Clusters of Dark Patterns Across Popular Websites in New Zealand

CHERIE LACEY
ALEX BEATTIE
Te Herenga-Waka, Victoria University of Wellington, New Zealand

TRISTAM SPARKS
Massey University, New Zealand

"Dark patterns" are interface design techniques that aim to trick or mislead Internet users. Most dark-patterns research has been undertaken in the United States and Europe and by user experience or human computer interaction researchers. In this study, we adopt a media and communication studies and science and technology studies approach to investigate where dark patterns "cluster" in online environments. A walkthrough of the top 100 New Zealand websites leads us to the following findings: (1) dark patterns cluster around financial transactions; (2) the most common types of dark patterns constitute a form of interface interference; and (3) dark patterns are often deployed as mechanisms to drive revenue, facilitate customer surveillance, and reduce business operations costs, and appear to be largely imported from overseas markets.

Keywords: dark patterns, e-commerce, walkthrough, interface design, user experience

The Dark Arts of Interface Design

In August 2021, the New Zealand Commerce Commission released a report that criticized sales tactics used on customers from the two largest supermarket chains in New Zealand. Both the Countdown and New World supermarkets offer rewards-based loyalty schemes that present discounted prices to members and other benefits, such as "two-for-one" deals. Not only do the schemes provide a means for supermarkets to gather valuable data about consumers' purchasing decisions and shopping habits but, in addition, they create an interface, or touchpoint, where customers learn about supermarket products before making purchasing decisions. Central to the Commerce Commission's concerns is that the rewards-based loyalty schemes create a manipulative interface that misleads supermarket customers. The report claims that these supermarket loyalty schemes reduce price transparency, overstate the true value of the reward,

Cherie Lacey: Cherie.Lacey@Vuw.Ac.Nz
Alex Beattie: Alex.Beattie@Vuw.Ac.Nz
Tristam Sparks: T.Sparks@Massey.Ac.Nz
Date Submitted: 2021-09-23

and increase the difficulty for consumers to make informed purchasing decisions about products (Commerce Commission New Zealand, 2021).

Rewards-based loyalty schemes are not the only "dark art" (Stock, 2021) or questionable business practice that aims to exploit human psychology for commercial gain. Embedded within digital interfaces such as websites and mobile applications are ethically dubious design techniques known as "dark patterns." The term dark pattern was coined by user experience (UX) designer Harry Brignull (2010) on the website www.deceptive.design, which catalogues instances where established design patterns and user behaviors are leveraged to manipulate or deceive users for the benefit of the product owner. Dark patterns are derived from the concept of design patterns, where designers capture an instance of a problem and a corresponding solution, abstract it from a specific use case, and shape it in a more generic way so that it can be applied and reused in various matching scenarios—typically within a user interface or a sequence of events in a software-enabled user experience. In instances where interactions are prescriptive—for example, entering an e-mail address in an online form—the design can make the user's task easier by providing options that smooth their pathway through an "intuitive" experience. A dark pattern is the use of this approach to mislead a user for the benefit of a product owner and tricks users into performing unintended and unwanted actions.

Mathur and colleagues (2019) summarize dark patterns as "interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make" (p. 2). Scholars argue that dark patterns are effective because they use insights about human psychology from behavioral science (Maier & Harr, 2020) and are often deployed to undermine user autonomy (Waldman, 2020), or encourage users toward privacy-unfriendly options (Luguri & Strahilevitz, 2021). Chivukula, Watkins, McKay, and Gray (2019) consider dark patterns to be a significant ethical issue in the fields of computer science and human computer interaction (HCI) and the practice of website development or UX.

In this study, we investigate where dark patterns "cluster" on popular websites in New Zealand. We seek to understand which online activities users are most likely to be engaged in when they encounter dark patterns and to take a snapshot of the prevalence of dark patterns in the largely unregulated digital environment of New Zealand. Our research is motivated by several factors. First, there is a lack of dark-patterns scholarship in the Global South, with studies largely being conducted in the United States and Europe. The studies of dark patterns from the Global North have revealed how digital interfaces on international platforms such as Facebook and Amazon manipulate their users to support outcomes that are beneficial to those platforms (Frobrukerrådet, 2018). Many New Zealanders use Facebook and Amazon but also New Zealand-specific websites to watch the news, access government and educational services, conduct e-commerce, do their banking, order food and alcohol, and more. Research about the presence of dark patterns on New Zealand websites does not currently exist. From our own research, knowledge about dark patterns among UX and design professionals in New Zealand is minimal (Beattie, Lacey, & Caudwell, forthcoming), and therefore, New Zealand websites could be deploying dark-pattern designs unknowingly.

Second, the frequency with which New Zealanders are encountering dark patterns is likely increasing. New Zealanders spend on average 6 hours and 39 minutes online per day (HootSuite, 2021), and the COVID-19 pandemic has further integrated the Internet into New Zealanders' everyday lives

(Preston, 2021). The Internet is not a distinct "cyberspace" but infrastructure for people to work, study, socialize, access essential services, purchase goods and services, and vote, among other activities. By interrogating New Zealand websites' utilization of dark patterns, we can begin to understand the degree to which New Zealand Internet users are *subjected to manipulation in their everyday lives*. As it stands, awareness and understanding of dark patterns are a significant blind spot in consumer protection and privacy law in New Zealand, and we hope this study offers useful insights for media, design, and privacy scholars, as well as regulators. As we have seen from previous research, gauging the presence of dark patterns is useful when encouraging regulators to consider interface design as a crucial part of any legislation that aims to protect user rights (Soe, Nordberg, Guribye, & Slavkovik, 2020; Utz, Degeling, Fahl, Schaub, & Holz, 2019). Furthermore, we suggest our findings will prove useful in supporting ongoing efforts to increase data literacy in the general population.

Third, our focus on popular national websites opens the door for greater understanding of the industry contexts in which dark patterns emerge. We explore which types of New Zealand-based websites use dark patterns and discuss the reasons these websites might engage in manipulative practices. Existing studies of dark patterns have largely neglected to ask these questions. This is, perhaps, because of disciplinary preferences. HCI studies have focused on defining typologies of dark patterns (Bösch, Erb, Kargl, Kopp, & Pfattheicher, 2016; Gray, Kou, Battles, Hoggatt, & Toombs, 2018; Mathur et al., 2019), debated which types of designs constitute a dark pattern (Mathur, Mayer, & Kshirsagar, 2021), or, more broadly, discussed the development of ethical design practices to combat dark patterns within HCI and UX practice (Chivukula et al., 2019; Gray, Bielova, Toth, Santos, & Clifford, 2021). Legal and privacy scholars have discussed dark patterns in the design of notice-and-consent mechanisms (Waldman, 2020), and their efficacy in steering users toward giving up personal data (Luguri & Strahilevitz, 2021), while behavioral economists limit their purview of dark patterns to "choice architecture," or the design of public policies such as opt-in/opt-out questionnaires (Rossi, Ducato, Haapio, Passera, & Palmirani, 2019). Drawing from our backgrounds in media and communication studies, science and technology studies (STS), and UX design research, we draw attention to the industry logics and economic systems that incentivize the production and spread of dark-pattern interfaces and contribute toward the development of a critical dark-pattern studies. Our research questions are:

RQ1: *Where are users most likely to encounter dark patterns in everyday online life?*

RQ2: *What are the most common types of dark patterns and which types of websites are using them?*

RQ3: *What does the most common type of dark patterns and the websites that use them reveal about the (re-)production of dark patterns on the New Zealand Internet?*

The rest of this study is structured as follows. In the next section, we provide an overview of previous studies that have researched the presence of dark patterns in different jurisdictions and digital contexts. These studies investigate the frequency of dark patterns in cookie-consent windows, mobile games, and shopping websites but do not explicitly investigate where dark patterns constellate during a user journey. We then detail our method in Section 3, describing our study set-up and corpus generation, the user journeys we analyzed, and our classification of dark patterns. In Section 4, we discuss our results.

We share that New Zealanders are likely to encounter dark patterns when making a purchase or when trying to cancel a service or subscription where websites use strategies of *interface interference* to steer the user toward options that benefit the product owner. We also take a snapshot of the presence of dark patterns in New Zealand over a three-month period and find that at least 54% of the most popular websites in New Zealand have one or more dark pattern. The implications of these findings, we argue, are that dark patterns are driven by commercial pressures to boost sales and reduce business costs. We suggest that future research on this topic needs to pay attention to the market logics of dark patterns, the role of dark patterns in surveillance capitalism (Zuboff, 2019), and the genealogies of dark-pattern libraries (cf. Dieter, 2015).

Literature Review: Dark Patterns Spotted in Cookie-Consent Windows, Mobile Games, and Shopping Websites

In recent years, European scholars have searched for dark patterns in cookie-consent windows. This was motivated by the introduction of the General Data Protection Regulation (GDPR) in the European Union (EU) in May 2018. The GDPR seeks to uphold informational self-determination by increasing transparency requirements for organizations' data-collection practices and strengthening users' rights about their personal data (Utz et al., 2019). Before the introduction of the GDPR, some commentators predicted that the new regulation would lead to a proliferation of dark patterns on EU-based websites (Paternoster, 2018), with fears that organizations would use deceptive design practices to circumvent the intent of the GDPR (Frobrukerrådet, 2018). In response, several EU-based studies (Nouwens, Liccardi, Veale, Karger, & Kagal, 2020; Soe et al., 2020; Utz et al., 2019) analyzed the interface design of cookie-consent notifications to determine how many used dark patterns to steer users toward the least privacy-friendly options. The study by Utz and colleagues (2019) determined that 57.4% of consent notifications in the European Union have one or more dark pattern. Further, their study showed that even small user-interface design decisions can "substantially" impact whether and how users interact with cookie-consent notices. For example, one of their experiments indicated that highlighting the "accept" button in a binary choice with "decline," and preselected choices for different uses of cookies has a strong impact on whether the user accepts the third-party cookies.

Nouwens and colleagues (2020) conducted a similar study into the use of dark patterns on consent pop-ups in the European Union following the introduction of the GDPR. Their results show that 88.2% of consent notifications contained one or more dark pattern. Nouwens and colleagues (2020) also ran user testing to determine the efficacy of dark patterns on users' privacy decision making, finding that there was a ~22% increase in acceptance when the opt-out option was concealed behind the initial notice (i.e., when at least two clicks were needed to opt out). A study by Soe and colleagues (2020) looked specifically at the prevalence of dark patterns in cookie-consent notifications for online news services. Manually analyzing 300 consent notifications from Scandinavian and English language news outlets, Soe and colleagues (2020) found that almost all of them (297 of 300) employed some level of what they deemed "unethical" design practice, ranging from nudges to dark patterns (p. 2).

To date, there are two U.S. studies that attempt to determine the presence of dark patterns. Di Geronimo, Braz, Fregnan, Palomba, and Bacchelli (2020) focused their study on popular mobile games in the United States. Manually analyzing 240 games, they found that 95% of them contained one or more type of dark pattern and, on average, popular games include at least seven different types of deceptive interface designs, such as making it impossible for a user to logout, or moving ad buttons (Di Geronimo et al., 2020, p. 473). The second is an experiment conducted by U.S.-based Mathur and colleagues (2019), who performed the first large-scale study of the prevalence of dark patterns. Mathur and colleagues (2019) developed an automated approach to detect the presence of dark patterns in ~11,000 shopping websites worldwide and created a large corpus of dark-pattern artifacts. They found dark patterns in 11.1% of websites but note that this number represents the lower bound on the total number of dark patterns on these websites since their automated approach only detected text-based user interfaces on a sample of product pages per website.

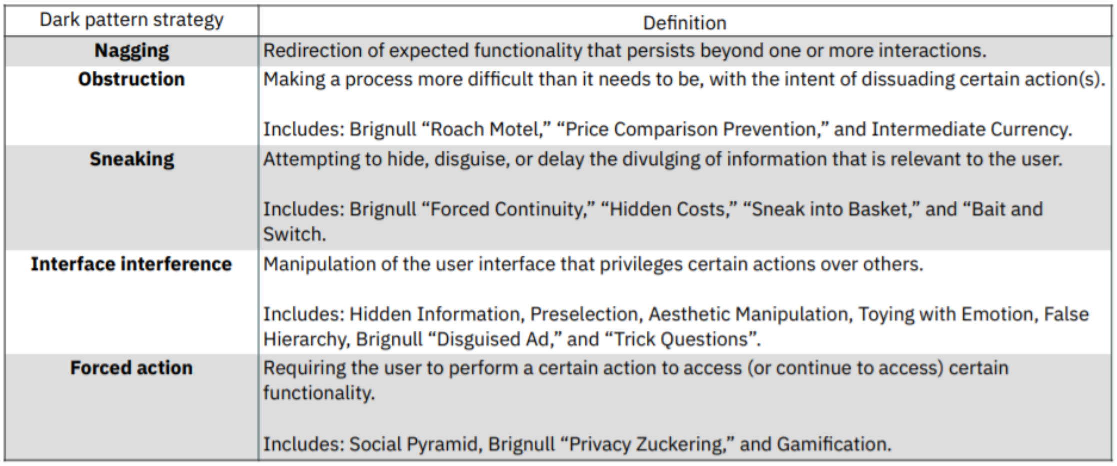
However, none of the existing studies into the presence of dark patterns has sought to understand where along a user journey dark patterns are likely to cluster. This is not to undermine the value in attempts to determine a base-line figure for the prevalence of dark patterns in particular environments. It is evident from this research that understanding the scale of dark patterns is useful when creating novel taxonomies and corpora of dark patterns (Mathur et al., 2019), publicly reproaching offenders (Brignull, 2010), and urging regulators to consider interface design as a crucial part of any legislation that aims to protect user rights (Soe et al., 2020; Utz et al., 2019). However, what is missing from this work to date is a rich account of where dark patterns congregate in online environments, and what a user is most likely to be doing when they encounter one.

Method: How We Identified Dark Patterns Across the New Zealand Internet

Our study is designed to gather empirical data about where dark patterns tend to cluster. We do so to spotlight which online activities tend to attract deceptive UX design practices so that we might better understand where users are subject to manipulation in everyday life. Our research also aims to take a snapshot of the prevalence of dark patterns on popular New Zealand websites over a three-month period to get a sense of the scale of the problem in New Zealand. To conduct our study, we took the following steps: developing our coding instrument; determining our corpus; defining our user journeys; undertaking a three-step empirical data collection and analysis.

Developing Our Coding Instrument

To develop our coding instrument, we turned to established frameworks or typologies of dark patterns. Mathur and colleagues (2021) identify a total of 19 definitions of dark patterns, which have been grouped into nine different typologies. Of these, Gray and colleagues (2018) taxonomy has become one of the most used for analyses of dark patterns. Gray and colleagues (2018) created their taxonomy of dark patterns from the ground up by collecting a corpus of dark patterns submitted by users on Twitter. The authors revamped the original dark patterns taxonomy developed by Brignull (2010), introduced new dark patterns, and grouped types of dark patterns into five broad strategies, which we summarize in Figure 1.



Dark pattern strategy	Definition
Nagging	Redirection of expected functionality that persists beyond one or more interactions.
Obstruction	Making a process more difficult than it needs to be, with the intent of dissuading certain action(s). Includes: Brignull "Roach Motel," "Price Comparison Prevention," and Intermediate Currency.
Sneaking	Attempting to hide, disguise, or delay the divulging of information that is relevant to the user. Includes: Brignull "Forced Continuity," "Hidden Costs," "Sneak into Basket," and "Bait and Switch.
Interface interference	Manipulation of the user interface that privileges certain actions over others. Includes: Hidden Information, Preselection, Aesthetic Manipulation, Toying with Emotion, False Hierarchy, Brignull "Disguised Ad," and "Trick Questions".
Forced action	Requiring the user to perform a certain action to access (or continue to access) certain functionality. Includes: Social Pyramid, Brignull "Privacy Zuckering," and Gamification.

Figure 1. Gray and colleagues (2018) taxonomy of dark patterns.

