Many of New Zealand's most popular websites use 'dark patterns' to manipulate users – is it time to regulate?

October 15 2021, by Cherie Lacey, Alex Beattie

Credit: AI-generated image (disclaimer)

More than half of the most popular New Zealand websites may be unfairly manipulating visitors, according to our latest research into the use of "dark patterns" in sites with a "co.nz" domain name.

While legal, dark patterns have been [described](#) as a type of online design employed to manipulate users into "making decisions that, if fully informed and capable of selecting alternatives, they might not make."

They're effective because they use insights about human psychology to [undermine user autonomy](#) or encourage users towards the [least privacy-friendly options](#).

Common examples include the so-called "[roach motel](#)," where it's easy to get into an online situation but difficult to get out of it—such as signing up for and then trying to cancel a streaming subscription.

There are also [disguised ads](#), which are presented as other kinds of content or navigation to encourage you to click. Some retail websites use dark patterns to nudge users to spend more.

Dark patterns have been widely criticized in the [US and Europe](#). For instance, amendments to the [California Consumer Privacy Act](#) seek to ban "the use of dark patterns to subvert or impair the process for consumers to opt out of the sale of personal information."

However, little research has been undertaken in Aotearoa New Zealand. The Commerce Commission [ruled against](#) Jetstar's online opt-out pricing tactics in 2016, but dark patterns don't appear to be on the government's legislative radar.

How do I unsubscribe?

We found dark patterns are well and truly a feature of New Zealanders' online experiences. Our list of the top 100 local sites (based on user traffic) included media, e-commerce, government, telecommunication, property and banking websites.

We simulated everyday use of the sites: arriving on a homepage, scrolling through and engaging with media content, purchasing a product, subscribing to and canceling a service.

A more complete picture was limited by our inability to fully access certain government or banking websites, but overall the results showed 54% of sites had one or more dark patterns. E-commerce sites were the biggest offenders, followed by media sites.

The research also reveals dark patterns tend to cluster around financial transactions, followed by homepage navigation, and when attempting to cancel a service or subscription.

Shopping and media

Online shoppers are most likely to experience a dark pattern when purchasing a product or service. Examples include a countdown timer to encourage immediate purchase, or activity notifications (such as when a user is made aware other customers are browsing the same item) to invoke the fear of missing out.

Are you sure? A typical example of the subscription cancellation – or 'suspension' – process. Screenshot, Author provided

Shoppers are also likely to encounter a dark pattern in the form of pop-up windows when first arriving on an e-commerce site. Many of these direct users to sign up for notifications or newsletters in exchange for a discounted price or early "VIP" notice of upcoming sales.

News consumers are especially likely to encounter dark patterns in the

form of interface interference to boost engagement metrics and drive advertising revenue—for example, the auto-play function on embedded video content.

Subscribers to premium media services are most likely to encounter some form of obstruction when attempting to cancel a service, donation or subscription—the "roach motel" again.

Customer surveillance

Another common dark pattern we observed involved a form of customer surveillance—the requirement that online shoppers register their personal details to use a site, even when simply browsing items.

As well as enabling ongoing contact between the business and the potential customer, this provides the opportunity for the business to gather valuable behavioral data about consumer habits.

These types of dark patterns normalize the exchange of personal details for very little in return. Although consent may be implied when a user hands over their details, most users remain uninformed about how their data will be used.

Dark patterns also appear to be used to reduce business costs through interface design that discourages certain types of communication, such as speaking to a customer service representative, in favor of more cost-effective options like "frequently asked questions" pages, online forms or an automated web chat.

Many New Zealand websites are deliberately designed to triage customer queries and drive down business costs associated with dealing with them.

Regulation versus education

Lockdown culture is [changing](#) online spending habits. Time spent online is [increasing rapidly](#), with New Zealanders now averaging six hours and 39 minutes on the internet daily.

Alongside these shifts in user behavior, artificial intelligence is increasingly being used to shape user experiences based on individual data profiles and behavior histories.

As a result, people are increasingly likely to be subjected to personalized, targeted manipulation as they conduct online activities—particularly online shopping.

Greater awareness of the dark arts of interface design may help users avoid this in their everyday online lives. But changes to relevant regulation, such as the Fair Trading Act and the Privacy Act, would also enhance New Zealanders' consumer and privacy rights.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation