MADE TO MANIPULATE

The impact of deceptive online design practices on wellbeing and strategies to mitigate harm

Report by Chandni Gupta, Churchill Fellow 2023
Awarded by The Winston Churchill Memorial Trust

Winston Churchill Trust
Learn globally, inspire locally.

Indemnity Clause

THE WINSTON CHURCHILL MEMORIAL TRUST

Report by Chandni Gupta, Churchill Fellow

2023 Churchill Fellowship

The impact of deceptive online design practices on wellbeing and strategies to mitigate harm

I understand that the Churchill Trust may publish this Report, either in hard copy or on the internet or both, and consent to such publication.

I indemnify the Churchill Trust against any loss, costs or damages it may suffer arising out of any claim or proceedings made against the Trust in respect of or arising out of the publication of any Report submitted to the Trust and which the Trust places on a website for access over the internet.

I also warrant that my final Report is original and does not infringe the copyright of any person, or contain anything which is, or the incorporation of which into the final Report is, actionable for defamation, a breach of any privacy law or obligation, breach of confidence, contempt of court, passing-off or contravention of any other private right or of any law.

Chandni Gupta

07 / 04 / 2025

Acknowledgements

I would like to thank the following incredible people and organisatons I met during my Fellowship for their input, time and advice:

Singapore: Assistant Professor Renwen Zhang, Centre for Trusted Internet and Community, National University of Singapore, Dr Natalie Pang, National University of Singapore, Centre for Trusted Internet and Community, Consumers Association of Singapore (CASE), Competition and Consumer Commission of Singapore, and Nir Eyal

Norway: Datatilsynet, Norwegian Consumer Council (Forbrukerrådet) and SIFO at OsloMet University

The Netherlands: Authority of Consumers & Markets, Dr Cristiana Santos, University of Utrecht, and Dr Amit Zac, University of Amsterdam

United Kingdom: Citizens Advice, Competition and Markets Authority, Harry Brignull, Mozilla, Projects by IF and Which?

Belgium: BEUC, European Commission's Directorate-General for Justice and Consumers (DG JUST), and European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT)

France: Fair Patterns by amurabi, OECD Secretariat for the Committee on Consumer Policy, and UFC-Que Choisir

United States: California Consumer Privacy Act, Consumer Federation of America, Electronic Frontier Foundation, Federal Trade Commission and Future of Privacy Forum.

In addition to the above, soon after completing my Fellowship, I travelled to India where I met about this topic with a tech policy think tank, Pranava Institute, and the Ministry of Consumer Affairs. Given the advancements in India on this topic in the last year, I have also incorporated key insights from those conversations.

The views expressed in this report should not be attributed to the individuals or organisations noted above. I am responsible for the views in this report, including any errors or omissions.

My sincere gratitude to the Winston Churchill Memorial Trust for awarding me this extraordinary, once-in-a-lifetime opportunity to explore deeply a subject that I feel so passionate about.

Thank you to the wonderful team at the Consumer Policy Research Centre (CPRC) for their immense support. In particular, I am deeply grateful to CPRC CEO, Erin Turner, who has supported this journey right since inception, from encouraging me to apply for the Fellowship to creating space and providing the flexibility I needed to take time out from my role at CPRC to dive deep and give it my all for this Fellowship.

Last but certainly not the least, thank you to my beautiful family for their constant support and belief in me – especially my husband, Navneet, and my son Sahil, who are my ultimate cheer squad!

Statement of Recognition

I acknowledge the Traditional Custodians of the lands and waters throughout Australia, in particular the Wurundjeri people of the Kulin nation, the land where I wrote much of this report. I pay my 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.

Suggested citation: Gupta, C., 2025, *Made to Manipulate - The impact of deceptive online design practices on wellbeing and strategies to mitigate harm*, https://www.churchilltrust.com.au/fellow/chandni-gupta-vic-2023.

In the first week of my Churchill Fellowship, I had the opportunity on a beautiful Sunday in Oslo to visit the Nobel Peace Prize Center. This quote from Nelson Mandela struck such a chord with me that I brought it back home and have kept it close as I write this report.

Some ideas in this report may seem far-fetched and certainly a pipe dream for now, but so did many other ideas in the world before they became reality. If we are aspiring towards an online world that is fair, safe and meaningful for all, it will take many pipe dreams to make that happen. All we can do now is work together, whether it's government, businesses or civil society and create pathways that benefit all, not just a select few.

Executive summary

In a world where you can have almost anything delivered to your door in minutes and in your inbox in seconds, it can feel like our world is one of abundance and infinite choice. However, what is this choice costing us? Is this choice just a mirage?

Deceptive and manipulative patterns, also known as dark patterns, are design features embedded into websites and apps to influence our choices, and often not in our best interests. It can be making a subscription process difficult to cancel so you continue paying for what you no longer need or want, pre-ticking boxes so you share more of your data with more companies or embedding a hidden cost through pre-ticked selections in an online checkout. These subtle yet sinister patterns may appear as a mild annoyance in isolation, but their cumulative effect is costing people financially, costing their privacy and degrading their experience online. Australia can no longer continue to ignore these harms.

In just over seven weeks, I had the privilege to travel across seven countries, visiting over 25 organisations/entities and interviewing over 70 people through one-one-one meetings, group workshops and roundtables. What was clearer than ever before is that Australians should no longer have to disproportionately bear the impact of dark patterns and the burden of protecting their own wellbeing online. A fairer choice architecture will need a collective effort that starts with the right laws in place, strong enforcement and stronger incentives to put people over profits.

What needs to change

Here in Australia, we need wellbeing to be at the centre of our consumer protection framework, whether through defining it in law or introducing positive obligations on businesses to account for the mental load that is placed on consumers every day. We need to recognise that to truly achieve wellbeing, people need to have genuine control over their choices and that power is shared in the digital economy and not sitting with just a select few.

The Federal Government must introduce an economy-wide ban on unfair business practices and ensure dark patterns are clearly captured through this prohibition. While a market-wide law is being developed, both State and Federal Governments should introduce an immediate ban on subscription traps, making it illegal for businesses to add more steps to cancel than the number of steps it takes to subscribe. Similar bans could also be imposed on nagging consumers when they have already said no or using language that belittles or degrades them for not choosing the company's preferred option.

We also need strong regulators – regulators that have the power to enforce directly, require businesses to compensate effected consumers and force them to delete data and algorithms that were developed or acquired through deceptive and manipulative practices. To ensure regulators have the capacity to do all this, we need to ensure they are funded proportionately to the market they are overseeing. Some businesses in the digital economy have shown time and time again that they cannot be left to course-correct themselves or self-regulate. Imposing babysitting fees on such businesses, similar to the supervisory fee model that currently exists in Europe could help build regulator capacity to widely and deeply monitor the market and to mitigate widespread consumer harm. This is especially pertinent as deceptive practices move from the visual interface to non-visual and virtual interfaces with support from artificial intelligence.

It is time for Australia to step-up its game and deviate from the pathway that entrenches the practice of dark patterns as the norm. Australians deserve better.

Contents

Introduction

My research into dark patterns at the Consumer Policy Research Centre has found that Australians are losing time, money, control over their data. Ultimately, it is costing them their wellbeing.[1] Dark patterns are pervasive. They are exploiting our vulnerabilities through a cocktail of cognitive biases and information asymmetry to influence us in making decisions that we otherwise would not have intended to make. This deceptive and manipulative practice has become so prevalent online that we are close to hitting the tipping point where we all accept them as the norm of being an online consumer. Fortunately, around the world there are experts, consumer advocates, academics, regulators, government officials and businesses who are working hard to ensure dark patterns don't become a way of life. This Fellowship report is a culmination of my conversations with these incredible individuals and entities.

Through this Fellowship I had the opportunity to meet with experts from Singapore, Norway, The Netherlands, United Kingdom, Belgium, France and United States. Around the world, laws are being introduced to mitigate the impact of dark patterns. Regulators are using innovative approaches to detect dark patterns at scale and taking action against this practice.

Organisations are considering consumer wellbeing through a lens of trustworthy online design and showing others what good practice can look like, considering factors such as emotional stress and cognitive load.

From direct bans on subscription traps and enforcing laws against unfair business practices, to publishing 'good practice' pattern libraries and advocating for better incentives for compliance, there is a shift in the dial towards a fairer, safer online market.

There is a real opportunity right now for Australia to learn from the advancements that are being made around the world and apply it here so Australians too can enjoy the same protections in the digital economy that consumers in other parts of the world now take for granted. We need more businesses designing for fairness, not just for finance. Ultimately, a shift away from deceptive and manipulative patterns can help increase consumer wellbeing and create an online world that Australians enjoy, not endure.

Contact details:

Chandni Gupta
Email: chandni.gupta@cprc.org.au
Churchill Trust website: https://www.churchilltrust.com.au/fellow/chandni-gupta-vic-2023/

Keywords

dark patterns, deceptive design, manipulative design, subscription traps, confirmshaming, forced continuity, choice architecture, UX design, false hierarchy, unfair trading, consumer protection, digital economy

[1] CPRC, 2022, *Duped by design - Manipulative online design: Dark patterns in Australia*, https://cprc.org.au/report/duped-by-design.

Terminology used in this report

- **Dark patterns:** Deceptive and manipulative patterns, also known as dark patterns, are design features embedded into websites and apps to influence people's choices, often not in their best interests. They use a mix of cognitive biases and information asymmetry to influence consumers in making decisions that they otherwise would not have intended to make. The terms are used interchangeably in the report, especially when quoting interviewees.

- **Online choice architecture:** This refers to how options are presented for people on websites or apps to guide them through particular outcomes.

- **UX design:** This is short for User Experience Design and, in this report, refers to the process of planning and creating the experience a user will have when interacting with a website or app.

Types of dark patterns referred in this report:

- **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.

- **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.

- **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.

- **Confirmshaming:** This 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.

- **Forced continuity:** This is a dark pattern which uses complex design features and website navigation in a way that impedes consumers' ability to cancel or move out of a particular service. This is often referred in relation to subscription traps.

- **False hierarchy:** The practice 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.

- **Nagging:** This 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.

- **Data grab:** While the aim of many dark patterns can be to harvest more personal information, this term was coined by Consumer Policy Research Centre to acknowledge the implementation of a collective use of various dark patterns for the sole purpose of collecting more consumer data.

Is it deception or is it just clever marketing?

The term, dark patterns is relatively new (dating back to 2010 when it was initially coined by UX design expert and author of the book Deceptive Patterns, Harry Brignull).[2] However, it is a technique that has existed in some shape and form since the rise of capitalism.

