We need a code to protect our online privacy and wipe out 'dark patterns' in digital design

September 16 2020, by Cherie Lacey, Alex Beattie

Credit: AI-generated image ([disclaimer](#))

A digital building code is needed to help designers better protect the privacy of people when they use online platforms and websites.

At the moment no such code exists in New Zealand. Our [study](#) with designers shows they try to be ethical in what they do. But commercial

pressures from clients and uncertainty around the privacy implications of design mean privacy concerns are often overlooked.

That can put designers at risk of accidentally creating what are known as dark patterns on platforms that lure people to do things such as buying extras they don't need or signing up for something they don't want.

Dark patterns condemned

Some websites are intentionally designed with dark patterns in mind. They are widely condemned for their ability to manipulate users to perform actions against their best interests.

Types of dark patterns include the "roach motel," where you get into a situation very easily, but then find it very difficult to get out of. One common example is premium subscriptions.

There are also disguised ads, whereby advertisements are presented as other kinds of content or navigation, to get you to click on them. Some retail websites use dark patterns to nudge users to spend more.

Dark patterns have been criticized in New Zealand for misleading consumers. In 2016 the Commerce Commission fined airline Jetstar for preselecting optional extras on its ticketing website. During the online checkout process, customers needed to "opt out" of these additional services, such as travel insurance, seat selection and extra baggage.

Jetstar ultimately stopped the practice of opt-out pricing for domestic and international flights sold in New Zealand.

Privacy dark patterns

Dark patterns also undermine online privacy. [Overseas privacy experts](#) argue website designs can unfairly guide users towards the least privacy-friendly options.

For example, interfaces can repeatedly pester users with requests for consent, or obstruct access to a website until registration is completed and personal information is disclosed.

Privacy dark patterns tend to exploit people through methods such as "[overchoice](#)"—the problem of having too many choices, which can overwhelm or paralyze consumers.

Children and young people tend to be especially vulnerable to dark patterns, as highlighted by a recent [case against Google](#) for illegally gathering children's personal data on YouTube without parental consent.

Designers on dark patterns

So far little is known about what design professionals themselves think of dark patterns and the privacy implications of their practice for users. [Research](#) on [#darkpatterns](#) on Twitter shows some designers call out and publicly shame organizations that engage in manipulative design practices.

Many discussions of dark patterns imply designers themselves are complicit in undermining a user's privacy.

In our [research](#), we interviewed designers to find out what they thought about dark patterns. We wanted to understand the ethical awareness of designers in relation to user privacy and how ethical decision-making occurs in practice.

While the designers said they would like to advocate for greater privacy

for users, they are often unable to do so for a range of reasons.

They said privacy considerations are not a clear or conscious step during a design project. Many feel they are unable to raise concerns about user privacy with the client or product owner.

They experience commercial pressures to reduce costs and are often disconnected from discussions about data privacy during the course of a project.

Many designers felt caught between designing for usability and designing for privacy.

Some had never heard of a dark pattern, while others saw them as design mistakes rather than the intention of the designer or the product owner.

One designer said: "I think you have to kind of be conscious of accidentally doing dark patterns—you know, customers will click through and just constantly click the green button, and they don't read a thing."

Building privacy in design

Based on our research, we think there's a missing layer of accountability in New Zealand when it comes to personal data protection. Designers are ideally positioned to take this place by building greater privacy mechanisms into their interface designs.

But they need support to make the best design decisions for users.

Support for designers could manifest in several ways. For example, in the United States a bill has been introduced that seeks to ban dark patterns outright. But this has been criticized as a blunt approach.

"Privacy by design"—the practice of embedding privacy protections into products—is a promising approach but does not provide specific advice on the role of design in capturing personal data.

The need for a code

We believe certainty and help with regard to online privacy could come in the form of design standards, a type of digital building code that protects online privacy.

Design standards might help to avoid the creation of dark patterns and reduce the construction of porous digital environments that leak our personal data.

A digital building code—written by designers, for designers—would give practitioners something to rely on when advocating for user privacy. It would provide more certainty about what constitutes a secure digital environment. It would also address the missing layer of accountability we identified in our research.

In a move towards developing such a code we're hosting a workshop with designers and privacy experts on October 20 in Wellington. Attendance is free but registration is mandatory.

It could be the first step towards design standards to ensure greater online privacy protection.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation