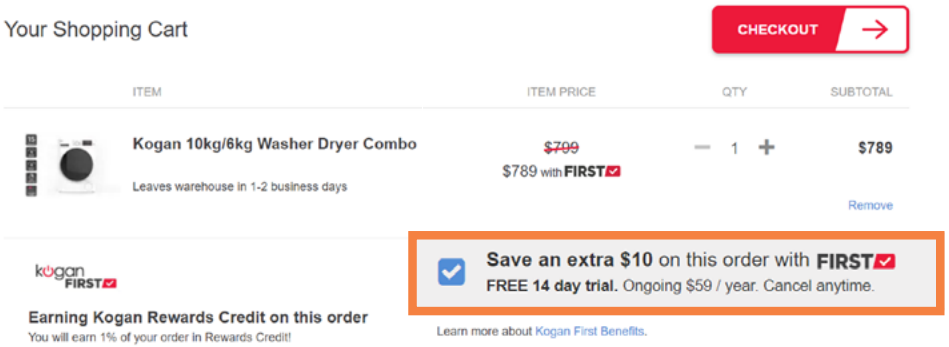



**Figure 5:** Membership program automatically added as a free 14-day trial during checkout.

### The harm caused by hidden costs

Almost nine out of ten survey participants (88%) have encountered additional costs being shown to them only at the end of a purchase process – just prior to payment. Almost two in five Australians (39%) found it deceptive, more than a third (36%) found it annoying and more than one in four Australians (29%) found it manipulative.

When mapping the spectrum of harm, we see the hidden costs dark pattern to potentially be a breach of misleading and deceptive conduct as the false or inaccurate impression a business gives to consumers of what a product or a service offers could also be taken into account in an investigation.[11]

*I have often went ahead and was going to buy something only to final the checkout that the prices have changed and the products are dearer than stated. I usually try to cancel the order but when I can't cancel I just close the page. Then I get lots of emails saying I left something in my cart.*

Comment from consumer survey participant

## Disguised advertisements

Disguised advertisements are click-bait, designed to make consumers navigate away from the site they originally visited. The format, wording and design of the content often mirrors regular content on the website or app. While some websites or apps include wording such as "Sponsored" or "Advertisement" near the ad, it is often in small, pale-coloured font. Research indicates a sizable proportion of consumers cannot differentiate between adverts and organic search results, despite the presence of these identifiers.[12] While in Australia, traditional media such as radio and television have strict rules for ensuring there is a clear delineation between content and advertisements, in the online world the line between ads and content is blurred.[13]

### What does it look like?

Our sweep identified disguised advertisements in mainly news and media websites and search services. For example, on a real estate website, advertisements for house and land packages outside of the search location, appeared seamlessly between actual property listings, both in the app and on the website (Figure 6). The word "Advertisement" appears above the sponsored listing but is extremely small and pale in print in comparison to the rest of the site.

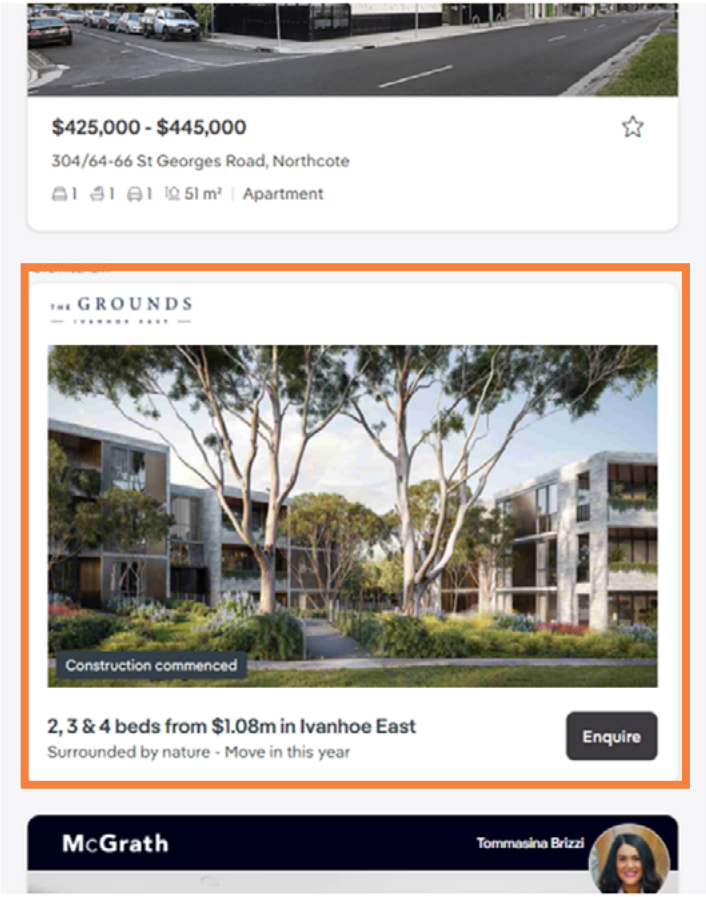



**Figure 6**: Advertised content appears in the same format and style as other property listings on the app.

### The harm caused by disguised advertisements

Our survey revealed that 85% of Australians had recalled seeing online content they found difficult to determine if it was content that was part of the site or an advertisement. Close to half (45%) found it annoying while one in three (33%) found it deceptive. More than one in four (28%) found that advertisements disguised as content made the website or app more confusing. This indicates a further exacerbation of search costs faced by consumers who already indicate these are much higher in an online environment compared to traditional non-digital settings. While it may not lead to immediate harms such as financial loss or providing more personal information than necessary, it may create additional search costs and more generally can deteriorate a consumer's online experience. But in some instances, this misleading advert could result in a clear economic harm – a mistaken purchase of a particular product or service. An organisation or business should be required to treat their online presence with the same obligations as their presence across other mediums. Advertising content online should not be treated differently to other mediums.

## Trick question

A trick question usually appears as a pop-up or on an online form asking the consumer to confirm a particular choice – which can be more subtle than other dark patterns. The options are not always clear, often due to the use of confusing language. This makes it difficult in instances where consumers are deciding whether to opt-in or op-out of specific options, settings or services.

### What does it look like?

Trick questions are often used when consumers are being asked to consent to data use and sharing practices. The introduction of GDPR in Europe led to a plethora of trick questions when it came to consent, where options provided were both confusing and could be construed as misleading for consumers, especially when used in combination with false hierarchy tactics (e.g. green button to consent to all types of data sharing and red button to adjust settings which often had to be done manually). The new legislation introduced at the beginning of 2022 by the European Union, has helped steer the industry towards better practices. However, as such a law doesn't exist in Australia, trick questions for data consent continue to appear (sometimes more just as a statement) for Australian consumers (Figure 7).

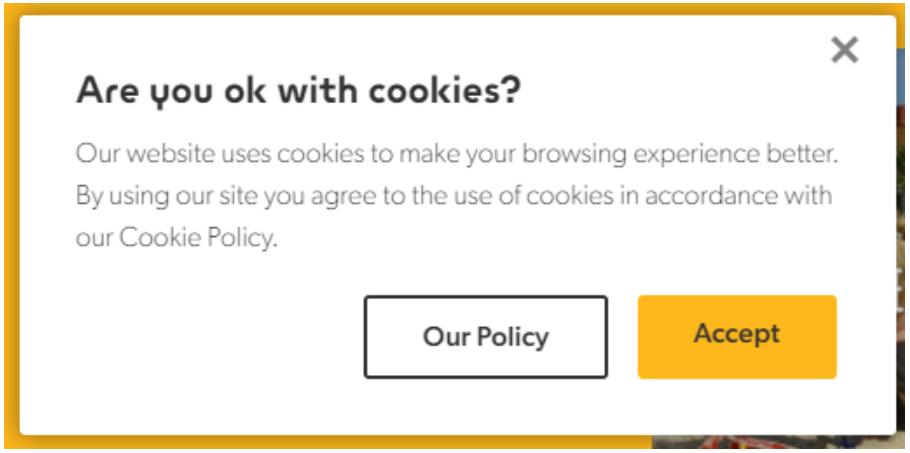



**Figure 7:** The question in this example is moot. When a user chooses the Our Policy option, it is a lengthy privacy policy and there is no option to adjust or change the settings.

## The harm caused by trick questions

Majority of consumers (85%) recalled seeing questions in an online form that use confusing language where it was not clear how to opt in or out of an option/service. Just over one in three Australians (34%) find it annoying, over one in four (26%) find it deceptive and over one in five (22%) consider this manipulative.

While not illegal, it is deeply unfair that websites push consumers to navigate unnecessary choices not in a consumer's best interests – adding significant cognitive burden. Currently, a trick question may be seen as misleading if information that is critical for a consumer's decision-making process is hidden via small print or is withheld entirely. This is often difficult to prove and the harm may only be evident after a specific period of time. An unfair trading prohibition could assist in mitigating this issue via a fairness test that could be incorporated into law. In addition, businesses should have obligations to ensure the choices they present to consumers have been tested for comprehensibility and are in the best interest of the consumer.

*"It is annoying when you have to opt out rather than opt in to some of these questions to continue the search…"*

Comment from consumer survey participant

## Scarcity cues

Instilling a fear of missing out (FOMO) in the minds of consumers, scarcity cues demand attention by creating the notion of limited supply or limited time to act This has the ability to set urgency to actions that either may not be present nor even necessary. This 'FOMO effect' can lead to consumers purchasing products and services far earlier than they may have intended or spending more than they may have spent had the cues not been present.

### What does it look like?

The "FOMO effect" is created in various forms such as through:

- low stock messages (e.g. only four left)
- high-in-demand messages
- countdown timers.

Our sweep identified several scarcity cues across a range of online businesses. Low stock messages were seen across both low and high value products (Figure 8).

'High-in-demand' messages appeared across a range of sectors However, in some instances the numbers can appear arbitrary, as regardless of style or colour that a consumer may select of a particular product, the number is often the same (Figure 9).

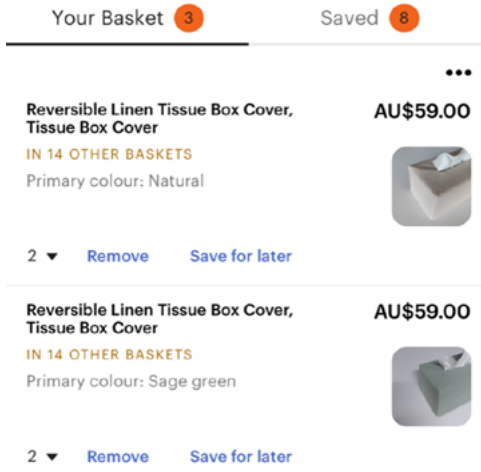



**Figure 9:** Two different colours of the same product are selected but the "high-in-demand" messaging notes same number for "in other people's carts".

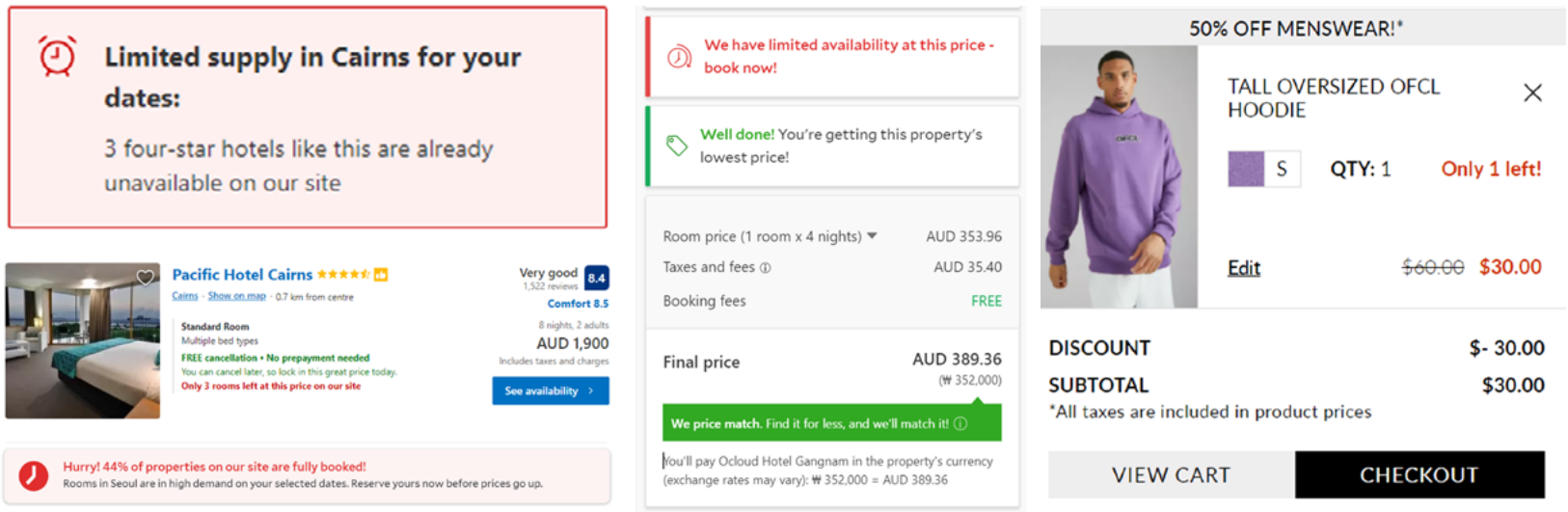



**Figure 8:** Examples of low stock messages from Agoda, Booking.com and Boohoo

Countdown timers were prominently seen on retail, entertainment and travel websites. On some sites it appeared on the header of the site – visible across the website, while on others it appeared at the final stage of payment creating a sense of urgency that may reduce cart abandonment (Figure 10).[14]

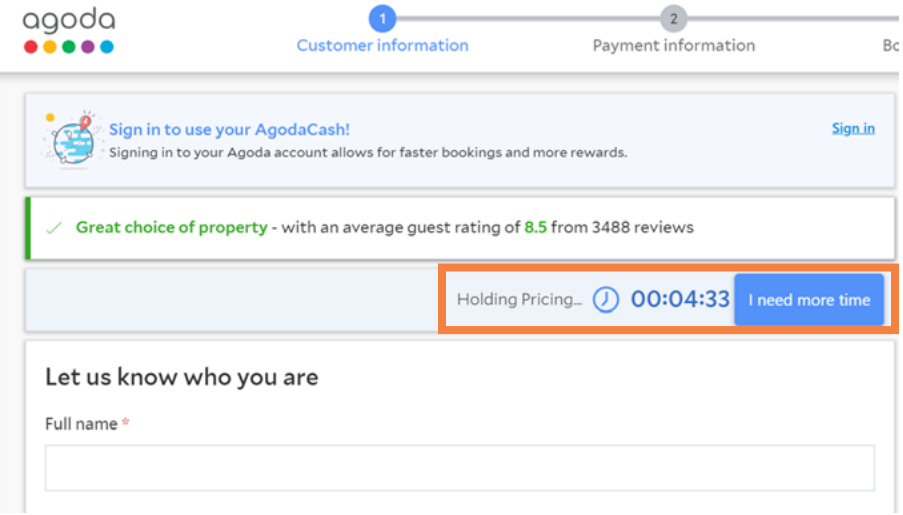



**Figure 10:** A countdown timer is added to the final stage of payment on the Agoda website and is shown as the length of time that the price will be held. The 'I need more time' button extends the timer by a few more minutes.

In some cases, once the countdown timer ran out, it was only replaced by another timer for another sale (Figure 11) and in others the countdown timer included a millisecond counter as well, again creating a sense that there is little time to wait or waste.

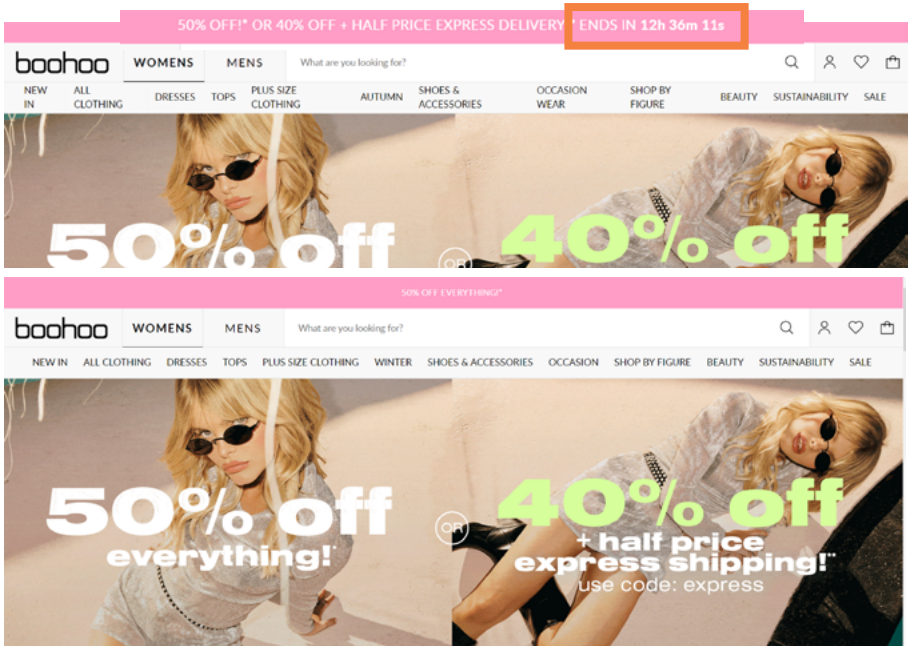



**Figure 11:** Boohoo's use of countdown timer: The first screenshot was taken on 4 May 2022 indicating that only a little over 12 hours remained to claim 50% off or 40% off with express shipping at half price. On 24 May 2022, the same offer, using the same imagery is shown again but this time without any countdown timer.

Bundling of scarcity cues was also identified on some websites where a combination of two types of scarcity cues were used to create further pressure for consumers to make a decision (Figure 12).

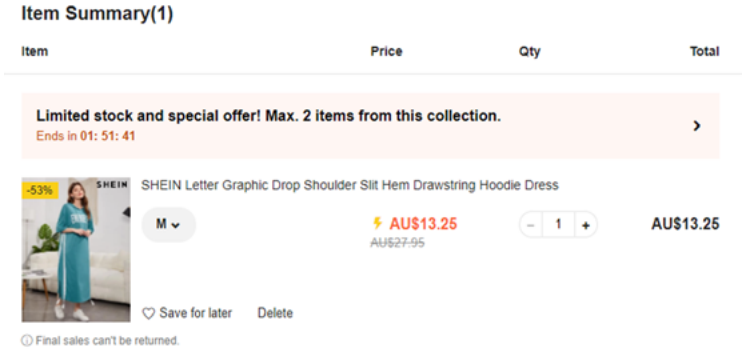



**Figure 12:** The online clothing retailer, Shein, combines both stock alert and a countdown timer to create a sense of urgency.

### The harm caused by scarcity cues

One of the most recalled dark patterns, 89% of Australians confirmed seeing notifications or information that state a product, service or offer is in high demand, low in stock or available for a very limited time. More than one in three Australians (35%) found this practice manipulative, while more than one in four (28%) found it deceptive. One in four (26%) felt they couldn't trust the information.

Trust in information is critical online as it is what consumers rely on to make decisions. In the spectrum of harm, scarcity cues sit squarely in the space of credence claims. The information asymmetry for the consumer is vast. There is no way for a consumer to confirm whether the urgency created is genuine, whether stock levels are indeed accurate or whether other consumers are also considering making the same purchase at any moment. Proactive surveillance by a regulator could help reduce the number of scarcity cues that consumers are exposed to, ensuring only accurate claims are seen by customers. Those that are found to be false, could be investigated further for a breach of laws on misleading and deceptive conduct.

*I don't like when a website says only one left for multiple products only when put in cart, then ya feel like it's pressure to buy it.*

Comment from a consumer survey participant

## Activity notifications

Activity notifications inform consumers about what other people are doing on the website or app. They often appear as innocuous notifications, either as a pop-up or embedded on the screen of a product or service that a consumer is viewing at the time.

### What does it look like?

Our sweep revealed that while activity notifications were innocuous, they were also persistent. Activity notifications in the form of a pop-up appeared frequently during a browsing session – often more prevalent on retail websites. A new activity notification appeared anywhere from every four to eleven seconds (Figure 13).

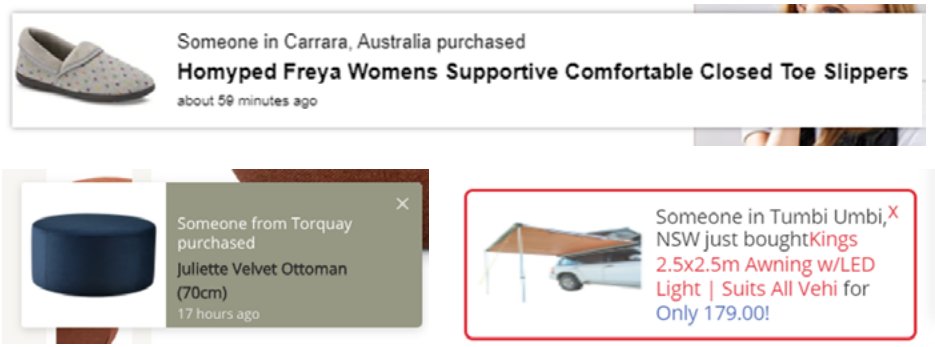



**Figure 13:** Examples of pop-up activity notifications.

Activity notifications were also bundled with and/or presented as a scarcity cue, creating an element of urgency to purchase a product or book a service (Figure 14).

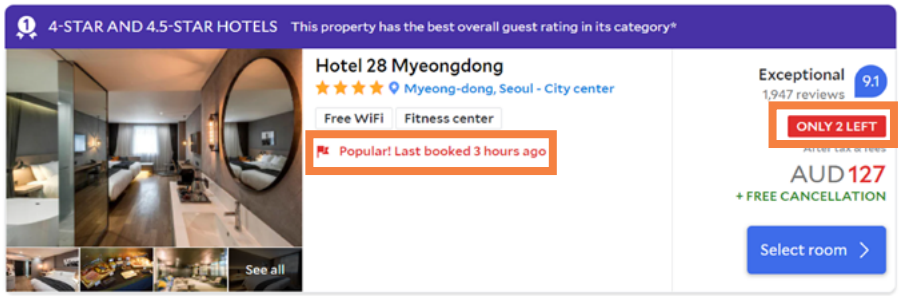



**Figure 14:** Agoda combines activity notification with a scarcity cue to create the urgency.

## The harm caused by activity notifications

A prevalent dark pattern, 86% of consumers surveyed recalled seeing information telling them about what other people are doing on the website or app. This included purchases, views or visits. One in three (33%) Australians find it annoying while about one in four (27%) felt they couldn't trust the information. More than one in five (23%) considered this manipulative.

Similar to scarcity cues, activity notifications sit within the credence claim category of the framework. Again, consumers have no way of knowing or validating whether these notifications are true or not. Also, some activity notifications were dated as "two weeks ago" and many could have been a rolling loop of a handful of activity that may have occurred on the site over any given period of time. However, given the frequency at which they are displayed on the website, it gives the impression of a hype of activity and an urgency to act which places undue pressure on consumers to enter into a purchase.

*Pop ups letting you know that a shopper in another part of the country has just purchased something is the most annoying pop up.*

Comment from consumer survey participant

## Confirmshaming

Confirmshaming is when specific language is used to suggest that a particular choice is shameful or inappropriate. It aims to make a consumer feel guilty or foolish for selecting the option that the business clearly does not want the consumer to make.[15] Often this is used to encourage consumers to:

- remain subscribed to a service
- share more personal information than necessary to complete a transaction (e.g. nudging consumers to create an online account)
- spend more than they may be originally intending (e.g. discounts offered at sign-up but require a minimum spend)
- subscribe to marketing content, including personalised advertising.

Confirmshaming is often also presented in forms of a false hierarchy where the discouraged option using the shameful language often appears smaller and less prominent than the preferred option by the business.

### What does it look like?

CPRC identified this example of confirmshaming from eBay in relation to unsubscribing from eBay Plus – a paid subscription program (Figure 15) and another from the footwear retailer Brand House Direct (Figure 16) which encourages customers to provide name and email address for a discount coupon. These designs are influencing consumers to either spend more money or share more personal information than they intend to. In both cases, the business outcome is to drive consumers towards a choice that the business can monetise, either immediately or in the future.

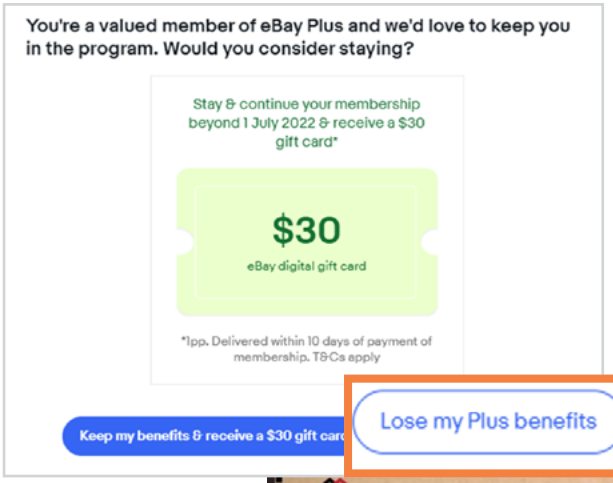



**Figure 15:** Cancelling eBay Plus membership is presented as "Lose my Plus benefits" while the alternative choice is "Keep my benefits and receive a $30 gift card".

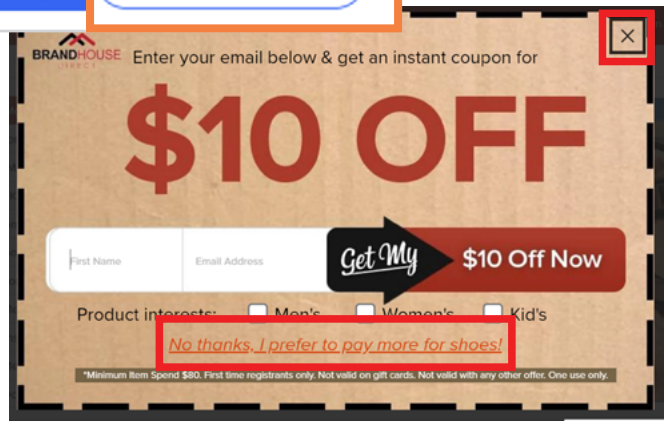



**Figure 16:** Brand House Direct positions the decision to not share personal information with them as choosing to pay more for shoes. The link is not clickable and the only way to close the pop-up is via the X button on the top right-hand corner.

### The harm caused by confirmshaming

The majority of consumers surveyed recalled seeing the practice of confirmshaming. The survey revealed that 80% had seen language used on a website or an app which suggests that a certain choice is irresponsible or shameful. Almost two in five (38%) consumers found it manipulative, almost one-third (30%) found it annoying and over one in five (22%) found it deceptive.

Confirmshaming has potential to cause consumer harm by manipulating financial and data-sharing decisions. However, it is unlikely to be a breach of current provisions of the ACL. It is a practice that is unfair but not illegal. However, a prohibition on unfair practices could help create a shift away from these design practices.

## Hotel California (Forced continuity)

Named after the song which famously includes the line, *"You can check out any time you like but you can never leave"*, Hotel California,[16] also known as forced continuity, is a dark pattern which uses design features and website navigation in a way that impedes consumers' ability to cancel or move out of a particular service.

The Hotel California strategy is often used to discourage people from cancelling an online subscription or service, including services involving a free trial. It can often involve complex website or app navigation paths that require several clicks, vague terminology and continuous attempts to encourage the consumer to reconsider a request. This design treatment is very likely to cause consumer frustration and lead to financial costs depending on the degree of difficulty a consumer has when trying to cancel or stop charges.

### What does it look like?

Amazon is well-known for its use of the forced continuity dark pattern when it comes to unsubscribing from their services. In 2021, the Norwegian Consumer Council's investigation at the time led to identifying that while it only takes consumers three screens/clicks to subscribe to Amazon Prime, a consumer needs to navigate up to 12 screens/clicks to unsubscribe from the service.[17]

Our sweep found that while it may no longer take 12 screens to unsubscribe from an Amazon service, it still requires navigating more than 5 screens (some involving lengthy content) to finalise cancellation of an Amazon Music Unlimited subscription. The consumer is unable to unsubscribe directly from the Amazon Music app but is redirected to the main Amazon app. Once there, the consumer is requested to provide a reason for cancellation after which Amazon provides alternative plans which the consumer must navigate before confirming cancellation which isn't explicitly confirmed showing only one button with the prompt "Continue subscription".

Similarly, our sweep found that navigating through cancelling an eBay Plus subscription involved multiple steps (Figure 17). Combining a mix of dark patterns (confirmshaming, forced continuity and false hierarchy), it takes four additional steps after selecting "cancel membership" to successfully cancel it.

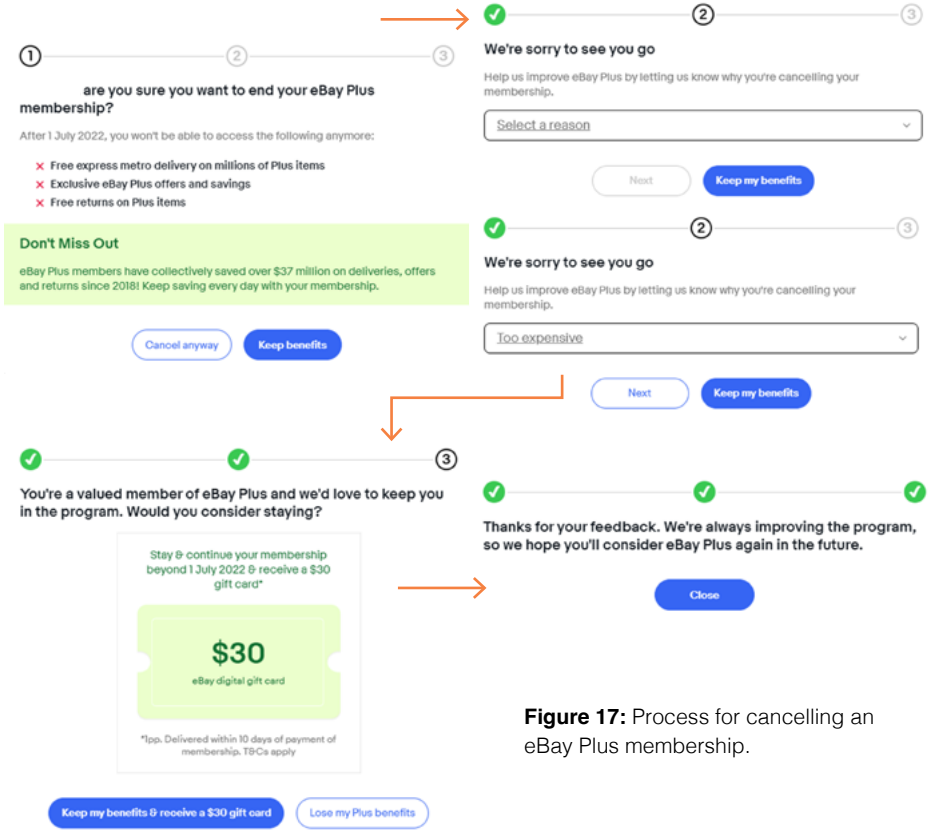



**Figure 17:** Process for cancelling an eBay Plus membership.

Conversely, it only takes one click after clicking on the eBay Plus icon to join the service and if a user creates a new eBay account, the first pop-up upon creating their account is a prompt to subscribe to the service's free trial followed by choice of subscription plan by adding the payment details directly into that pop-up and clicking Continue (Figure 18).

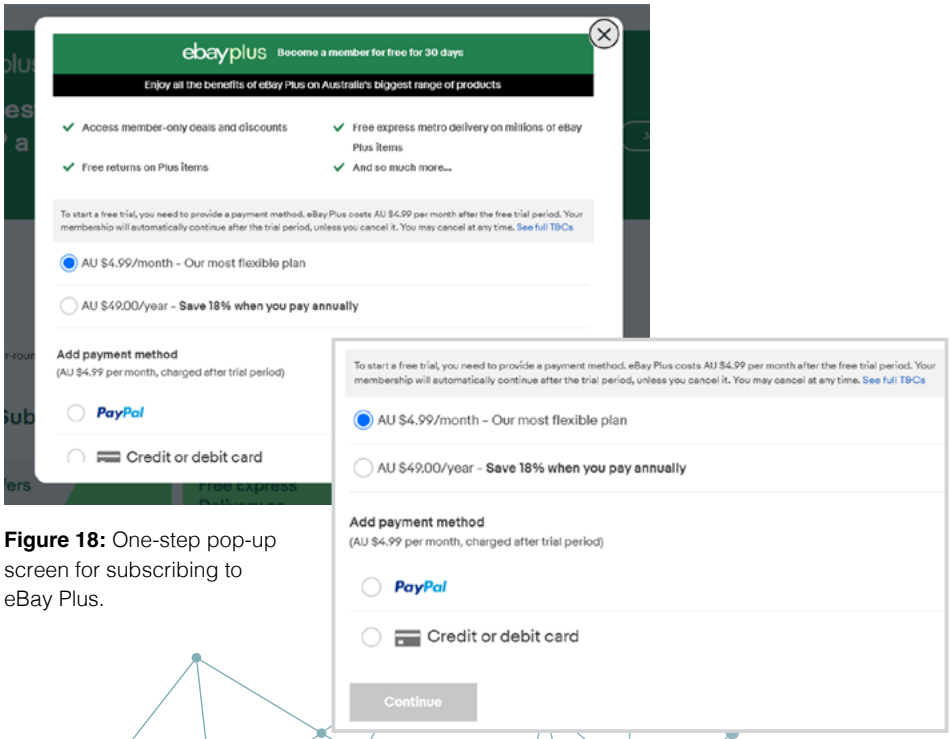



**Figure 18:** One-step pop-up screen for subscribing to eBay Plus.

## The harm caused by forced continuity

Three in four (76%) consumers surveyed had experienced difficulty cancelling an online subscription, including unsubscribing before a free trial ends. While 44% of Australians found the practice annoying and 39% found it deceptive, this practice also led to consumers forming perceptions that in the long-term could prove damaging for businesses. More than two in five Australians (41%) found that it made them want to stop using the website or app and 39% of Australians felt they couldn't trust the business.

Forced continuity is yet another design type that is not explicitly illegal in Australia but it can lead to consumers being forced into keeping products or services that they no longer need, with the propensity to cause them financial harm. This potential market-based harm may be exacerbated or compounded for those consumers already experiencing circumstantial vulnerabilities (e.g. sudden illness or bereavement) or systemic vulnerabilities (e.g. lower digital literacy).[18]

In the spectrum of harm, forced continuity is unfair practice but certainly not illegal.[19] A prohibition on unfair practices could help introduce measures that protect consumers who may feel trapped or locked into services they no longer need. For example, one way to achieve this is for government to impose obligations that a service should be as easy to opt-out of as it is to opt-in. Laws requiring that businesses offer simple online cancellation services have already been enacted in specific cases in Australia. For example, in 2018, the National Consumer Credit Code was amended to allow easier online credit card cancellation options after a Senate Inquiry found that consumers could easily sign up for a credit card but typically had to take multiple complex steps to cancel.

## False hierarchy

The practice of false hierarchy aims to nudge consumers to a particular choice, even if more than one option is provided. Often this is done to make the "preferred choice" stand out over others through size, placement or colour. False hierarchy tends to appear as an invitation to consumers to sign-up to marketing content in return for discounts or that push consumers towards a purchase. It can often lead to consumers sharing more personal information or lead them to spending more than they intended to as the offer or discount received may involve a minimum purchase amount.

### What does it look like?

Our sweep identified several examples of false hierarchy where the least preferred option was paler or less prominent in colour, smaller in size or available only via a small X icon on the top right corner to close the pop-up. The preferred option was displayed clearly, often using background button colours such as green or blue, which often correlate with a calming and positive/correct action (Figure 19).[20] Alternatively, some designs used a prominent colour from the website's own colour palette, indicating a natural progression.[21]

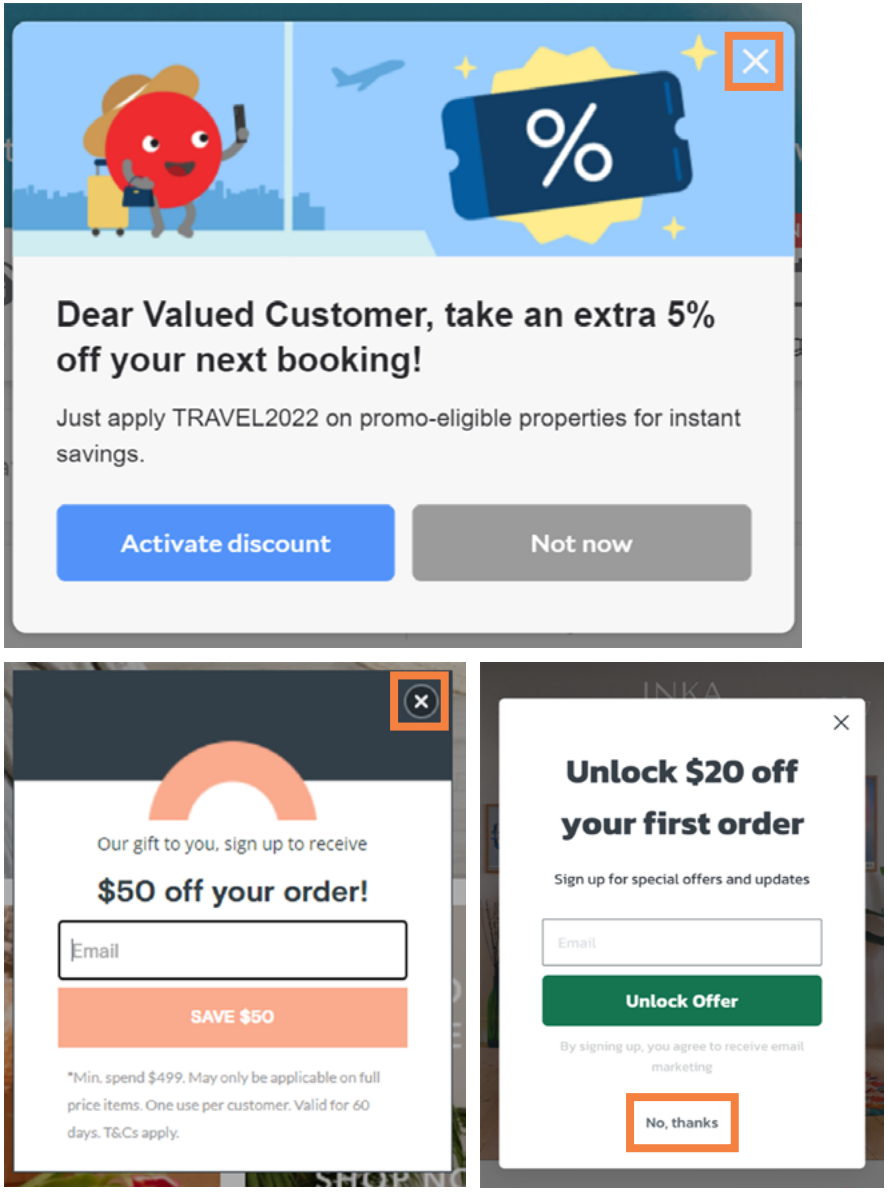



**Figure 19:** Examples of false hierarchy – we have drawn an outline around the "not preferred" action.

In some instances, an alternative option is not provided to consumers at all. Displayed as a pop-up, the only way to detour away from the false hierarchy is to click outside of the pop-up to make the “preferred option” disappear (Figure 20).

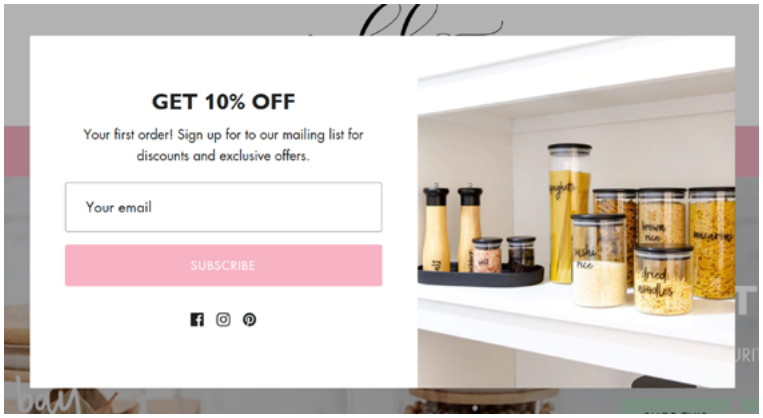



**Figure 20:** No alternative button or close symbol provided. Consumers must click outside of the pop-up if they wish to navigate around the false hierarchy.

### The harm caused by false hierarchy

Most Australians (86%) have recalled seeing false hierarchy on websites or apps where one option is made to stand out more through colour, size or placement on the webpage.
One in four Australians (26%) found this practice to be manipulative. Given its prevalence in parts of websites or apps where personal information is sought, it can potentially have long-lasting implications for a person’s privacy. Often many such pop-ups either fail to include information on the organisation’s privacy policy or include it via a link in fine print. It creates a choice architecture that is heavily swayed towards benefitting businesses but has very little regard for meaningful consumer outcomes.

## Redirection or nagging

Redirection or nagging occurs when a consumer is continuously moved away from the activity they wanted to complete. This can often be in the form of a pop-up inviting consumers to join an email subscription, claim a particular offer or entice them into remaining on the website or app.

### What does it look like?

Our sweep revealed that pop-ups were the most prevalent and persistent technique of nagging. The fast-fashion online retailer, Shein, used several pop-ups to encourage users to share their email or to set-up an account (Figure 21). As soon as one pop-up was closed, immediately a new pop-up would appear with an invitation of a new offer to claim.

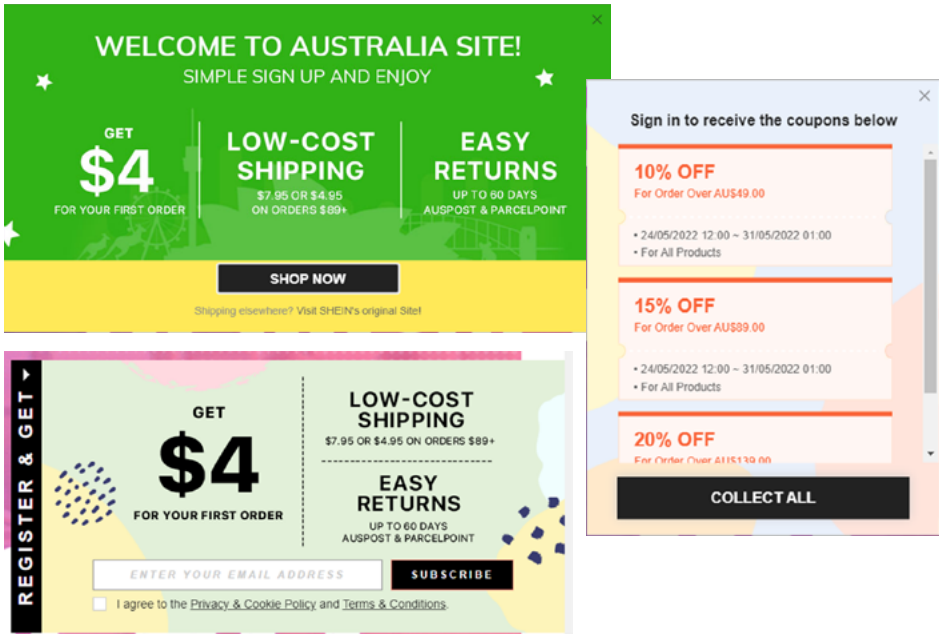



**Figure 21:** On Shein’s website, users have to navigate through three instances of pop-ups, one after the other before being able to access the site.

Some websites seem to have a built-in cursor reader so as the cursor moved towards closing a site, changing tabs or was stagnant for a specific period of time, a pop-up would appear encouraging the consumer to remain on the website by signing-up to a new offer or to share contact details so a quote or the shopping cart could be emailed to the consumer (Figure 22).

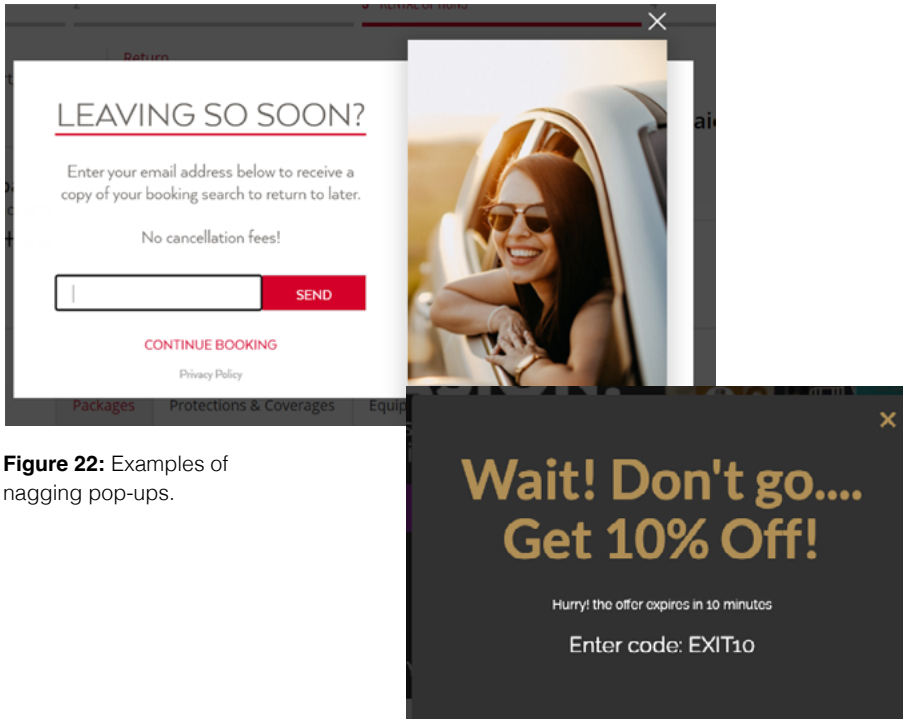



**Figure 22:** Examples of nagging pop-ups.

To what extent emails provided in these instances are then stored or added to customer databases or profiles is unclear but given the benefits of data harvesting for businesses, it is likely the personal information shared as result of these pop-ups would not be for one-time storage or use. Nagging can also occur after a consumer has left the website or app when contact details have been shared (Figure 23).

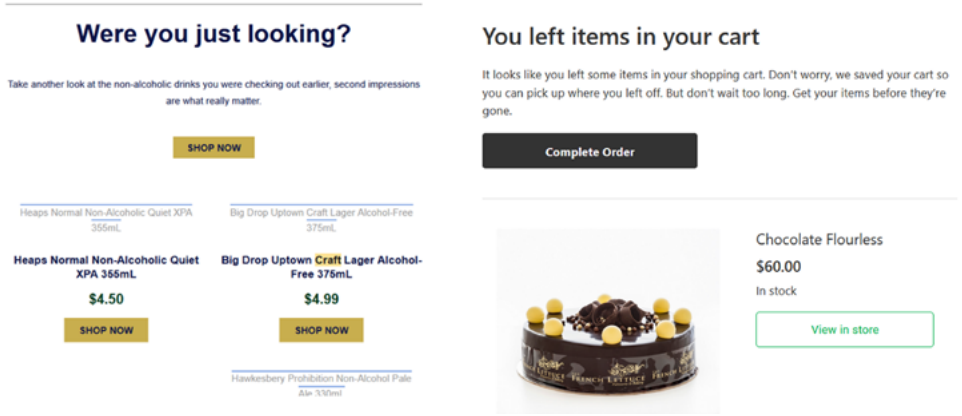



**Figure 23:** Examples of nagging emails that remind consumers what they may have been browsing or products they may have abandoned in cart.

## The harm caused by redirection or nagging

Most consumers surveyed (88%) recalled seeing a pop-up appear and interrupt or move them away from what they wanted to do on the website or app. These included requests to turn on notifications, constant invitations to join an email subscription or encouragement to claim an offer. Almost half (48%) of Australians found it annoying, while about one in five (21%) wanted to stop using the website/app. One in five (20%) also found the practice to be manipulative.

Pressure sale tactics have been applied by businesses well before the digital era. In a physical setting, it can be, in some instances, difficult for a consumer to retreat but once retreated, a consumer is unlikely to be nagged due to lack of personal information available to the business. However, in an online setting, consumers can be redirected and nagged even after they've moved away from the website. It creates an unfair advantage for a business which is able to use consumer data to continue to place pressure on a customer for longer periods of time.

## Data-grab

While the aim of many dark patterns can be to harvest more personal information, our research identified that certain design features and functionality have been built specifically into websites or apps for the sole purpose of collecting more consumer data. We have coined these as “data-grab” dark patterns.

### What does it look like?

Data-grab can happen in various forms including:

- pre-ticking the option to receive marketing content from the business (Figure 24)
- forcing a consumer to create a customer profile and/or requesting more information than necessary to browse or purchase a product or service (Figure 25)
- showing a message on the website or app notifying consumers that by using the website they accept their data terms and conditions (Figure 26).

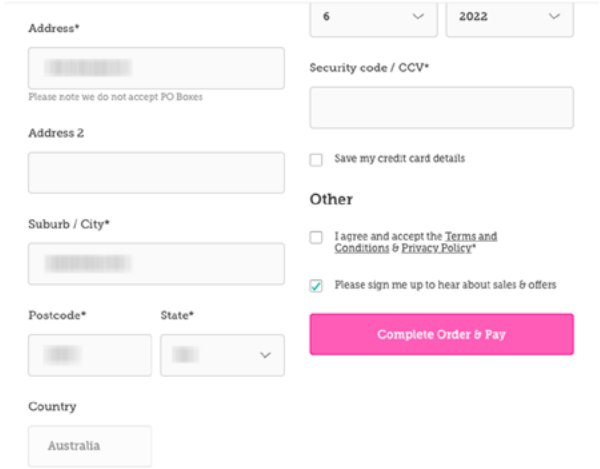



**Figure 24:** During this checkout process, the option to sign-up to sales and offers is pre-ticked.

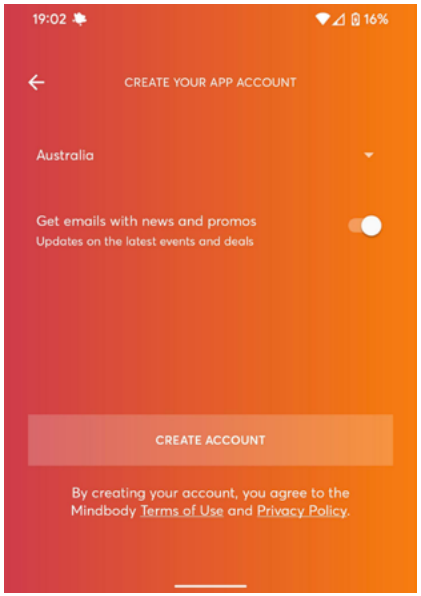



**Figure 25:** To just view the timetable for a yoga class, the businesses uses an app in which the user must create an account before accessing the timetable.

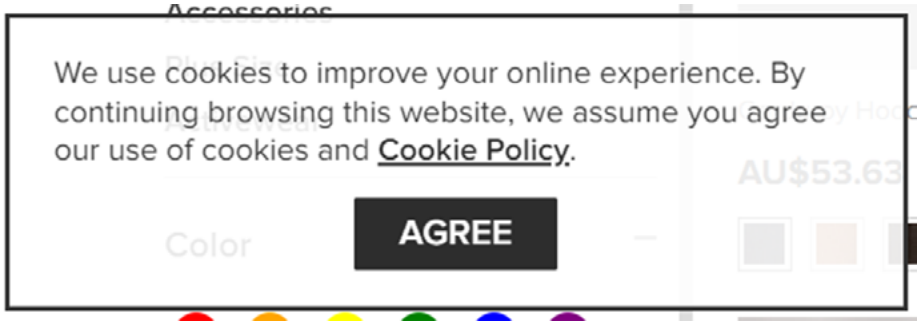



**Figure 26:** No alternative is provided and the consumer must choose between agreeing to an already set cookie policy or being excluded from browsing the site.

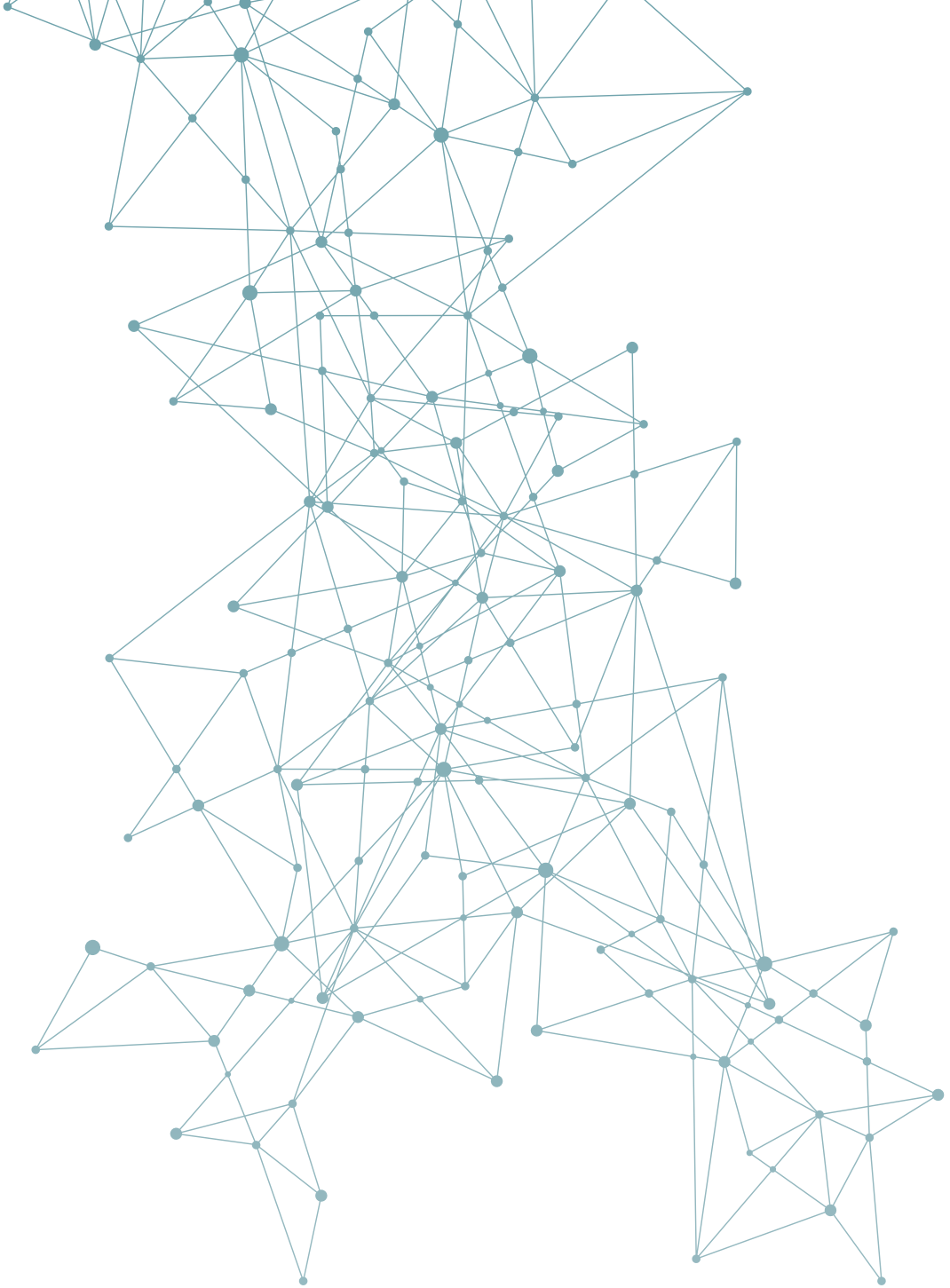
### The harm caused by data-grab

The majority of consumers surveyed (89%) recalled being asked for more information about themselves than what was needed to access a product/service. Almost two in five (39%) Australians noted that the practice concerns them, while one in three (33%) felt they couldn’t trust the business. Nearly one in three (32%) Australians wanted to stop using the website or app.