In my conversation, Harry Brignull shared a story of dark patterns in a telecommunication setting back early 2000s. During his work with a UK mobile provider, Brignull found that the voicemail greeting by the provider was incredibly long and could be shortened for an improved customer experience. However, upon being asked to shorten the greeting, the head of the voicemail department at the time outright refused to shift. At a time where calls were charged by seconds, the head stated, "*This is the only money my team makes – through the length of the calls.*" When business metrics are driven only towards achieving a profit, customer experience can suffer. While this shows that profit-seeking manipulative design has existed in some form for a long time, the digital economy has supercharged this practice. It is the volume of, and velocity at, which dark patterns are implemented that has led to its inclusion in enforcement priorities around the world, including Australia.

Governments have codified dark patterns into law and many consumer protection, competition and privacy regulators are implementing new strategies to achieve a market shift away from such practices. However, many experts I interviewed confirmed that despite the exponential implementation of dark patterns, its subtle and secretive nature means that businesses are continuing to get away with it. Many experts including consumer advocates and some regulators confirmed that the line between deception and marketing is becoming more blurred. However, at the same time, many feel that there is now enough known about dark patterns to draw a clear line. That clear line comes from understanding consumer impact, identifying whose interests are being served and exploring how much choice an individual truly has in the online environment – can a person freely take their business somewhere else?

During my conversation with Nir Eyal, author of the books *Hooked – How to build habit forming products*[3] and *Indistractable*,[4] he noted that there is place in our world for positive nudges and persuasion, but not for coercion and that is where he believes dark patterns sit.

> *"Persuasion is helping people do things they want to do... the opposite, coercion, is when we get people to do things they don't want to do, things they will regret later."*
>
> Nir Eyal, Author

Another lens to consider is through asymmetry in both information and power. It is often that consumers may be choice informed, but not choice enabled. The deception sits in the difference between a consumer's preferred choice and a business' preferred choice. Dark patterns can subtly guide users into making choices that benefit businesses rather than themselves.

Tobias Judin, Head of International at Datatilsynet (Norway's Data Protection Authority) shared that businesses that use dark patterns are exploiting their market power. Information overload and the inability to seamlessly untether from a product or service, means that people can become stuck

---

[2] Brignull, H., 2023, *Deceptive Patterns - Exposing the Tricks Tech Companies Use to Control You*, https://www.deceptive.design/book/contents/get-started.
[3] Eyal, N., 2014, *Hooked - How to Build Habit-Forming Products*, https://www.nirandfar.com/hooked.
[4] Eyal, N., 2019, *Indistractable – How to Controle Your Attention and Choose Your Life*, https://www.nirandfar.com/indistractable.

paying for what they don't want or need, have their personal information shared beyond what is required to deliver that product or service to them, and stay on a platform because portability is next to impossible.

"If you are leveraging power imbalances and if people are not front and centre of the [online] design, then it's deceptive."

Tobias Judin, Datatilsynet

The Norwegian Consumer Council (Forbrukerrådet) has pioneered much of the consumer advocacy in the dark patterns space. Speaking to their digital policy experts further confirmed the power asymmetry consumers experience as they shared their thinking on lock-in effects. The team shared three types of lock-in effects[5] that consumers face on a daily basis:

- **Technical lock-in**: Lack of data portability and proprietary tech and standards that are incompatible with other systems or platforms.
- **Service-based lock-in**: Occurs in the form of soft socialisation to mitigate the fear of isolation (i.e. but everyone I know is on that platform). An example of this is when you must use the same platform as your connections to be able to communicate with them due to lack of interoperability.
- **Legal lock-in**: When people are unable to escape terms and conditions that they may not have had the opportunity to appropriately engage with in the first place. This can then be exacerbated when the product or service is licenced instead of owned, hence the inability to modify it in any way.

When such lock-in effects are present, dark patterns thrive. For example, consider the numerous times we are asked to provide our personal information when engaging online. Often this data is required to access a product or a service online but when it is no longer required, ideally it should be erased or at least not be used for purposes beyond the intention of delivering the original product or service. However, in reality, individuals are living in a digital inclusion-exclusion paradox, swinging between the pendulum of needing and wanting to access products and services online, yet often unable to do so without compromising on their privacy.

For many consumers, activating a genuine choice here is no longer an achievable reality. It comes to no surprise then that the results from EU's Digital Fairness Fitness Check from October 2024 revealed that unfair practices, such as the use of dark patterns, are costing EU consumers at least EUR 7.9 billion per year. This is in stark contrast to the cost on businesses to comply with the consumer law which was estimated to not exceed EUR 737 million.[6]

[5] Norwegian Consumer Council (Forbrukerrådet), 2021, *You Can Log Out, But You Can Never Leave – How Amazon manipulates consumers to keep then subscribed to Amazon Prime*, https://storage02.forbrukerradet.no/media/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.
[6] European Commission, 2024, *Commission evaluation shows the benefits and limitations of online consumer protection laws*, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4901.

A wellbeing mindset in consumer protection

Wellbeing as a concept has not traditionally been an underpinning feature in legislation, enforcement or traditional business strategies, though it is starting to be considered in some government budget processes. It is a lens that we may need to include more deeply in consumer protection to truly create an online experience that is fair and safe for digital consumers. Digital wellbeing cannot just be defined by screen time alone, nor can it only be about how much people engage in the digital world. Digital wellbeing should be defined by what that engagement looks and feels like.

"It's not about how much time people spend [on a platform], it's about how they use it... Time is a much lower bar when people are duped out of money."

Nir Eyal, Author

Academics from the National University of Singapore's (NUS) Centre for Trusted Internet and Community have developed a Digital Wellbeing Indicator Framework[7] (Figure 1) featuring 27 different competencies, three of which specifically touch on aspects related to digital consumption (Figure 2):

- **Consumer awareness and literacy**: Ability to access relevant information on products and services including the nous to recognise and evaluate marketing and advertising.
- **Autonomy and data management**: Ability to make transactions that take into account an individual's preferences and being treated fairly by businesses.
- **Consumer rights and competencies**: Access and the ability to assert consumer rights, including access to fair and inexpensive dispute resolution.[8]

However, deceptive and manipulative practices such as dark patterns can erode all these competencies. From being nudged towards options that are not in an individual's best interest to then being unable to seek meaningful help or redress, these can all degrade the online experience and eventually impact wellbeing. One example of this that many experts raised is heavy reliance of consent in how and what data is shared online and with whom. This practice often suggests that there is choice, but that is often a fallacy as the navigation built into the online design fails one to enable it.

[7] Centre for Trusted Internet and Community, *Living Well Digitally*, Last accessed: 14 January 2025, https://ctic.nus.edu.sg/living-well-digitally.
[8] Yue, A., Pang, N., Torres, F., and Mambra, S., 2021, *Developing an Indicator Framework for Digital Wellbeing: Perspectives from Digital Citizenship*, NUS-CTIC Working Paper Series No. 1., https://ctic.nus.edu.sg/resources/CTIC-WP-01(2021).pdf.

Figure 1: NUS domains of digital wellbeing
Source: https://ctic.nus.edu.sg/living-well-digitally/

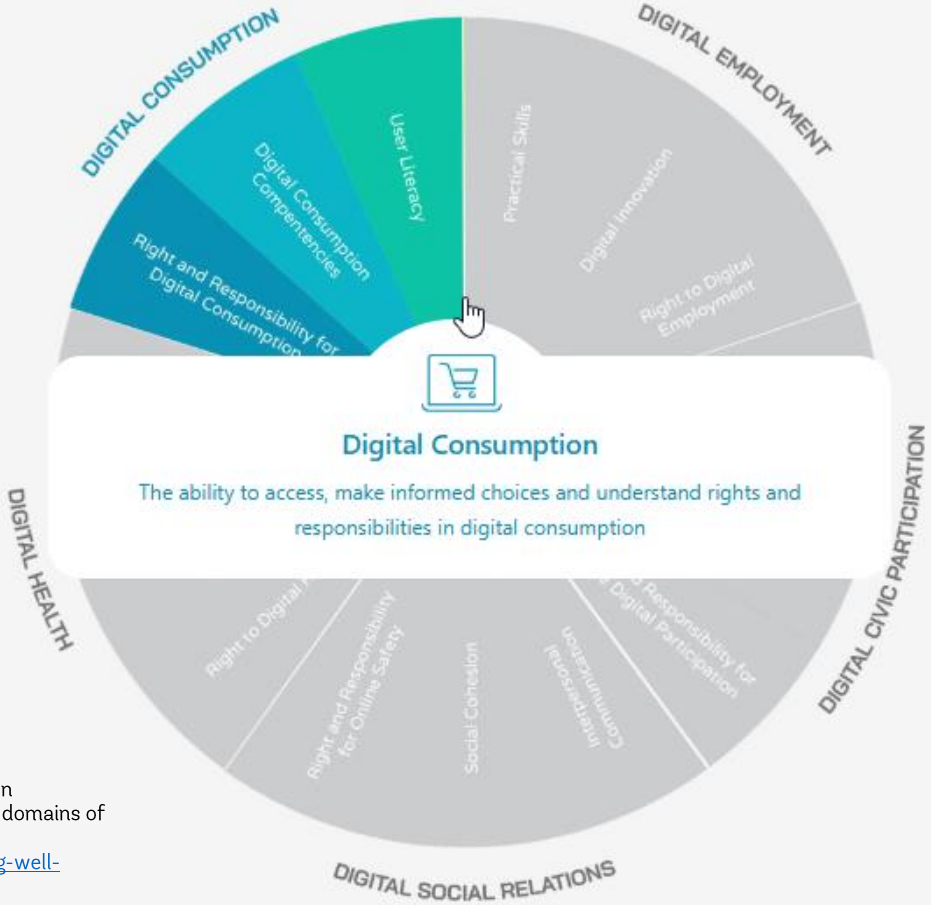


Figure 2: Digital Consumption competencies with the NUS domains of digital wellbeing: https://ctic.nus.edu.sg/living-well-digitally/

When dark patterns such as data-grab, (which can also be layered with false hierarchy and confirmshaming), are overlayed in a consent framework with a dangling carrot to 'access', that offer of choice is, in effect, disingenuous.

"Privacy by consent is grossly inadequate."

Associate Professor Natalie Pang, NUS

NUS academics call for an ecological approach to digital wellbeing, recognising the continuous interdependency between people and the digital systems they interact with. An ecological approach takes into account that there are layers in how we are influenced and that as individuals, we are part of an interconnected network of communities, neighbourhoods and societies. These interconnected networks and our broader surroundings help shape our social norms and wellbeing can be a thread that connects all of this – an overarching guiding principle. Businesses and governments alike can use a wellbeing framework such as the Digital Wellbeing Indicator Framework to create systems, processes and customer journeys that are empathy-driven and consider, not just profitability but also embed a community wellbeing mindset within a business.

Creating trustworthy products and services – a step towards wellbeing

When analysing the NUS Digital Wellbeing Indicator Framework, the word 'assert' is poignant when it comes to accessing consumer rights. To assert, you require confidence and to have confidence, you need trust. Trust plays a critical role for people to confidently navigate the digital economy. Digital wellbeing has the potential to become a positive by-product of a trustworthy relationship between businesses and the communities they serve.

Often the word 'trust' can be found in a company's mission statement, values or policies but operationalising it can be challenging in a world where friction is seen as a key pathway to retention and engagement. In light of this, organisations have emerged to assist others with ingraining trust into their day-to-day operations.

One such organisation is Projects by IF based in London that focuses on building trustworthy systems, particularly in data privacy and AI (artificial intelligence) governance. The organisation's language such as moving organisations away from 'unhappy paths' for their customers is one of hope and empathy. Valerian Adani, Partner at Projects by IF acknowledged that the liminal feeling of trust cannot simply be created at whim, but it can earned.

"You can't make people trust you, but you can design trustworthiness by meeting their expectations."

Valeria Adani, Projects by IF

However, trust is contextual, so unlike other return on investments (ROIs), it is difficult to measure. It is a long-term metric and while it may not be seen as urgent by organisations, Adani emphasises that it's essential for sustainable relationships between people and organisations.

"Many [organisations] treat the work like a band-aid but it should be a vitamin."

Valeria Adani, Projects by IF

Regulation appears to be helping organisations move towards developing more consumer-centric pathways with legal and compliance departments of companies being often the first to reach out. Regulation becomes the catalyst to reflect inwards and then it is up to the organisation to decide whether it wishes to implement the bare minimum and comply or whether it genuinely incorporates trustworthiness in its processes.

One example of an organisation that states to go beyond baseline compliance is the not-for-profit organisation, Mozilla, well-known as the provider of the free web browser, Firefox. Speaking to the

Mozilla team, it was clear that their manifesto, which includes a pledge for a healthy internet and the aim of "*...building a sense of shared humanity*",[9] is not just a statement but is something that is embodied by those within the organisation.

"A browser is a mirror to what people are doing in their lives... we take that responsibility seriously."

Gemma Petrie, Principal Researcher at Mozilla

In particular, Mozilla shared that it utilises a wide range of research methods, from behavioral insights to in-depth qualitative research, to evaluate user experiences. User research helps them assess comprehension, evaluate navigation, and uncover barriers within an online consumer journey. In addition, Mozilla's mission shapes its key performance indicators (KPIs), creating unique incentives for its UX teams compared to those at exclusively profit-driven companies. This becomes a critical business value which enables Mozilla to create for people, not profit.

Trust is not incentivised, revenue is

Many experts that were interviewed as part of this Fellowship raised the issue of power imbalances that exist in many organisations. These power imbalances make it difficult for UX designers to raise concerns with senior leaders of consumer journeys that may cause consumer harm. Experts and advocates relayed that many business models today are focused on KPIs driven towards measurement and engagement, but so few are asking what that system is doing to designers and consumers, and what would be more qualifiable metrics to codify.

Frithjof Michaelsen, EU Policy Lead at the French consumer organisation, UFC-Que Choisir, confirms this factor through his research into gaming development. He notes that, in general, new businesses are motivated less by solving problems or innovating fairly and more by optimising revenue generation.

"We live in a pro-business world. In gaming, businesses are often starting with the agenda to monetise and then they develop a game around it."

Frithjof Michaelsen, UFC-Que Choisir

Several experts also confirmed that in recent years, online design has become less about understanding and meeting customer needs and more about being treated as a production activity.

"Design is being shrunk down to a delivery role – a means to an end."

Harry Brignull, UX Design Expert and Advocate

An example of this on scale is the field experiment run for StubHub, a ticketing company, to test hidden fees through the process of drip pricing. StubHub divided its US customers into two categories: 1) people who saw an all-inclusive pricing, comprising of all fees; and 2) people who only saw the base pricing upfront with other charges such as fees shown at checkout point. The study found that customers in the second cohort spent 21% more on tickets and were 14% more likely to complete the purchase.[10] This experiment was done on millions of US customers, showing the direct line between dark patterns and revenue generation.

---

[9] Mozilla, *The Mozilla Manifesto Addendum - Pledge for a Healthy Internet*, Last accessed: 14 January 2025, https://www.mozilla.org/en-US/about/manifesto.
[10] Foy, M., 2021, *Buyer beware: Massive experiment shows why ticket sellers hit you with last-second fees*, Berkeley Haas, https://newsroom.haas.berkeley.edu/research/buyer-beware-massive-experiment-shows-why-ticket-sellers-hit-you-with-hidden-fees-drip-pricing.

Another example is OECD's dark pattern behavioural experiment in 2024 involving 35,000 individuals across 20 countries.[11] Preliminary results indicate that many of the dark patterns tested were highly effective in influencing consumer decision-making, suggesting they could similarly be effective for businesses in the real world seeking to increase revenue or retain customers. One series of experiment involved people selecting which televisions they would purchase. Television options featuring scarcity cue dark pattern via a countdown timer pared with misleading discount price resulted in a 51% increase in purchases, while nagging to buy an add-on TV wall mount resulted in a 95% increase in purchase of the wall mount.

A second set of experiments then informed participants that they had been automatically signed up to a new streaming service, testing a range of dark patterns as they tried to cancel it. As it is often the case in the real world, the dark patterns were layered throughout the cancellation process, and together they were found to lead to an 88% increase in the acceptance rate.

With uptake statistics like the ones in both studies above, and with little to no incentive to course-correct, businesses are more likely to implement dark patterns to help boost their bottom line.

Another reason why dark patterns thrive is the lack of contestability due to the lack of competition. In a market where processes and systems cannot be challenged and no viable alternatives are available, consumers have no choice but to navigate the path laid out for them (i.e. lock-in effects, as previously discussed). Mozilla recognises that its competitors can create tech barriers that nudge people towards preferential browsers (e.g. Microsoft-enabled products automatically defaulting to Edge browser, Apple to Safari, Google to Chrome) and hence, these competitors capture a larger market share. Essentially, these businesses are being challenged to compete on the competitor's turf.[12] However, company values such as not being purely profit-driven, ensuring interoperability and having a community mindset, means that KPIs for Mozilla developers are likely to have different drivers to other organisations. In that space, trust becomes a unique value proposition.

"Experiencing trust is going to be what we compete on."

Kush Amlani, Mozilla

Currently, however, organisations that pride themselves on bringing social good can be disadvantaged in the marketplace. Other organisations can easily absorb their customers and become larger. One reason for this is that it is difficult for people to discern between businesses they should and should not engage with. Deception is hidden and people do not have the means to say that one company is deceptive while another is not. Even if people can identify them, it can be difficult to move on as businesses use unfair and exploitative tactics such as dark patterns to not just acquire customers but also to retain them, at all costs.

[11] OECD, 2024, *Protecting and empowering consumers in the digital transition*, Issues Note, Consumer Policy Ministerial Meeting, https://cdn-assets.inwink.com/bbf51d8a-98be-4045-bbf0-7906c7d6a676/7cad27fc-5d58-4326-8edd-dfe9015a2386?sv=2018-03-28&sr=b&sig=sEfvNTJApyQYKJtb5F%2BNT0wFUSpJejkWkucg7KXuNoo%3D&se=9999-12-31T23%3A59%3A59Z&sp=r&rscd=inline%3B%20filename%3D%22protecting-and-empowering-consumers-in-the-digital-transition-issues-note.pdf%22.

[12] Brignull, H., and Bowles, C., 2024, *Over The Edge – How Microsoft's Design Tactics Compromise Free Browser Choice*, https://research.mozilla.org/files/2024/01/Over-the-Edge-Report-January-2024.pdf.

Regulating and enforcing dark patterns – no silver bullet

While dark patterns may look the same around the world, they are regulated in diverse ways with some jurisdictions imposing obligations through general prohibitions, others through specific, and many with a combination of both.

Below is a snapshot of many of the key reforms related to dark patterns around the world:

Jurisdictions	Dark pattern obligations
European Union	**Unfair Commercial Practices Directive (UCPD)**[13] including its guidelines specifically calls out dark patterns noting that "*... traders should take appropriate measures to ensure that the design of their interface does not distort the transactional decisions of consumers*".[14] Guidance notes examples of dark patterns include subscription traps, trick questions, and confirmshaming.
	The **Data Act** prohibits dark patterns such as the data-grab noting that third parties, "*...should access only information that is necessary for the provision of the service requested by the user.*"[15] It also prohibits dark patterns overall, noting the following: "*Neither third parties nor data holders should make the exercise of choices or rights by the user unduly difficult, including by offering choices to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a user digital interface or a part thereof. In that context, third parties or data holders should not rely on so-called 'dark patterns' in designing their digital interfaces.*"
	The EU Data Protection Board has also released specific guidelines on deceptive design patterns in social media interfaces[16] under the **General Data Protection Regulation (GDPR)** signalling that dark patterns are prohibited within the social media space.

[13] European Union, *Unfair commercial practices directive*, Last accessed: 10 November 2024, https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en.
[14] European Commission, 2021, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29.
[15] European Union, *Data Act*, Last accessed: 10 November 2024, http://data.europa.eu/eli/reg/2023/2854/oj.
[16] European Data Protection Board, 2023, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

	The **Digital Services Act (DSA)** which came into effect in 2024, specifically calls out dark patterns present on online platforms that include non-neutral, biased choices or make cancellation processes more difficult than the sign-up process.[17] It describes dark patterns 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.*"
	Article 13 of the **Digital Markets Act (DMA)** on anti-circumvention attempts to cover dark patterns for gatekeepers noting that entities cannot, "*...make the make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof*".[18] The Act applies to entities that have been designated as gatekeepers based on their size, control and position in the EU market.[19] Currently the DMA only applies to the following six companies: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft.
	The **EU Artificial Intelligence Act (EU AI Act)**, does not mention dark patterns, however it does state that prohibition of an AI system that, "*...deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm."*[20]
	The **Consumer Rights Directive (CRD)** includes dark patterns and prohibitions relating to cancelling financial services contracts, specifically noting prohibitions on dark patterns that, "*...materially distort or impair, either on purpose or in effect, the ability of consumers who are recipients of the financial service to make autonomous and informed choices or decisions.*"[21]

[17] European Commission, 2024, *Questions and answers on the Digital Services Act**, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.
[18] European Union, *The final text of the Digital Markets Act (DMA) - Article 13, Anti-circumvention*, Last accessed: 10 November 2024, https://www.eu-digital-markets-act.com/Digital_Markets_Act_Article_13.html.
[19] European Commission, 2023, *Questions and answers on the Digital Markets Act: Ensuring fair and open digital markets**, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349.
[20] European Union, Artificial Intelligence Act, Last Accessed: 6 January 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[21] European Commission, *Consumer Right Directive*, Last accessed: 10 November 2024, https://eur-lex.europa.eu/eli/dir/2023/2673/oj

Singapore	While no specific dark pattern legislation exists in Singapore, the jurisdiction does have a law against unfair business practices (**Part 2 Unfair Practices of the Consumer Protection (Fair Trading) Act**). The Act specifically notes the following: "*It is an unfair practice for a supplier, in relation to a consumer transaction —* *(a) to do or say anything, or omit to do or say anything, if as a result a consumer might reasonably be deceived or misled;* *(b) to make a false claim;* *(c) to take advantage of a consumer if the supplier knows or ought reasonably to know that the consumer —* *(i) is not in a position to protect his or her own interests; or* *(ii) is not reasonably able to understand the character, nature, language or effect of the transaction or any matter related to the transaction; or* *(d) without limiting paragraphs (a), (b) and (c), to do anything specified in the Second Schedule.*"[22]
United Kingdom	The **Unfair Trading Regulations 2008**[23] incorporates a general prohibition on unfair business practices, which has been used by the Consumer and Markets Authority (CMA) to enforce against dark patterns.
	While the recently introduced **Digital Markets, Competition and Consumers Act** (DMCC) does not specifically mention dark patterns, it does enable CMA to take direct action against unfair practices, imposing fines of up to 10% of a company's global turnover.[24] The Act specifically applies to tech-based entities with Strategic Market Status (SMS) defined as those with, "*...(a) substantial and entrenched market power, and, (b) a position of strategic significance in respect of the digital activity.*"[25] Statements from the UK Government suggest that subscription traps would certainly be mitigated through the enforcement of the DMCC.[26]
United States* *Note that these protections are accurate as at November 2024 but may be subject to change following the new administration.	While dark patterns are not specifically noted in the **Federal Trade Commission Act** as it has been in force for almost a century, Section 5 of the Act prohibits unfair business practices by defining unfair as causing or likely to cause, "*...substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.*"[27]
	In October 2024, the Federal Trade Commission (FTC) also released the **Click-to-Cancel Rule** under President Biden's Government, which updated

[22] Singapore Government, *Part 2 - Unfair Practices, Singapore Statutes Online*, Last accessed: 10 November 2024, https://sso.agc.gov.sg/Act/CPFTA2003?ProvIds=P12-#pr5-13.
[23] UK Government, *The Consumer Protection from Unfair Trading Regulations 2008*, Last accessed: 10 November 2024, https://www.legislation.gov.uk/uksi/2008/1277/pdfs/uksi_20081277_en.pdf
[24] UK Government, *Digital Markets, Competition and Consumers Act 2024*, Last accessed: 10 November 2024, https://www.legislation.gov.uk/ukpga/2024/13/content.
[25] UK Government, *Chapter 2 – Strategic Market Status of Digital Markets, Competition and Consumers Act 2024, Last accessed: 6 January 2025*, https://www.legislation.gov.uk/ukpga/2024/13/part/1/chapter/2.
[26] UK Government, 2024, *Digital Markets, Competition and Consumers Act receives Royal Assent*, https://www.gov.uk/government/news/digital-markets-competition-and-consumers-act-receives-royal-assent.
[27] United States Government, *Section 5 of Federal Trade Commission Act*, Last accessed: 30 October 2024, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim.

	its already in-force **Negative Option Rule**. The rule requires cancellation to be as easy as the sign-up to a subscription.[28]
	Many states across the US have strengthened their privacy acts to include prohibitions on dark patterns. The **California Consumer Privacy Act** led the charge for other states to follow by banning dark patterns that have, *"...the substantial effect of subverting or impairing a consumer's choice to opt-out".*[29] The obligation applies to practices such as using confusing or persuasive language about why they shouldn't opt-out and forcing users to navigate through unnecessary steps.
India	The Indian Central Consumer Protection Authority has released guidelines banning specific dark patterns.[30] The Reserve Bank of India imposes a positive obligation as an **e-mandate for recurring payments**, including subscriptions. For recurring payments under IND 15,000 (approximately AUD 270), the consumer must be notified 24 hours in advance of the payment taking place. For recurring payments of more than IND 15,000, additional authentication is required to process it, such via a one-time-pin.[31]

A theme across many of the jurisdictions is the reliance on a broad prohibition to tackle dark patterns. In many jurisdictions, a law against unfair business practices has been in place well before dark patterns was a term and, in others, well before the internet was even introduced. Having such a prohibition has meant that as markets and digital experiences evolve, regulators in those jurisdictions have had the power to act against dark patterns. Several regulators and consumer advocates confirmed this by stating that key highlights of an unfair trading prohibition are that the law is both tech and time neutral, and that it applies to all businesses. There are no carve outs, no exemptions.

One such example is the US FTC which, for the past few years, has made enforcement against dark patterns a key priority. It has done this by leaning on the law against unfair practices which was first introduced to the US in the 1930s. In 2022, the FTC reached a settlement of USD 245 million with Epic Games for using a range of dark patterns to, "*charge consumers for virtual merchandise without their express informed consent.*"[32]The following year, the FTC filed a complaint against Amazon for using dark patterns that trick consumers into subscribing to Amazon Prime services.[33] These types of actions are unlikely to be seen in Australia at this stage, given the absence of an unfair trading prohibition.

---

[28] https://www.ftc.gov/news-events/news/press-releases/2024/10/federal-trade-commission-announces-final-click-cancel-rule-making-it-easier-consumers-end-recurring.
[29] Office of the Attorney General, 2021, *Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act*, https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data.
[30] Central Consumer Protection Authority (India), 2023, Guidelines for Prevention and Regulation of Dark Patterns, https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf.
[31] Reserve Bank of India, 2022, *Press Release 2022-2023/335 – Governor's Statement, Section: e-Mandates on Cards for Recurring Payments – Limit Enhancement*, https://www.rbi.org.in/commonman/english/scripts/PressReleases.aspx?Id=3363.
[32] Federal Trade Commission, 2022, *$245 million FTC settlement alleges Fortnite owner Epic Games used digital dark patterns to charge players for unwanted in-game purchases*, https://www.ftc.gov/business-guidance/blog/2022/12/245-million-ftc-settlement-alleges-fortnite-owner-epic-games-used-digital-dark-patterns-charge?utm_source=govdelivery.
[33] Federal Trade Commission, 2023, FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel, https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their.

Limitations in access and reach of dark pattern obligations

While the array of laws combatting dark patterns around the world are impressive when compared to Australia, there are limitations that Australia should be aware of when developing its own laws and regulations against dark patterns.

Limiting scope of laws to specific entities

While the EU has a suite of legislation tackling dark patterns, the Unfair Commercial Practices Directive (UCPD) is the only law that is applicable across the market. The Digital Markets Act (DMA) only applies to six entities and the Digital Services Act (DSA) is specific for digital platforms with additional obligations for a select few that fall under the definition of Very Large Online Platforms (VLOP) or Very Large Online Services (VLOS).[34]

EU consumer advocates note that there are overlaps and contradictions between the laws. They claim, for example, the DSA covers dark patterns that are not covered within the UCPD. Article 5-2 of the DMA has very poignant requirements such as an obligation to not nag an individual for a minimum of one year if they have withdrawn consent for their data to be collected or used by the entity. The DMA also has an obligation for the gatekeeper to ensure that those individuals who have not consented to their data being collected or used but would still like to use the service, the alternative, less personalised service should, *"...not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service."* When it comes to withdrawing consent, the obligation clearly states that it should not be more difficult to withdraw consent than to provide it in the first place.[35]

Ideally, all businesses in the EU should be complying with such obligations. Yet, at present, these explicit obligations have only been applied to the six organisations that are classified as gatekeepers within the EU along with a similar obligation in the DSA for online platforms.

The same can be observed in the UK's Digital Markets, Competition and Consumers Act which applies to only those that are identified as Strategic Market Status (SMS) entities while its *Unfair Trading Regulations 2008* applies market-wide. Representatives from UK-based consumer organisations, Which? and Citizens Advice, noted that the SMS definition is likely to only be applicable to a select few businesses and that the DMCC exempts both the telecommunication sector and the utilities sector. Australia should avoid creating protections that are applied too narrowly and are not responsive to new market players.

Limiting application of laws to business-to-consumer products and services only

An issue that many experts and advocates in the EU raised was that while dark patterns are present on websites and apps, many of those businesses are using very similar content management or consent management platforms. However, speaking to regulators and advocates, there is a lack of clarity as to whether current laws would apply to B2B facilitators such as e-commerce platforms, online marketing firms or software suppliers, including those that impact consumer experience.

---

[34] European Commission, *DSA: Very large online platforms and search engines*, Last accessed: 26 October 2024, https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.
[35] European Commission, *Digital Markets Act*, Last accessed: 11 January 2025, https://ec.europa.eu/competition/digital_markets_act/cases/202417/DMA_100055_135.pdf.

For example, it was unclear whether a content management platform such as Shopify, used by many small businesses to create e-commerce websites, would be captured by some of the dark pattern obligations. In the EU, it appeared that the DSA may apply to them but when it came to the UCPD, if a dark pattern was found on a website that used Shopify to create its e-commerce platform, the enforcement action would be taken against the business, and unlikely on the content management platform.

The same appears to be the case for consent management platforms, though GDPR does appear to apply to such platforms. Dr Cristiana Santos, Assistant Professor at the Utrecht University in The Netherlands, has raised the issue of consent management platforms and the lack of obligations and enforcement that exist against them across several publications.[36] For example, Dr Santos notes that there are, perhaps, approximately only a handful of main consent management platforms that service most of the online interfaces that consumers interact with.

> *"Consent Management Platforms manipulate data collection. They are captured by the law, but they are not being enforced and there is no willingness to do so."*
>
> Dr Cristiana Santos, Utrecht University

It appears to be a lost opportunity to potentially course-correct the market at scale, given the architecture behind an online interface can act as a building block for a more consumer-centric online experience overall.

Limiting the scope of who can be protected from harm

Both the UK and the EU in their respective laws against unfair practices refer to the 'average consumer'. In the EU specifically, it states that an average consumer is, "*…reasonably well informed and reasonably observant and circumspect*". This approach leaves much of the interpretation to courts which has not always been consistent. In November 2024, the Court of Justice of the European Union (EU) clarified the definition further, noting that cognitive biases have the potential to influence decision-making.[37] In an online world where information asymmetry and risk of experiencing vulnerability is high, the concept becomes even less fit for purpose. The newly established DMCC adds a qualifier of 'vulnerability' to its average consumer definition, but consumer advocates foresee that there may be issues with enforcing it. Australia should not constrain any laws to a theoretical concept of a consumer.

Creating space for grey by remaining silent on key aspects

One aspect that some experts and advocates raised was when guidance on laws and regulations is detailed across many key aspects but remains silent on other issues, causing inconsistencies in multi-jurisdictional enforcement and business interpretation. One such example is guidance from the European Data Protection Board on cookie banners. Whilst the guidance provides detailed nuances on requirements of pre-ticked boxes, it is silent on other details, such as the colour of "Accept all" and "Reject all" buttons, except noting that there is a need for contrast that is not misleading. The guidance specifically notes this in its deceptive button colours and contrast section, stating that, "*…cookie banners need to be assessed on a case-by-case basis*".[38]

---

[36] Santos, C., Nouwens, M., Toth, M., Bielova, N., Roca, V., 2021, *Consent Management Platforms Under the GDPR: Processors and/or Controllers?,* Privacy Technologies and Policy, http://dx.doi.org/10.2139/ssrn.4205933.
[37] European Union Judgement of Court, 2024, *Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (AGCM),* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0646.
[38] European Data Protection Board, 2023, *Report of the work undertaken by the Cookie Banner Taskforce,* https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

Various experts noted that it appears that the members of the EDPB were unable to reach a unanimous decision when it came to the button colours. Hence, they may have leant towards a case-by-case approach, ultimately leaving the decision to individual Data Protection Authorities. However, this has led to inconsistencies in how choice is displayed on cookie banners across Europe and how the consent buttons are enforced. Dr Santos draws on the example where jurisdictions consider that a 'red' colour should donate 'only necessary cookies', while other jurisdictions such as Belgium have noted that a red or dark colour should be used for 'accept all'.[39]

"These inconsistencies create nothing short of a soap opera."

Dr Cristiana Santos, Utrecht University

Consumer regulators have also noted that inconsistent guidance or lack thereof can lead to regulatory arbitrage. Some regulators shared that it was not uncommon for businesses, upon meeting with the regulator, to state that they just need to know the grey space where they can play. This further confirms that some businesses are continuously looking to play around the edges of compliance, pushing the limits of fairness, especially in laws that have no ex-ante obligations. Consumer experience, wellbeing and meaningful choice are concepts far down the priority list for those businesses.

Limiting course-correction through minimal enforcement

Complex and tiered enforcement hierarchies can make it difficult for enforcement action to have a widespread effect. As an example, within the UCPD in the EU, enforcement action can only be taken at the national level and not by the European Commission (EC). Due to the subsidiarity nature of the UCPD, the EC can only play the role of a negotiator with the non-compliant business to achieve EU-wide course-correction. In 2021, the EC negotiated with Amazon to have its cancellation process to Prime simplified and reduced to just two steps.[40] This occurred after consumer organisations around the EU came together to make a complaint that Amazon's cancellation process breached the UCPD.[41] While Amazon did correct its process, it was not fined, despite breaching the law for several years. Businesses that have significant market power will only course-correct when they are caught out or are pressured to do so.

Advocates, experts and even regulators have noted this limitation as barrier to utilising UCPD powers to their fullest. While there is the Consumer Protection Cooperation (CPC) network that brings together regulators across EU, many raised that due to the limited enforcement regime, the network is unable to jointly impose sanctions.

This barrier was also recognised through the EU's Digital Fitness Check, the results of which were released in October 2024.[42]

"It is cumbersome to go from investigation to sanctions because sanctions can only be at country -level. Businesses need a deterrent; there is no real risk at the moment".

Egelyn Braun, EU Official at European Commission

---

[39] Santos, C., Gray, C., Bielova, N., and Ahuja, S., 2024, *Usable and Lawful: Can Consent be Both?*, https://ssrn.com/abstract=4961361 or http://dx.doi.org/10.2139/ssrn.4961361.

[40] European Commission, 2022, *Consumer protection: Amazon Prime changes its cancellation practices to comply with EU consumer rules*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_4186/IP_22_4186_EN.pdf

[41] Norwegian Consumer Council (Forbrukerrådet), 2022, *Amazon makes it easier to cancel Prime following complaints from European consumer organisations*, https://www.forbrukerradet.no/siste-nytt/amazon-makes-it-easier-to-cancel-prime-following-complaints-from-european-consumer-organisations.

[42] European Commission, 2024, *Review of EU consumer law*, https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en.

With many of the smaller regulators not having the resources or capacity to pursue enforcement, it can leave a significant gap for some businesses to exploit. The UCPD includes the ability for businesses to be fined up to 4% of its global turnover but that is something still yet to be seen. The Fitness Check confirmed that while laws have existed, enforcement has been severely lacking.

This is similarly the case in the UK which also has a tiered regulatory approach. Fair trading is split even further – not even at a city level but even narrower at a borough level, often with only a handful of people working in fair trading in each borough. Enforcing the law on multi-national cooperations is not only difficult, but next to impossible for fair trading offices.

Within the US, while the FTC has been seen as an effective regulator, privacy advocates in the US have raised concerns about the limited enforcement that has taken place on dark pattern related obligations under the privacy acts. For example, in California, the CCPA includes obligations on businesses to ensure that steps that a consumer needs to take to opt-out of data sharing cannot be harder than the steps to opt-in. While the intention is to provide symmetry of choice to consumers, advocates have noted that the lack of enforcement has meant that many such obligations have not been adequately tested.

"If you don't give laws teeth, then it is just pretty words."

Hayley Tsukayama, Associate Director of Legislative Activism, Electronic Frontier Foundation

Privacy experts noted that in some cases, it is not the law, but the lawsuits that are helping to change business behaviour.

"Class actions have the ability to significantly disrupt the market".

Lee Matheson, Deputy Director for Global Privacy, Future of Privacy Forum

The team at Future of Privacy Forum also noted the changing political landscape where federal agencies have less authority over time. Where once Chevron deference may have been widely used, with courts deferring to an agency's interpretation, more decisions are being made by court.

Addressing limitations through innovative law and enforcement strategies

Fortunately, many of the limitations noted in the previous section are actively being addressed by governments and regulators in ways that can lead to meaningful change for consumers.

Direct fines

Traditionally, enforcing laws has meant that regulators investigate and then the matter is presented in court. For many laws, this has meant that enforcement becomes an expensive exercise with long lead times and no real incentive for the business to course-correct until it is absolutely necessary. However, new laws such as the DSA in the EU and the DMCC in the UK, enable regulators to fine directly. In the EU, this includes fines of up to 6% of global revenue and in the UK, the DMCC enables CMA to directly impose fines of up to 10% of the global revenue or GBP 300,000 (whichever is higher).[43] These penalties can also be applied when a business fails to provide information to the regulator, such as results of A/B testing of the product's online choice architecture.

Enforcing with a problem-solving mindset

Regulators that have led the way in mitigating the use of dark patterns appear to have a mindset that goes beyond merely achieving compliance in the marketplace. One such example is the Authority of Consumers and Markets (ACM) in the Netherlands. Speaking to the team there, it was clear that investigations are taken up, not primarily due to potential judicial outcomes, but on what will create systemic change. The goal in such an agency is to solve a problem for its citizens.

> *"We are willing to be the vanguard. If we can explain why we lost, we are creating an opportunity for change."*
>
> Dries Cuijpers, Senior Enforcement Official, ACM

ACM has a dedicated behavioural insights team that is integrated into its enforcement program. The use of behavioural economics has helped them to unpack terms such as the 'average consumer'.

To illustrate, the team noted that the term, 'average consumer' can be limiting given the narrow definition that pre-dates the internet. However, ACM's behavioural expertise has been key for the agency in better understanding the negative effects of dark patterns on consumers. Use of behavioural economics has been instrumental in providing the evidence for those effects in concrete enforcement cases.

This is important as products offered to consumers are no longer just sitting on a shelf in a local store, sold through a local merchant. In a pre-online world, when definitions for terms such as the average consumer were initially developed, information disclosure at the point of sale could have been held as an adequate standard in ensuring a consumer could make a rational decision. However, in today's online world, there can be limitations to this rationality due to information overload, time-

[43] European Commission, 2024, *Questions and answers on the Digital Services Act**, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348. UK Government, *Digital Markets, Competition and Consumers Act 2024*, Last accessed: 10 November 2024, https://www.legislation.gov.uk/ukpga/2024/13/content.

bound decision points (further exacerbated through scarcity cues) and the complexity in how disclosures are presented. In a such an environment, is it truly possible to make choices freely?

It is this thinking that has led to ACM developing an in-house, automated dark pattern detection tool for misleading countdown timers. This enabled ACM to conduct a crawl on 30,000 websites, a number that would be physically impossible and in fact economically impractical for a regulator to conduct manually. The investigation led to significant media coverage and opened the door for ACM to directly engage with non-compliant businesses and those businesses who may have been playing in the grey.[44]

Another example is the Norway's Data Protection Authority, Datatilsynet, which, in September 2023, won its case against Meta for unlawfully engaging in behavioural marketing.[45] The case was then raised with the European Data Protection Board (EDPB) before the temporary ban expired in Norway, the EDPB extended a permanent ban across EU and the European Economic Area covering all 30 countries.[46] These outcomes can truly only occur if enforcement agencies are willing to look outside of the box and pursue solutions that help bring broader change, far wider than their own jurisdictions.

Introducing pre-emptive obligations

While laws in other sectors may have upfront obligations, many relating to consumer protection tend not to. This means enforcement often takes place after the fact and, at times, when widespread harm has already occurred. The DSA in the EU is a shapeshifter in that regard, requiring designated entities to proactively assess risk of manipulation and provide access to relevant data to authorities and researchers to aid in understanding the impact of the platform on its users and to help mitigate any systemic risks early. Entities are also required to conduct independent audits to ensure they are complying with their DSA obligations. If entities do not comply with their commitments, then limitations can be placed on the business for up to five years.

The DSA is still relatively new, and consumer organisations note that its impact will likely be seen over the coming years. However, the European Commission officials noted that they have already started to see a positive shift. There are already several information requests and investigations that have been made under the DSA, all of which are published on the European Commission's digital strategy website.[47] In January 2024, the Commission sent its periodic public request to all designated entities to show how they comply with the DSA.[48] It was through these submissions that non-compliance was identified across several entities, including LinkedIn which, as a result, by June 2024 fully disabled the functionality that allows, "*...advertisers to target LinkedIn users with ads on the basis of their membership in LinkedIn Groups in the EU Single Market.*"[49] While the LinkedIn example also involved a complaint from civil society organisations in February 2024, the power of the regulator to act quickly was supercharged because of the proactive obligations of transparency and reporting placed on LinkedIn through the DSA.

---

[44] Authority of Consumers & Markets, 2023, *ACM confronts online stores using misleading countdown timers with their practices*, https://www.acm.nl/en/publications/acm-confronts-online-stores-using-misleading-countdown-timers-their-practices.
[45] Datatilsynet, 2023, *The Norwegian Data Protection Authority won against Meta in Oslo District Court (in Norwegian)*, https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/datatilsynet-vant-i-oslo-tingrett.
[46] Datatilsynet, 2023, *The Norwegian Data Protection Authority's decision against Meta is extended to the EU/EEA and made permanent*, https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/the-norwegian-data-protection-authoritys-decision-against-meta-is-extended-to-the-eueea-and-made-permanent.
[47] European Commission, *Supervision of the designated very large online platforms and search engines under DSA*, Last accessed: 9 February 2025, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.
[48] European Commission, 2024, *Commission sends requests for information to 17 Very Large Online Platforms and Search Engines under the Digital Services Act*, https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under.
[49] European Commission, 2024, *Statement by Commissioner Breton on steps announced by LinkedIn to comply with DSA provisions on targeted advertisement*, https://digital-strategy.ec.europa.eu/en/news/statement-commissioner-breton-steps-announced-linkedin-comply-dsa-provisions-targeted-advertisement.

EC representatives also noted that the Commission was investing in in-house surveillance and will be commissioning a five-year study to help monitor the market for compliance. The significant resources assigned to enforce the DSA is all credit to Article 43 of the DSA which requires designated entities under DSA to pay an annual supervisory fee.[50] This model means that governments have a fighting chance to place resources where needed to effectively monitor entities that hold significant market power.

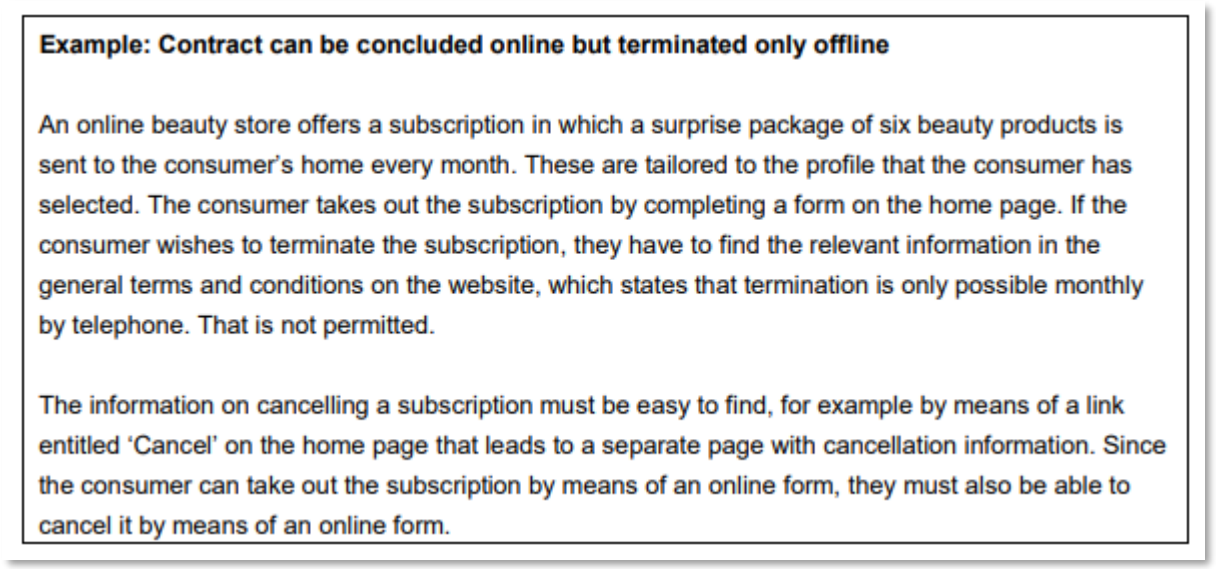
Supporting prohibitions through clear guidance

Given the breadth of the market that many dark pattern laws apply to, the legal framework alone is insufficient to drive compliance, especially for small businesses who may not be able to afford the level of legal support that larger businesses can access. This is where guidance from government and/or regulators helps add clarity to the obligations.

"Small businesses are disadvantaged in the marketplace—compliance is a grey area."

Harry Brignull, UX Design Expert and Advocate

ACM's guidance on online consumer protection[51] is an example of how a regulator can help provide certainty on compliance with clarity and being upfront on what it, as a regulator, will consider as non-compliant. The guidance is clear, contains practical, concrete examples and is easy-to-read, being absent of legalese content (Figure 3).



Example: Contract can be concluded online but terminated only offline

An online beauty store offers a subscription in which a surprise package of six beauty products is sent to the consumer's home every month. These are tailored to the profile that the consumer has selected. The consumer takes out the subscription by completing a form on the home page. If the consumer wishes to terminate the subscription, they have to find the relevant information in the general terms and conditions on the website, which states that termination is only possible monthly by telephone. That is not permitted.

The information on cancelling a subscription must be easy to find, for example by means of a link entitled 'Cancel' on the home page that leads to a separate page with cancellation information. Since the consumer can take out the subscription by means of an online form, they must also be able to cancel it by means of an online form.

Figure 3: One of the examples in the ACM guidelines Protection of the online consumer – Boundaries of online persuasion

Several experts propose that clear guidance from regulators can become an effective deterrent for non-compliance, with some suggesting that guidelines can be seen as 'soft law'. While regulators state a clear demarcation between law and guidance, a sign of good guidance can lead to enabling a market to self-correct, avoiding enforcement action.

[50] European Union, *Digital Services Act*, Last accessed: 26 October 2024, http://data.europa.eu/eli/reg/2022/2065/oj.
[51] Authority of Consumers & Markets, 2024, *Bescherming Online Consument – Grenzen aan online beïnvloeding: Voorkom misleiding in een online omgeving (Protection of the online consumer - Boundaries of online persuasion)*, https://www.acm.nl/system/files/documents/leidraad-bescherming-online-consument.pdf (in Dutch) (NB: the screenshot above is from a previous English-translated version).

Redress

A key part of an effective consumer protection framework is access to redress when things go wrong. While regulators, academics and consumer organisations confirmed that it is rare to receive complaints on dark patterns, there was unanimous agreement that if harm has occurred, especially financial, consumers should have access to appropriate remedies.

"Redress goes beyond being compensated. It is also about ensuring people feel safe raising a complaint and genuinely feel their voice is being heard."

Assistant Professor Renwen Zhang, NUS

In the US, FTC settlements with non-compliant businesses often include reimbursement of some form for affected consumers. These reimbursements are managed directly by FTC where FTC establishes a platform for impacted consumers to reach out directly and seek compensation. For example, in the settlement case with Epic Games (previously mentioned), Former FTC Director, Samuel Levine, noted that the significant proportion of the settlement was to help account for compensation back to consumers.

"Redress should help make people whole. It's critical for compensating consumers for the time and money they've lost, and for ensuring lawbreaking isn't profitable is important to get money back into the consumer's pocket."

Former Director for Bureau of Consumer Protection, FTC

While laws can help prevent harm from occurring in the first place, in the instances harm does occur, having an accessible redress framework is critical for effective consumer protection.

Another example of effective redress is the one delivered by consumer organisation, CASE, in Singapore. Consumers can raise consumer affairs related complaints directly with CASE. Once the organisation has reviewed the complaint, it negotiates with the associated company on behalf of the consumer. Mediation can take place face-to-face or online and is designed to achieve an outcome that is fair for the consumer.

Assistant Director for Consumer Relations at CASE, Wilfred Ang, noted that it takes an average of one to three months for a complaint to be resolved. When complaints are unable to be resolved by CASE, consumers have the choice to escalate their matter to the Singapore's Small Claims Tribunals for a legal decision if it falls within their jurisdiction. While timing is dependent on availability of the tribunal, most cases resolve in under three months. This is a far cry from tribunal cases in Australia which can take up to several years for cases to resolve. Insights from complaints are also directly shared with the regulator, the Competition and Consumer Commission of Singapore (CCCS), to help identify trends and possible cases for further investigation. There is a mutually respected relationship between the CASE and the regulator; one that has been built on a mindset of efficiency.

In addition to local redress initiatives, Singaporean consumers also have access to a multi-lateral consumer redress program. As a physical office of the businesses is needed within Singapore for CASE to be able help resolve a consumer complaint, the cross-border framework across nine countries in Asia enables consumers to seek remedies from suppliers based outside of Singapore. Such innovative approaches means that redress becomes more of a reality than a ruse.

Accounting for wellbeing in consumer protection

Wellbeing, as a concept within the consumer protection ecosystem, has not traditionally been prioritised as an outcome for government or industry. In conversation with the team at the European consumer organisation, BEUC, it was clear that in traditional enforcement models, it can be difficult to prove that a practice has directly impacted a person's wellbeing.

> *"Consumer law was developed with only the economic interest of consumers."*
>
> Agustin Reyna, Director-General of BEUC

However, there is hope, as language within consumer policy is shifting and emotional and psychological harms are slowly being considered. The most notable one being the inaugural OECD Ministerial on Consumer Policy held in Paris in October 2024. Bringing together over 40 consumer affairs delegations from around the world (including Australia), they together released a declaration on protecting and empowering consumers through the digital and green transition.[52] The commitments within the declaration had a clear focus on wellbeing, noting that it become a priority for both businesses and government policy. The declaration also included references to the impact on mental health and recognised that practices such as deceptive and manipulative practices online can lead to consequences that are "*…serious and far-reaching, resulting in substantial and wide-ranging consumer harm, including direct financial loss, erosion of privacy and physical and psychological harm, including addiction*". How the commitments within the declaration are implemented is yet to be seen but it is a positive development at an international level to put wellbeing in consumer policy as an actionable outcome.

There are now examples from other jurisdictions where wellbeing is being considered as part of enforcement. In March 2024, the Italian Competition Authority fined TikTok EUR 10 Million for infiltrating users with videos that are likely to harm an individual's "*…psycho physical safety*".[53] The content was related to TikTok Lite, a rewards program that incentivises users to create specific content in return for rewards. The functionality was subsequently banned from across the EU.[54]

The wellbeing and vulnerability nexus

One way the concept of wellbeing could be socialised within the consumer protection framework is possibly through the lens of widespread vulnerability. Traditionally, vulnerability has been proxied through a set of demographics, often categorising specific communities as vulnerable. However, in the digital economy, vulnerability has a much more fluid state.

In 2023, Dr Amit Zac from the University of Amsterdam led experimental research to study the effects of dark patterns on consumers. The research found that when it comes to exposure to dark patterns, lower-income consumers are no more susceptible to dark patterns than other cohorts. Generally, consumers across all groups tested were found to be susceptible to dark patterns.

---

[52] OECD, 2024, *Declaration on Protecting and Empowering Consumers in the Digital and Green Transitions*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0504.
[53] Italian Competition Authority, 2024, *PS12543 - TikTok Sanctioned for an Unfair Commercial Practice*, https://en.agcm.it/en/media/press-releases/2024/3/PS12543.
[54] European Commission, 2024, *TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act*, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161.

"Vulnerability is far more contextual."

Dr Amit Zac, University of Amsterdam

Considering vulnerability in the equation of wellbeing may help to decipher the extent of harm caused by dark patterns. It is not the case that a select group of people are vulnerable, but that dark patterns are exposing vulnerabilities in all of us, adding to our mental load.

Correlation over causation

Some experts and advocates also noted that, when it comes to deceptive and manipulative design, it is difficult to identify the chain effect of harms, in particular impacts on wellbeing. The chain effect of harms is where wellbeing may not be the direct harm incurred, but other harms such as time impost, loss of money, loss of control over privacy combined can exacerbate the mental load on consumers. However, consumers will rarely raise this as a complaint with many consumer organisations noting that they rarely, if at all, receive complaints directly relating to dark patterns, given the subtle and hidden nature of the practice. This is specifically the case for privacy related harms which may feel far removed from the person who has been impacted.