These results are unsurprising given that CPRC's 2020 Data and Technology Consumer Survey revealed that 75% of Australians feel businesses have a high level of responsibility to provide protection against collection and sharing of personal information and eight out of ten consumers are uncomfortable with unnecessary sharing of their information.[22]

The data-grab dark pattern can have significant implications for consumers. Their personal information can be used to make predictions about them to drive commercially-beneficial outcomes for businesses. Personal information can also be highly sensitive and if not used with care would violate a consumer's privacy. Personal data can also be used to influence what someone consumes and at what price.[23]

The data-grab dark pattern could potentially breach the Australian Privacy Principles of being open and transparent on how personal information is managed or when there is a lack of notification that a particular action by a consumer will lead to collection of personal information.[24] Also, some design practices could be a breach of unfair contract terms law if a different set of personal information is sought from a consumer who enrols online to those that enrol in a physical setting without having any difference to the type of service they receive. However, existing laws, in particular the Privacy Act, do not go far enough to protect consumers. Currently, the definition of personal information is limited to data 'about' an individual (e.g. name, address, date of birth, health records, phone number). Due to the limited case law on this concept, there is presently uncertainty about whether personal information would include data - such as IP addresses and location histories – that goes beyond these traditional forms of personal information. Today, multiple sources of data may relate to an individual without using their real name. These can be collected and aggregated to easily assist in re-identification of the individual.[25]



# The consumer experience

Dark patterns create consumer harm. While some are irritating or annoying, others are leading to direct financial costs to consumers or are misleading people about what they are buying or what their rights are as consumers.

CPRC's consumer survey found that there is a high level of awareness that organisations use dark patterns to influence users into behaving a certain way (58% of survey participants). There is also a high level of frustration being experienced by Australian consumers when online.

"Manipulative" or "Deceptive" were in the top three responses to nine out of the ten dark patterns tested with Australian consumers. The deceit felt by Australian consumers, even with those dark patterns that at the outset may seem innocuous or ubiquitous, is significant. Our survey revealed that 83% of Australians experienced one or more negative consequences as a result of a website or app using design features aimed at influencing their behaviour.

Despite the growing ubiquity of dark patterns, it does not mean consumers have become accustomed to them or consider them as fait accompli; instead, it is deteriorating their experience in the digital economy.

*"I feel that it is many of the online stores that use these tactics to manipulate, trick or entice you to sign up for something you really don't want. I believe you have to be very vigilant when using some apps and websites."*

*"…I don't buy a lot online anyway but more so because I've experienced these types of websites. I would buy more online if the websites did less of this type of behaviour."*

Comments from consumer survey participants

Negative consequences ranged from impacting a consumer's emotional wellbeing to those impacting consumers financially or resulting in loss of control over personal information (Figures 27, 28 and 29).

**40%**
felt annoyed when using a website or app

**28%**
felt manipulated

**Figure 27:** Impact on Australian consumers' emotional wellbeing

**1 in 5 Australians** spent more than they intended (20%)

Almost **1 in 6 Australians** felt pressured into buying something (17%)

Nearly **1 in 10 Australians** accidentally bought something (9%)

**Figure 28:** Financial impact of dark patterns on Australian consumers

More than **1 in 4 Australians** created an account online they didn't want to (29%)

More than **1 in 4 Australians** accidentally signed up to something (29%)

**1 in 4 Australians** shared more personal information than they wanted to (25%)

**Figure 29:** Australian consumers feeling a loss of control over how their personal information is shared

## The impact on younger consumers

Younger consumers are even more negatively impacted by dark patterns. Younger Australians (aged between 18 and 28 years) are more likely to part with more of their money and their personal information than any other age group. This can lead to considerable impact on their financial wellbeing and mean more businesses have access to their personal information that can be used in future to target this group of customers (Figure 30). For example, younger consumers were 65% more likely to spend more than they intended to online and 34% more likely to create an online account they didn't want to due to dark pattern influences.

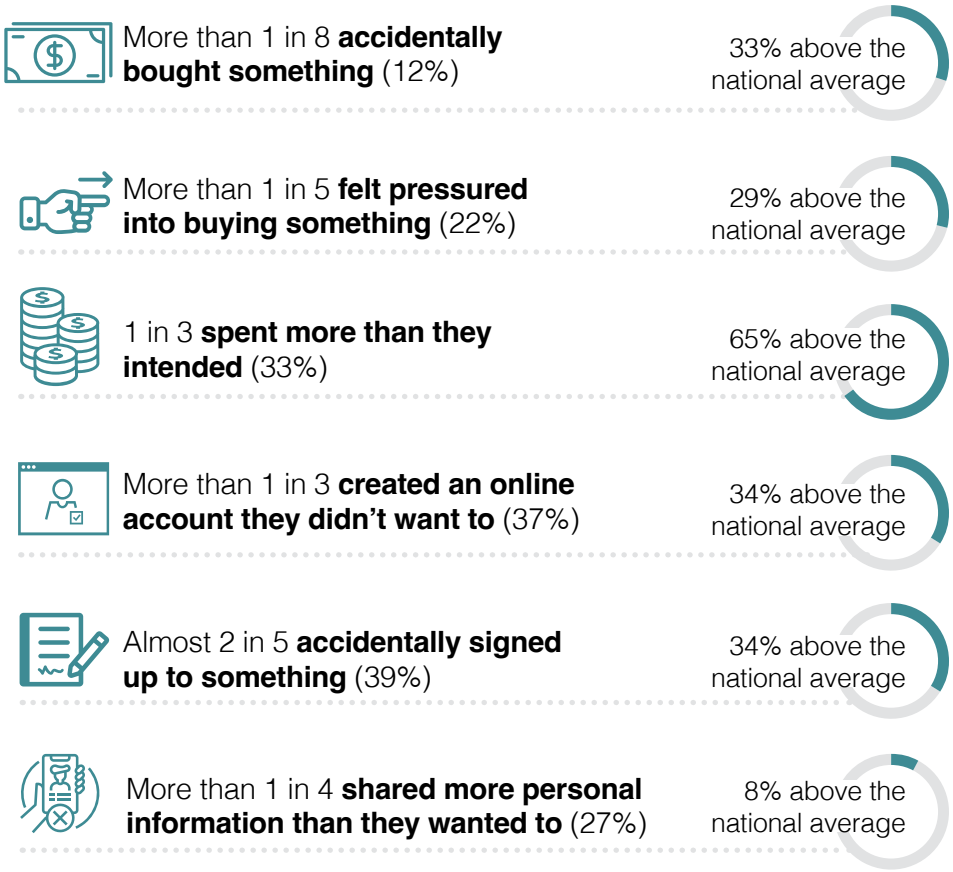



**Figure 30:** Impact of dark patterns on younger consumers aged 18-28 years

*"I hate it when they bombard you with many things such as ads, countdowns, pop ups, colours, deception and it makes it really hard to deal with."*

Comment from consumer survey participant aged between 18 and 28 years

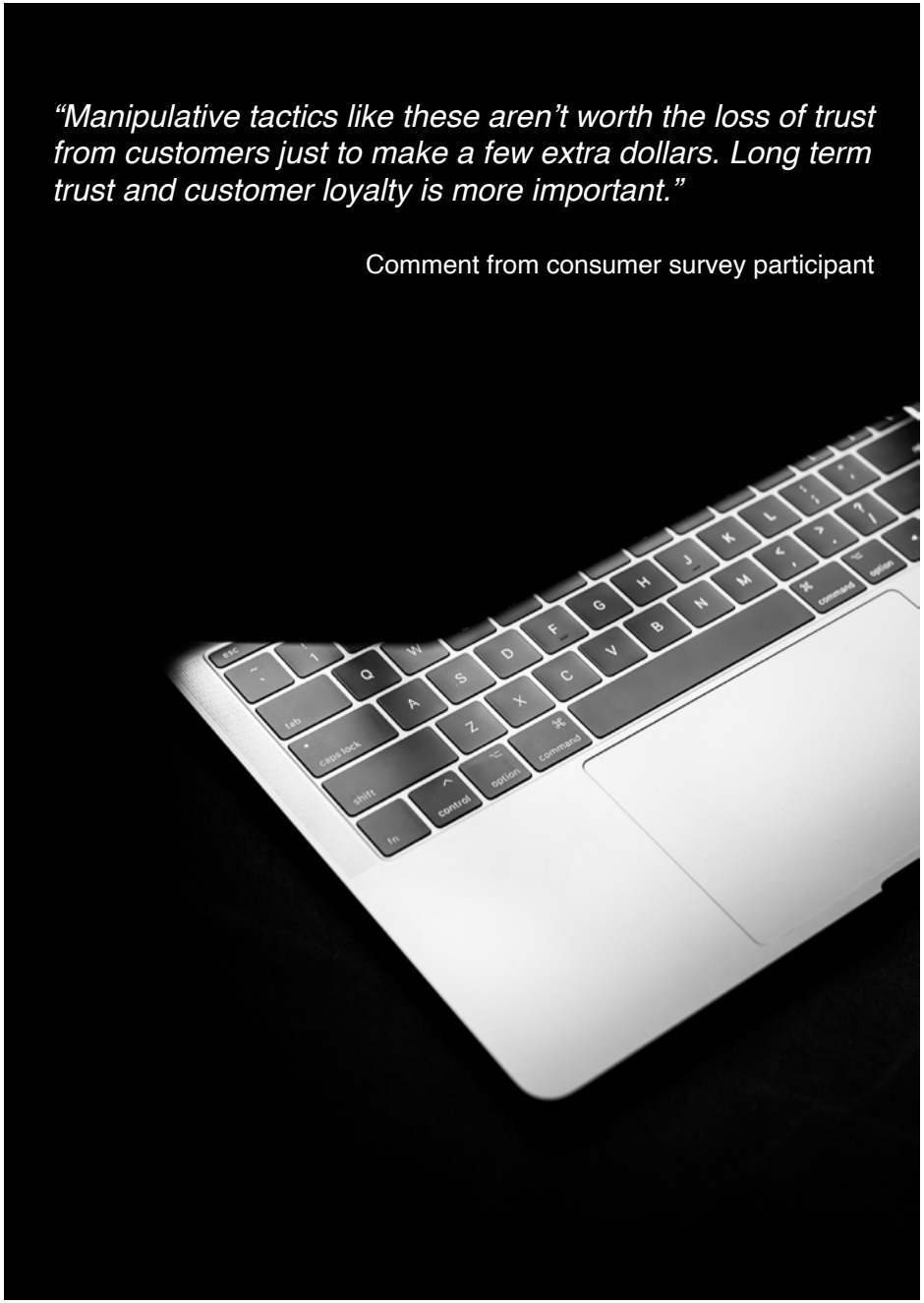
## The cost to business

Businesses that use dark patterns across their online platforms are likely to increasingly face consequences, whether that's from consumers turning to user friendly competitors or action from regulators when the dark patterns used cause direct consumer harm. While in the short-term dark patterns may lead to a financial gain or enable data harvesting that can be monetised, in the long-term it can negatively impact the businesses due to a loss of consumer trust and loyalty (Figure 31). Trust has been widely identified as a key component of well-functioning markets – 'individuals and organisations will find it difficult (if not impossible) to operate effectively if they do not enjoy the trust and confidence of the community in which they are located'.[26]


**Figure 31:** Australian consumers' perception of businesses using dark patterns

*“Manipulative tactics like these aren’t worth the loss of trust from customers just to make a few extra dollars. Long term trust and customer loyalty is more important.”*

Comment from consumer survey participant



# Addressing the harms and next steps

Australia has a real opportunity to step-up consumer protections in the digital economy. With the current review of the Privacy Act underway and ACCC’s Digital Platforms Inquiry which has consistently revealed gaps in the consumer law, the time has come to protect Australian consumers. The onus can no longer remain on consumers to navigate a digital economy that hasn’t been designed with consumer interests in mind. The “hands-off” approach to market stewardship of the digital economy has facilitated the growth of exploitative practices, leveraging consumer biases against them and heighten existing information asymmetries. Businesses need to take responsibility for their actions and proactively identify and stop potential consumer harm.

Internationally, jurisdictions have made significant strides in addressing the harms of dark patterns. The European Union introduced its Unfair Commercial Practices Directive in 2005 and has continued to strengthen it regularly. Its most recent iteration came into effect in May 2022. It includes obligations relating to data-driven personalisation and dark patterns.[27] In March 2022, the European Data Protection Board commenced consultation on new dark pattern recommendations for both designers and commercial users of social media.[28] Meanwhile, in April 2022, the United Kingdom’s Competition and Markets Authority released a detailed publication on choice architecture outlining how choice is structured, the information provided around it or how the pressure to choose can cause both competition and consumer harm. It also outlined its intent to take greater enforcement action in this space.[29]

In the United States, the Federal Trade Commission has publicly noted its enforcement focus on dark patterns, putting companies on notices who implement dark patterns that trap consumers into subscription services.[30] In March 2021, the US state of California, strengthened its 2018 California Consumer Privacy Act which banned dark patterns that have "the substantial effect of subverting or impairing a consumer's choice to opt-out". It applies to practices such as using confusing language and forcing users to navigate through unnecessary steps about why they shouldn't opt-out.[31]

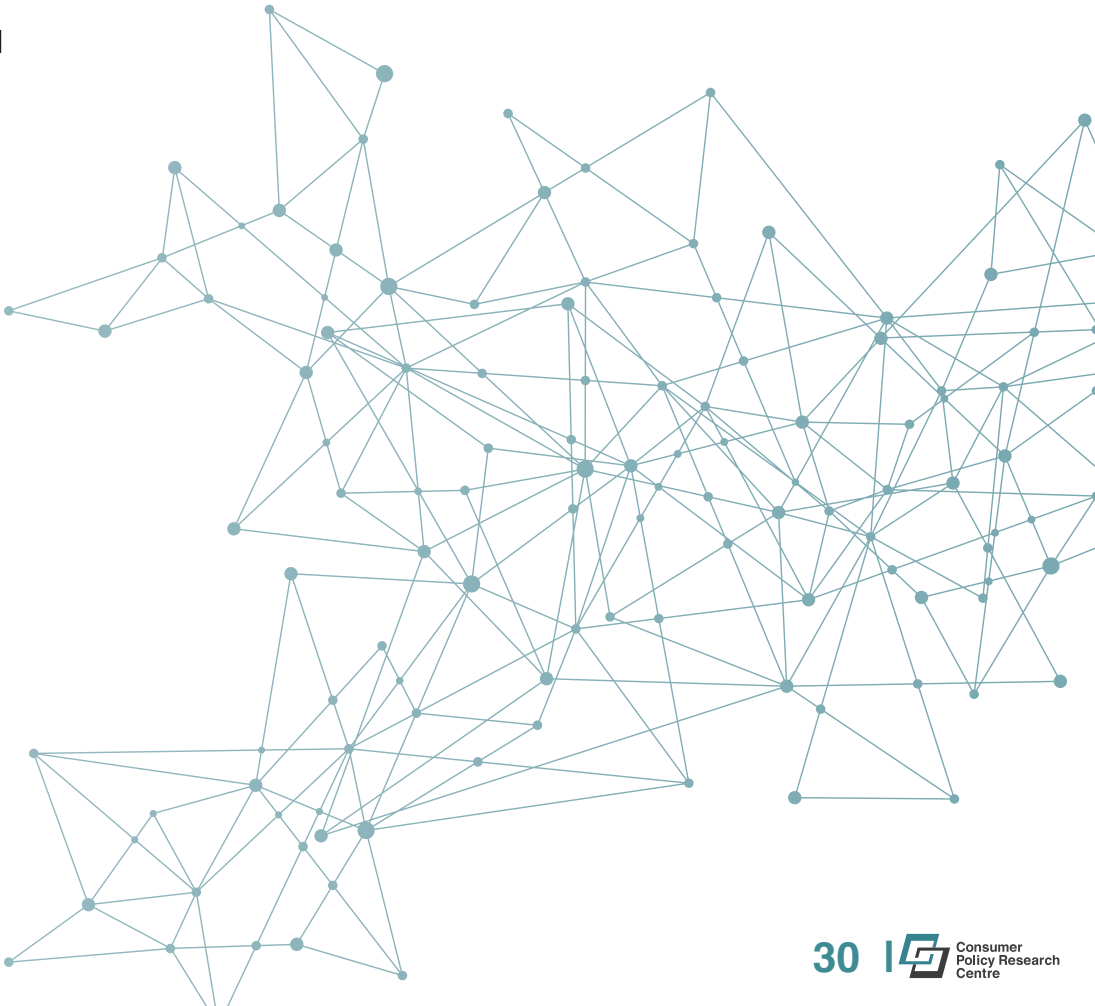
## What does the Australian Government need to do?

Currently the laws we have in place in Australia can only be used to deal with a narrow range of harms caused by dark patterns. For example, laws against misleading and deceptive conduct cannot necessarily apply to instances where businesses coerce consumers into a specific choice. In addition, when it comes to the unconscionable conduct provision under the ACL, court rulings indicate that the threshold of applicability is high, and many practices that have been identified as unfair in this report would not meet this threshold.[32]

The *Competition and Consumer Act 2010*, including the ACL, should be reviewed to ensure it is fit-for-purpose for the digital economy. However, wider whole-of-economy reforms are also needed to adequately protect consumers, such as:

- introducing an unfair trading prohibition
- strengthening unfair contract terms provisions
- reforming the Privacy Act to give consumers more control and agency over their data.

In addition to these reforms, Government must ensure dispute resolution models are relevant for the digital economy today and in the future. While the ACCC's recommendation of an ombudsman scheme for digital platforms led by the Telecommunication Industry Ombudsman[33] and the Attorney-General's proposal to introduce a Privacy Ombudsman[34] are a starting point, they are still only providing a piece-meal approach to support and redress. There is merit in considering a more holistic approach such as a Digital Ombudsman that provides consumer support across the digital economy and is flexible enough to respond to today's challenges and complex matters that are likely to arise in the future.[35]



## What can regulators do?

For legislation to be effective, it needs to be supported by regular surveillance and enforcement by the regulator to educate and shift the market towards a more consumer-centric approach to the digital economy. Australia needs a well-resourced regulator with the capacity and capability to audit and enforce breaches in the complex digital environment. Traditional compliance and enforcement models often take place post harm. This needs to be reimagined if protection is to be adequately delivered to consumers in the digital economy.

Regulators also need more sophisticated approaches to identify harm. Currently regulators largely rely on reports from consumers, identifying harm after it takes place. Consumers can't continue to be responsible for identifying and reporting breaches, especially for complex digital issues where they may not be aware of design and data-driven manipulation. Instead, regulators need to proactively uncover harm that is currently obfuscated. Regulators should be pushing businesses to be radically more transparent about their business models and practices – this is a first step to then removing unfair practices.

Monitoring and surveillance by regulators in this complex environment needs a diverse workforce that not only understands the implications of the law but also the technical architecture on which these business models are built upon. Experts such as ethical designers, data scientists, artificial intelligence engineers, information security analysts and other technical professionals need to be in the mix to support upstream regulation and mitigate the risk to consumers, potentially before widespread harm has occurred.

## What can businesses do today?

Businesses have the opportunity to be at the forefront of consumer-centric change and to lead by best practice. Our consumer survey revealed a significant portion of consumers reported leaving platforms, losing trust in businesses or having negative feelings towards businesses using dark patterns. Adjusting the mindset from a purely profit-driven perspective to a consumer-centric perspective may assist in reducing the prevalence of those negative outcomes and lead to better business outcomes in the longer-term.

Businesses, especially large corporations and those that design and supply off-the-shelf e-commerce products and services, should consider:

- conducting an audit for any dark patterns on their websites and apps amending and adjusting design features on their websites and apps that are causing consumer frustration or harm (in reference to the previous sections)

- undertaking regular consumer user experience (UX) testing that considers the consumer journey across their platform from the lens of the consumer, not the business.

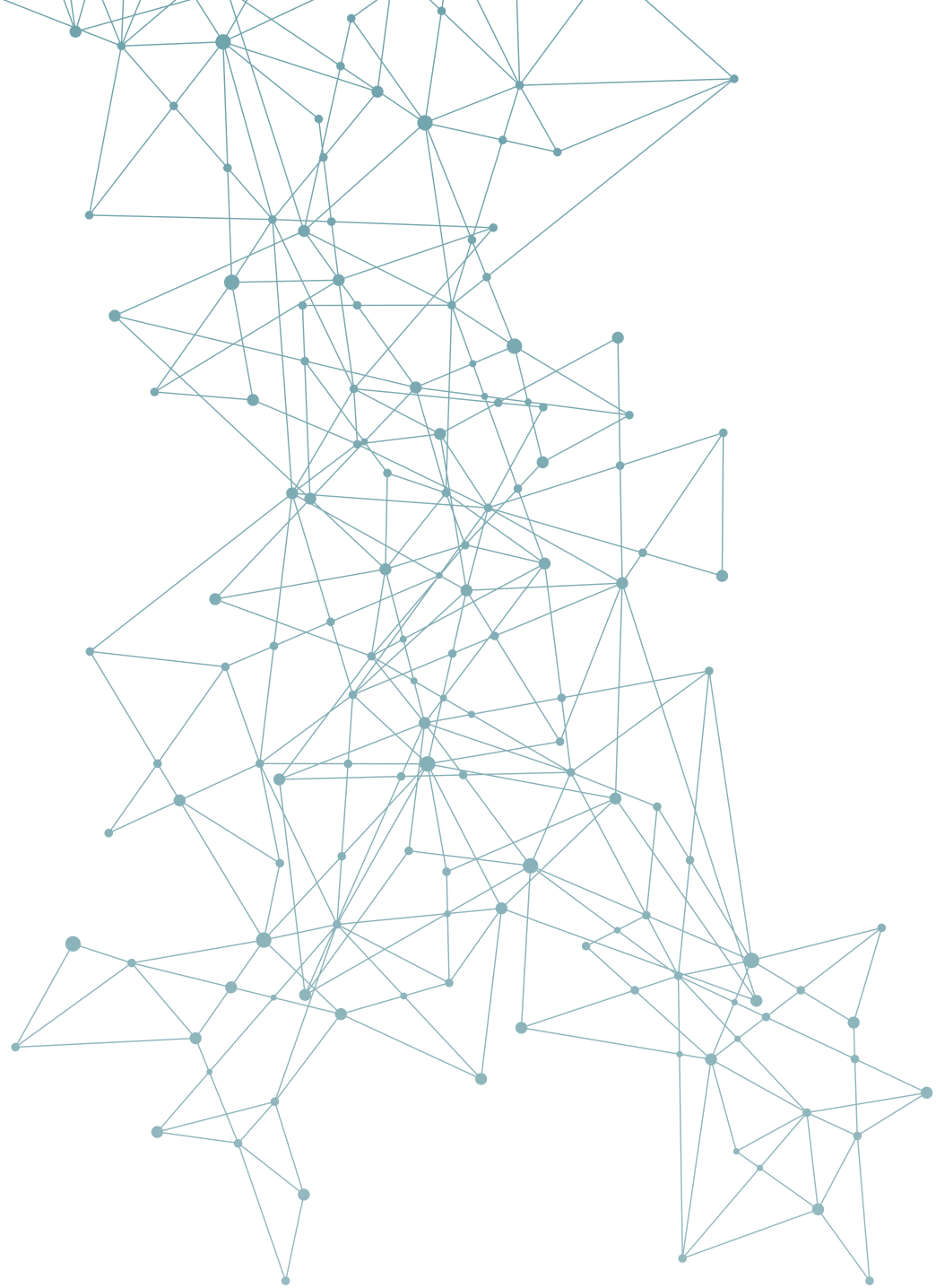
Our sweep indicated that dark patterns were prevalent on the websites and apps of both large and small businesses. Given that small businesses are unlikely to be in a position to develop bespoke websites or apps, off-the-shelf e-commerce products become an attractive alternative to create their online presence. However, small businesses can choose to embed those design features offered within the e-commerce products that are in the interest of their customers.

Small businesses should also consider conducting an audit of their websites and apps and seeing which features could be potentially dropped and which could be amended in a way that they mitigate consumer harm. Small businesses should also reconsider whether their current off-the-shelf e-commerce product is the best option for them when reducing the number of dark patterns on their website. For example, while almost all e-commerce products will include the functionality to request a newsletter or email subscription, small businesses should consider how that is being requested and how and where the consumer data is being stored and whether it is shared with third parties.

Businesses that champion consumer-centric design and abandon dark patterns have the opportunity to publicly portray it as best practice, garner trust from consumers and nudge other businesses to follow suit.

## Where to from here?

This research report on dark patterns provides a high-level insight into the practice and the potential consumer harm in Australia. More research will help to further understand the impact on consumers when engaging with specific industry sectors. As current laws are being reviewed and reconsidered, there's an opportunity to test whether they will adequately address these practices. We welcome the opportunity to work on this issue further with government, regulators, policy makers, academia and the community sector.



## Endnotes


1 Results of the Which? survey are available at: https://consumerinsight.which.co.uk/articles/dark-patterns.

2 Terms and Conditions of Ipsos' Digital Platform can be found here: https://www.ipsos.digital/terms-and-conditions.

3 Stone, D. et. al., "User Interface Design and Evaluation", (2005), The Open University UK., Morgan Kaufmann Publishers.

4 Chugh, B and Jain, P., "Unpacking dark patterns: understanding dark patterns and their implications for consumer protection in the digital economy", (2021), RGNUL Student Research Review, Vol.7(1)., http://rsrr.in/wp-content/uploads/2021/04/UNPACKING-DARK-PATTERNS-UNDERSTANDING-DARK.pdf.

5 Mathur, A and et.al, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites", (2019), Proc. ACM Hum-Comput. Interact. 3, CSCW, Vol. November/Article 81, p. 32, http://dx.doi.org/10.1145/3359183.

6 ACCC, "Advertising and selling guide", (Accessed May 2022), https://www.accc.gov.au/publications/advertising-selling/advertising-and-selling-guide/avoid-misleading-or-deceptive-claims-or-conduct/misleading-or-deceptive-conduct. See also: Australian Consumer Law section 18: https://www.legislation.gov.au/Details/C2013C00620/Html/Volume_3#_Toc368657554.

7 See Australian Consumer Law section 23: https://www.legislation.gov.au/Details/C2013C00620/Html/Volume_3#_Toc368657562 .

8 See Privacy Act 1988: https://www.legislation.gov.au/Details/C2014C00076.

9 CPRC, "Unfair Trading Practices in Digital Market: Evidence and Regulatory Gaps", (March 2021), https://cprc.org.au/publications/unfair-trading-practices-in-digital-market-evidence-and-regulatory-gaps/.

10 OECD, "Roundtable on Dark Commercial Patterns Online – Summary of discussion", (February 2021), https://one.oecd.org/document/DSTI/CP/CPS(2020)23/FINAL/en/pdf.

11 ACCC, "Advertising and selling guide", (Accessed May 2022), https://www.accc.gov.au/publications/advertising-selling/advertising-and-selling-guide/avoid-misleading-or-deceptive-claims-or-conduct/misleading-or-deceptive-conduct.

12 Daly, A., and Scardamaglia, A. "Profiling the Australian Google consumer: Implications of search engine practices for consumer law and policy." Journal of Consumer Policy 40, no. 3 (2017): 299-320.

13 ACMA, "Commercial television industry code of practice 2015", (Accessed May 2022), https://www.acma.gov.au/publications/2019-10/rules/commercial-television-industry-code-practice-2015.

14 Rausch, T.M., and Brand, B.M. "Gotta buy 'em all? Online shopping cart abandonment among new and existing customers", InderScience Online, (February 2022), https://www.inderscienceonline.com/doi/pdf/10.1504/IJEB.2022.121913

15 Gossett, S. "What is Confirmshaming and Why Should You Avoid it?", built-in, (19 January 2022), https://builtin.com/design-ux/confirmshaming.

16 Eagles, Hotel California, Asylum Records, 1976.

17 Norweign Consumer Council, "You can logout, but you can never leave", (January 2021), https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.

18 O'Neill, E, "The experiences of older consumers: towards markets that work for people", Consumer Policy Research Centre, (February 2021), Consumer Data Right Report 1: https://cprc.org.au/consumer-data-right-report-1-stepping-towards-trust-consumer-experience-consumer-data-standards-and-the-consumer-data-right/.

19 Details of the Treasury Laws Amendment (Banking Measures No. 1) Bill 2017 are available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5990

20 Mehta, R. and Zhu, R.J., "Blue or red? Exploring the effect of color on cognitive task performances", (2009), Science, Vol 323, Issue 5918, pp 1226-1229, https://www.science.org/doi/10.1126/science.1169144.

21 Reference re colours in interface design – UX report

22 CPRC, “CPRC 202 Data and Technology Consumer Survey”, (December 2020), https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/.

23 CPRC, “The Digital Checkout”, (December 2021), https://cprc.org.au/the-digital-checkout/.

24 See Australian Privacy Principles: https://www.oaic.gov.au/privacy/australian-privacy-principles.

25 Richmond, B, “A Day in the Life of Data”, CPRC (2019), https://cprc.org.au/research-report-a-day-in-the-life-of-data/.

26 The Ethics Centre, Trust, Legitimacy and the Ethical Foundations of the Market Economy, (2018), 4.

27 European Commission, “Unfair commercial practices directive”, (Accessed 24 May 2022), https://ec.europa.eu/info/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en.

28 European Data Protection Board, “Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them”, (March 2022), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

29 UK Competition and Markets Authority, “Online Choice Architecture: How digital design can harm competition and consumers”, (April 2022), https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers.

30 Federal Trade Commission, “FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions”, (28 October 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions.

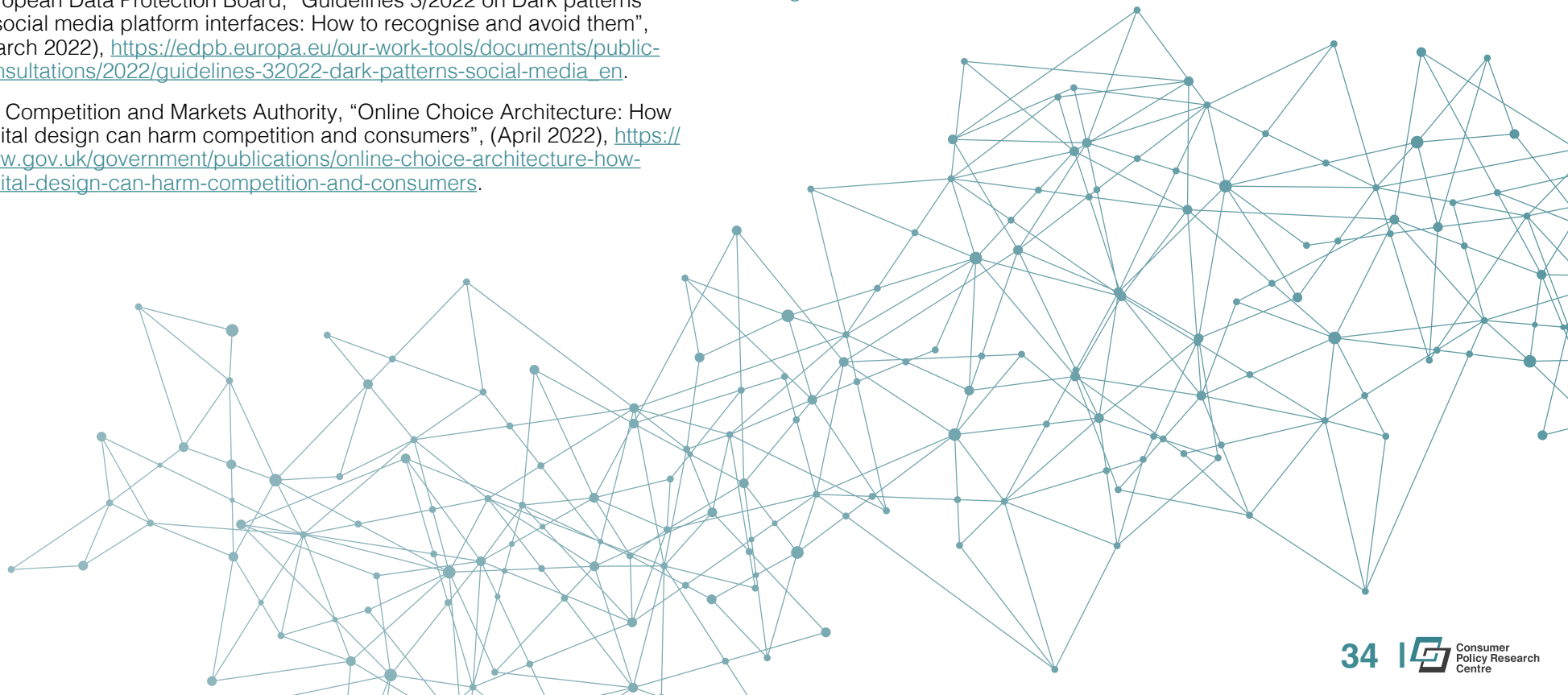
31 Attorney General of California, “Chapter 20. California Consumer Privacy Act Regulations”, (March 2021), https://oag.ca.gov/system/files/attachments/press-docs/CCPA%20March%2015%20Regs.pdf.

32 CPRC, “Unfair Trading Practices in Digital Market: Evidence and Regulatory Gaps”, (March 2021), https://cprc.org.au/publications/unfair-trading-practices-in-digital-market-evidence-and-regulatory-gaps/.

33 ACCC, “Digital platforms inquiry – final report”, (July 2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

34 Attorney-General’s Department, “Privacy Act Review – Discussion Paper”, (October 2021), https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.

35 CPRC, “The Digital Checkout”, (December 2021), https://cprc.org.au/the-digital-checkout/.




Consumer
Policy Research
Centre