"Privacy is intangible, so people don't complain."

Hayley Tsukayama, Electronic Frontier Foundation

When consumers recognise that they have experienced harm, they either cannot identify the direct cause, or they feel shame for perceiving that they have caused harm to themselves. Several experts referred to this as an accumulative effect of harms which can cause strain on the mental load. Unfortunately, this is one area that has not been taken seriously within enforcement strategies.

"There's the cascade effect or the cumulative effect. Both are hard to study and both are difficult to regulate but immensely problematic."

Dag Slettemeås, SIFO/OsloMet

One way around this is for regulators to look beyond direct causation and consider correlation as part of their investigations and enforcement strategies.

"Finding causation is difficult. The burden of proof sits with consumers."

Finn Lützow-Holm Myrstad, Norwegian Consumer Council

By broadening the focus to correlation, it can help account for the subtlety and secrecy of dark patterns and place the onus on the business to show that the choice architecture is fair and that they have considered their customers' best-interest.

Emerging harms – dynamic and in the dark

Many of the experts interviewed during this Fellowship raised their concerns about dark patterns being supercharged with the help of artificial intelligence (AI). Pinpointing individuals at their weakest point through AI to tap into when they may be at their most vulnerable is not a momentary suspension of disbelief by experts but a tactic that is likely to be widespread in the not-so-distant future. One example is of the AI-enabled chatbot Replika AI, which nudged in-app purchases through dark patterns such as confirmshaming with statements such as "*If you love me, buy me this*". These nudges were deliberately programmed into the application.

"It [Replika AI] leveraged emotional connections."

Associate Professor Natalie Pang, NUS

How people engage in searching for information is evolving and thus can give rise to dark patterns in a way that we are yet to see the full effect. For example, in a simple 'Google search' people know what to look for (e.g. sponsored tags, clear URLs noting source of content). However, the same search conducted within Generative AI means sponsored content, sources and other markers to validate a level of accuracy of and trust in the information are, in effect, absent. Director of the Consumer Protection Division at the CCCS, Ng Ming Jie, noted that the loss of consumer trust in information online can erode the consumer experience in the digital space and make it difficult for consumers to make informed and independent decisions.

"AI used in a wrong way can further tilt the information asymmetry against consumers online, making it difficult for consumers to spot any trick used to mislead them and to choose which online sellers to trust."

Ming Jie Ng, Director, CCCS

To date, dark patterns that can be confidently identified and have been codified into law are all static in nature; however, within AI-enabled choice architecture or non-visual choice architecture (e.g. voice-enabled products and services), dark patterns will not only be more difficult to identify but also more difficult to enforce.

"AI is becoming supercharged... both in personalisation and in persuasion"

Dag Slettemeås, Researcher, SIFO/OsloMet

"There are the dark patterns we see and then there are the dark patterns that are built-in."

Finn Lützow-Holm Myrstad, Director of Digital Policy, Norwegian Consumer Council

This becomes even more problematic in immersive technologies where dark patterns can be particularly subtle due to the blurring lines between the real and virtual worlds. From a privacy perspective, Deputy Director for US Policy at Future of Privacy Forum, Jameson Spivack, shared how in a virtual setting, data can be collected simply based on where you look and how long your eye gaze lingers at a particular part of the virtual world. The data can then infer interests, preferences, sexual orientation and even preferred language. Suddenly, privacy protections that are built on consent flows would be rendered obsolete.

"It [immersive technology] is creating a virtual space that reveals so many other data points."

Jameson Spivack, Future of Privacy Forum

Another practice that supercharges the notion of subtlety and opacity are algorithmic harms, which are known to be present but are often difficult to identify. Layering dark patterns within an algorithm, especially to enable it pinpoint when a particular dark pattern may be best deployed will likely exacerbate emotional harm and could severely impact wellbeing. Several experts and advocates noted algorithmic bias is still not measured to the same standard as bias in other settings.

"Definition of discrimination via algorithms has a lower threshold than the general definition of discrimination."

Hayley Tsukayama, Electronic Frontier Foundation

Many experts noted that if AI development fails to account for dark patterns before and after training the model, dark patterns will be embedded into the system's standard response. AI and algorithmic harms (e.g., hidden biases, exploitative data scraping) will require forensic methods to investigate. It will be essential for regulators to have access to proprietary algorithms and related data sets to truly have visibility of the impact such evolutions in technology may have on consumers.

Pivoting the patterns – recommendations for change

The Fellowship showed that there is certainly a way forward where dark patterns can be mitigated, and people's wellbeing can be put front and centre. This will require a shift in challenging the status quo and, where possible, codifying wellbeing into investigations, enforcement, redress and more. Below are key recommendations for Government and businesses to implement.

Make space for wellbeing in law and enforcement

Financial loss cannot remain the single indicator of harm. In the digital economy, where people are interacting online and accessing a myriad of products and services in just one day, we need to account for the mental load. Governments need to consider how wellbeing can be an obligation that businesses are required to meet. There is rhetoric that it will be difficult to define wellbeing but that does not mean that we should not try. It will take a concerted effort by governments, businesses and civil society but it is one that is possible. Consumer representatives from the UK noted that many years ago the term 'dominance' was a fuzzy concept, but it is one that is well documented and used today in law making.

Introduce an unfair trading prohibition

There is ample evidence already in Australia for why Australians deserve to be protected from unfair business practices.[55] However, what the Fellowship confirmed is the longevity value of such a prohibition. Standing the test of time and the tech evolution, it is the prohibition that advocates, experts and regulators unanimously agreed that has the broadest reach, making no exemptions. To make it truly effective, it is about ensuring there is a general prohibition complemented with an evolving blacklist of practices and strong enforcement powers for regulators to act in a timely manner. Such powers can include imposing direct fines, remediation for customers and access to a company's A/B testing and algorithms – essentially keys to the hood of the business.

Ban subscription traps now

While Australia waits for the new law on unfair trading prohibition, an immediate action the Federal Government can take is banning subscription traps immediately. There are similar bans around the world that the government could use as a template such as the US Click to Cancel Rule.[56] Putting a stop to poor subscription practices will immediately help put money back into the pockets of Australians and reduce the mental load of navigating complex subscription processes that are designed to keep people paying for what they don't need or want.

Introduce non-negotiables on nagging and negging

In addition to banning subscription traps, dark patterns such as nagging and confirmshaming, which is a form negging, should also be prohibited. Both aspects are designed to nudge people towards decisions that are profitable for businesses but are rarely in the best interest of the consumer.

---

[55] CPRC et. al., 2023, *Make unfair illegal - Submission from consumer advocates on Treasury's Consultation Regulatory Impact Statement, Protecting consumers from unfair trade practices*, https://cprc.org.au/submission/make-unfair-illegal.

[56] Federal Trade Commission, 2024, *Click to Cancel: The FTC's amended Negative Option Rule and what it means for your business*, https://www.ftc.gov/business-guidance/blog/2024/10/click-cancel-ftcs-amended-negative-option-rule-what-it-means-your-business.

Specifically in the privacy space, nagging the person continuously after they've said 'no' to sharing more personal information online (e.g. rejected a cookie banner request) but never check-in with them again once they've said 'yes', is a prime example that nagging has been embedded to help the business not the individual. The DMA's obligation on designated entities to not be able to request for consent to data sharing for one year after a person has declined is an excellent example of how easily such an obligation can be embedded in law.

Make enforcement more than about money

It was clear through conversations with both consumer advocates and regulators, that while pecuniary penalties should be proportionate to the business and its conduct, and the concept of penalties compounding based on period of non-compliance, fines alone are not enough. In 2022, news reports confirmed that Meta had accounted for EUR 3 Billion in its forecasted budget to pay for fines under the GDPR.[57] When paying fines becomes part of doing business, they are no longer an effective deterrent.

Remediate and remove

Several consumer advocates and experts specifically noted the need for governments to further explore enforcement strategies that ensure that businesses cannot continue to profit from dark patterns and other unfair practices. Currently, in Australia, while a business may stop a dark pattern practice, there is nothing stopping the business to continue profiting from data or innovations it developed as a result of the practice. Strategies to mitigate this could include direct remediation to impacted consumers and data disgorgement (similar to financial disgorgement). Data disgorgement means that a business would be forced to delete or surrender any data including algorithms and insights it acquired or through prohibited practices. This could also include any products and services that have been designed based on the use of the data acquired.

Share the story – from investigation to impact

Many experts and consumer advocates noted the need for enforcement agencies to be more transparent and vocal about the investigations and enforcement actions they are undertaking. Many feel that the media release becomes the key tool of communication and happens often only at the end of an enforcement action.

> *"We need enforcement agencies to think like marketers."*
>
> Harry Brignull, UX Design Expert and Advocate

There is value in the story-telling of an investigation, not just during but even after action has taken place. ACM in the Netherlands currently does this through presenting at marketing events, blogs, social media content, guest lectures for universities and even through direct connection with businesses and industry peak bodies, meeting them one-on-one. CMA in the UK also confirmed under the DMCC the agency will be able to publicise an enforcement case at various points in the investigation instead of just at the end. It is these types of initiatives that can create space for reputational regulation.

[57] Manancourt, V., 2022, *Meta faces record EU privacy fines*, Politico, https://www.politico.eu/article/eu-fines-meta-privacy-tech-security-facebook-whatsapp-instagram.

Impose babysitting fees on select businesses

It is clear that for many large, dominant online platforms, simply knowing the legislation may not be enough to dissuade their implementation of unfair practices. These businesses need to be continuously monitored and probed to ensure a fair marketplace. However, to ensure effective enforcement, governments can rarely compete with some of the global businesses that hold significant market power. Ideally, regulators should be funded proportionately to the market they are overseeing. This could be achieved through ensuring government budgets account for well-resourced regulators. It could also be implemented through a supervisory fee provision as per the DSA where businesses are required to contribute to an annual fee to be effectively monitored and assessed for compliance. This ensures that the regulator has oversight and businesses are contributing towards an effective marketplace.

Design for fairness, not financials

We need to see more businesses design online architecture with fairness in mind. We need to put an onus on businesses to put themselves in shoes of their current and potential customers and ask the questions, 'will you understand the choice you're making?', and 'will you regret the decision you've made?'. Nir Eyal's concept of the regret test where designers check and verify whether the intended design is moving from persuasion to coercion is one such example of taking time to reflect on the possible outcomes of the design and what they will mean for the individual navigating it.[58]

One way this could be codified is through a design accountability officer. If protections against dark patterns are introduced in Australia, there is an opportunity to consider introducing a similar concept of a Data Protection Officer under the GDPR that businesses must have in place. The aim of the officer is to act as an internal compliance check and raise concerns without the fear of retribution.

Show what good looks like

While clear guidance by regulators is a step in the right direction towards a more compliant and fairer marketplace, experts and advocates shared that regulator guidance mostly focuses on the non-compliant instead of best practice, providing a snapshot of what not to do.

> *"Guidelines are great, but they don't always translate across the lifecycle of a product."*
>
> Valeria Adani, Projects by IF

What many experts and advocates are instead calling for are examples of best practice, or at least examples of good practice. Such examples would provide clarity on what a fair and meaningful consumer journey could look like online. Projects by IF in London and Fair Patterns by amurabi which has developed an AI solution to find and fix dark patterns at scale are two organisations that are leading the way in showing what good looks like and helping organisations pivot towards better navigation and decision-making pathways for their customers. Both also host pattern libraries for online customer journeys for decision-making, service access, consent and much more (Figures 4 & 5).

[58] Eyal, N., *Want to Design User Behavior? Pass the 'Regret Test' First*, Nir and Far, Last accessed: 16 February 2025, https://www.nirandfar.com/regret-test.

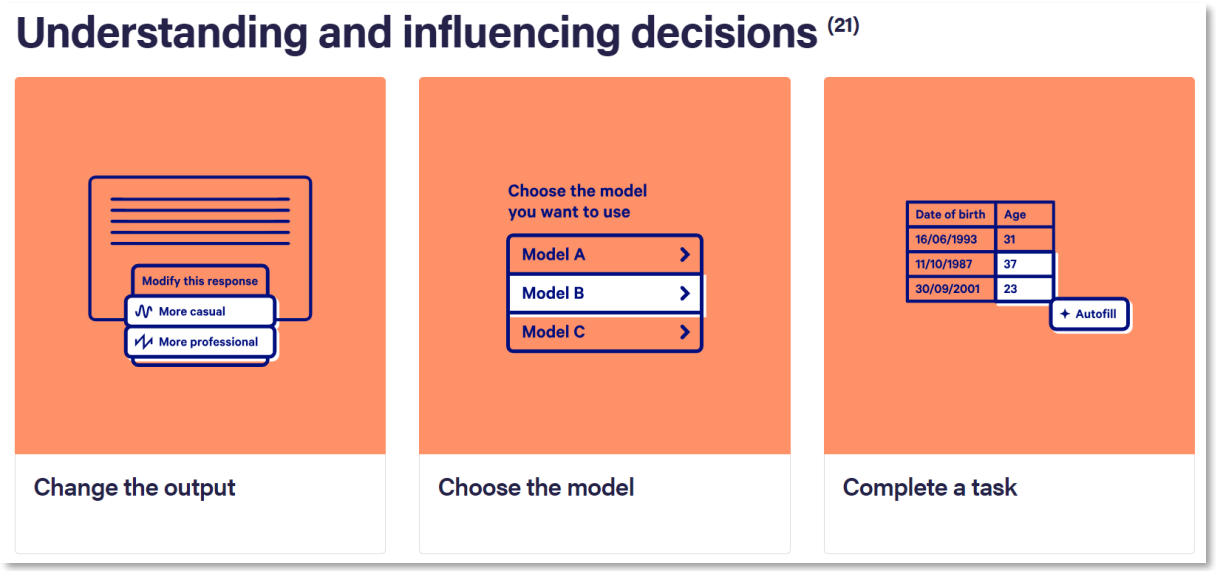


Figure 4: Pattern examples on the Projects by IF Design Patterns Catalogue.
Source: https://catalogue.projectsbyif.com/

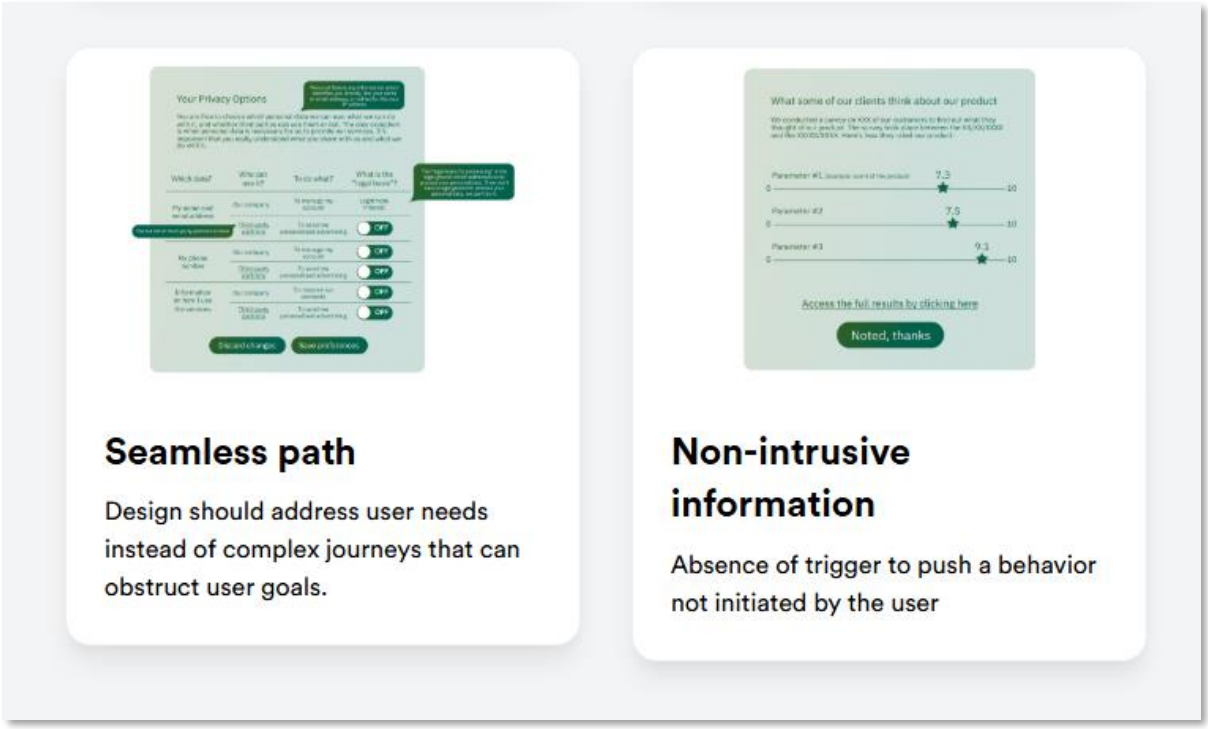


Figure 5: Pattern examples on the Fair Patterns Library
Source: https://www.fairpatterns.com/resources

"If you want results, you need something that is easy to implement."

Marie Potel-Saville, Founder of Fair Patterns

In India, not-for-profit organisation, Pranava Institute, has also developed a good practice manual, Design Beyond Deception, which has been created specifically for designers.[59] The manual is being used across India and in 2024, the institute conducted a Design Up Workshop to help designers unpack the consequences of dark patterns within online choice architecture.[60]

It is understandable that it may not naturally be within a regulator's remit to illustrate examples of good practice and compliant designs with the risk of being too prescriptive. However, an aspect that the Australian Government could consider is providing more funding to civil society so they have the capacity to develop tools and libraries such as these as a resource that businesses, especially small businesses can lean on when developing their online choice architecture.

[59] Vashist, T., Krishnakumar, S. and Kamalakannan, D., 2023, *Design Beyond Deception*, https://design.pranavainstitute.com/manual.
[60] Pranava Institute, 2024, *Workshop on Deceptive Design at DesignUp 2024!*, https://design.pranavainstitute.com/manual.

Where to from here

Speaking to experts, it is clear that choice and power in the digital economy play a significant role in an individual's experience and therefore, contribute to their wellbeing online. However, both elements appear to be disproportionately low in our current online world. What is needed is a recalibration from profit towards people where power is not asymmetrical but is shared across the economy and choice is genuine and respected. We need a new formula:

Having control over our choices + sharing power in the digital economy = wellbeing

If we are to adjust the balance, such a formula would need to be incentivised through consumer and competition frameworks. It would mean the burden of proof would no longer sit with individuals alone but on businesses to show that their practices put consumer interests first.

If we truly want a digital world that is fair, safe and meaningful, we must reimagine the constructs that the digital economy is currently built upon. As some countries are winding back digital protections, others are strengthening them, Australia is at a fork in the road. It could leave the digital world largely unregulated allowing practices such as dark patterns to thrive and continue to place the onus on consumers to navigate an online world that is not designed with their best interests in mind. Alternatively, Australia could take a stand to make fairness a genuine part of our consumer protection. Australia needs to be part of the coalition that keeps people safe online and upholds people's wellbeing as a basic precondition for all businesses.

Dissemination and implementation

The recommendations in this report will require a collective effort from Governments, businesses and civil society all working together to create a fairer digital market for Australians.

The intended audience for my report is the government, specifically regulators, consumer affairs departments and politicians who have oversight over their portfolio, academia

This report will be shared with the following groups:

- All organisations and individuals whom I met with during the Fellowship.
- Federal, state and territory Ministers and Shadow Ministers for consumer affairs and privacy.
- Australian Treasurer and the Attorney-General.
- Australian consumer law and privacy regulators.
- Australian academics in the consumer law and privacy space.
- Civil society organisations: consumer and privacy advocates.

With the support of my organisation, CPRC, I will also be holding a public webinar to share the insights and recommendations from my Fellowship to reach a wider audience, including Australian businesses.

Appendix – Fellowship itinerary

Date of Visit (2024)		Place	Institute/Organisation to be visited
From	To		
16/9	20/9	Singapore	Natalie Pang, Communications and New Media, National University of Singapore Renwen Zhang, Centre for Trusted Internet and Community, National University of Singapore Consumers Association of Singapore (CASE) Competition and Consumer Commission of Singapore Nir Eyal (interview conducted online on 8 January 2025)
21/9	25/9	Oslo, Norway	SIFO/OsloMet Norwegian Consumer Council Datatilsynet
25/9	28/9	Amsterdam, Netherlands	Authority of Consumers & Markets Dr Cristiana Santos, University of Utrecht Dr Amit Zac, University of Amsterdam
29/9	5/10	London, United Kingdom	Mozilla Projects by IF Harry Brignull, author of Deceptive Patterns Which? UK Consumer Organisation Citizens Advice UK
7/10	9/10	Paris, France	OECD Ministerial on Consumer Policy Meeting
10/10	13/10	London, United Kingdom	Consumer Markets Authority
14/10	20/10	Brussels, Belgium	BEUC, EU Consumer Organisation EU Consumer Law Fitness Check, Department of Justice Digital Services Act Enforcement, Communications Networks, Content and Technology
21/10	26/10	Paris, France	Consumer Policy Unit, OECD Fair Patterns French Consumer Association, Que Choisir
27/10	7/11	Washington DC, United States San Francisco, United States	Federal Trade Commission Future of Privacy Forum Consumer Federation of America California Privacy Protection Agency Electronic Frontier Foundation