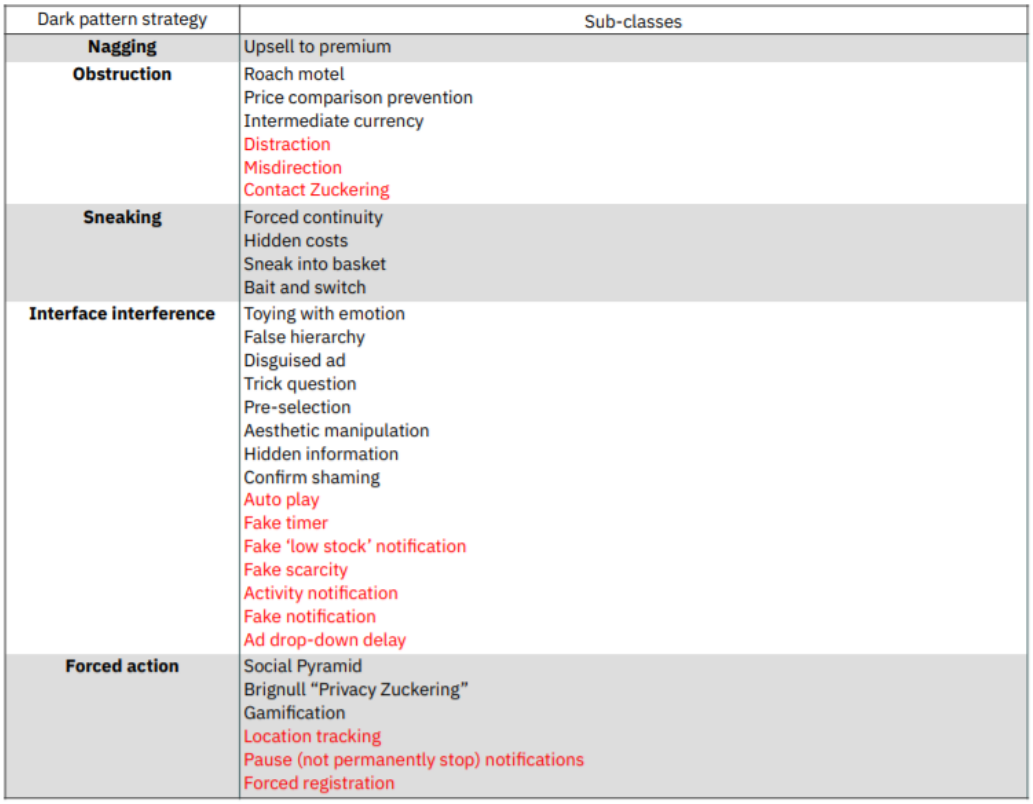
Gray and colleagues (2018) explain that "nagging" dark patterns often manifest as a repeated intrusion during normal interaction, where the user's desired task is interrupted one or more times by other tasks not directly related to the one the user is focusing on. An example is an e-commerce website that requires the user to click through multiple separate attempts to upsell before submitting an order. "Obstruction" often manifests as a major barrier to a particular task that the user may want to accomplish (Gray et al., 2018), and includes three subclasses: "intermediate currency" (multiple currencies, such as game gems), "price comparison prevention" (uncopiable product names), and "roach motel" (easy to open an account, yet hard to delete it). An example of obstruction occurs on websites that use a cookie-consent banner on the home page. These sites can make it difficult to opt out of cookies through the website itself; rather, the user must disable them on his or her browser by following a link to a third-party website, where users are presented with a lengthy text that must be understood before a user can disable cookies.

"Sneaking" often occurs to make the user perform an action they would prefer not to if they had knowledge of it (Gray et al., 2018), and comprises four subclasses: "bait and switch" (a certain action seems to have a specific result; instead it causes another, unwanted outcome), "hidden costs" (an item initially costs X, but in the basket its value increases), "sneak into basket" (unwanted items are added in the basket), and "forced continuity" (e.g., subscription is automatically continued after its free trial expires). An example of "sneaking" is a website that has multiple instances of hidden costs when signing up for their service. "Interface interference" is any manipulation of the user interface that privileges specific actions over others, thereby confusing the user or limiting discoverability of important action possibilities (cf., false or hidden affordances; Gray et al., 2018). This category includes the most subclasses: "hidden information" (options to accept conditions are small/grayed-out), "preselection" (unfavorable options are preselected), and "aesthetic manipulation" (distracting manipulation of the user interface). This last subclass has four components: "toying with emotions" (countdown to offers or emotive language), "false hierarchy" (one option is more prevalent), "disguised ad" (interactive games), and "trick questions" (double negatives). An example of "interface interference" is a news website that uses delayed drop-down advertisements to encourage users to accidentally click on the ad instead of the intended article.

The last strategy, "forced action," may manifest as a required step to complete a process or may appear disguised as an option that the user will greatly benefit from (Gray et al., 2018). This category has three subclasses: "social pyramid" (adding friends to obtain benefits), "privacy Zuckering" (sharing more personal data than intended), and "gamification" (forced grinding tasks to obtain something otherwise available with money). An example of forced action is a media website that requires users to create a detailed user profile to access content, especially if the profile requires users to hand over more data than is necessary for the service to be functional—for example, the user's gender preference.

As Gray and colleagues (2018) themselves recognize, categories of dark patterns are not mutually exclusive, and it is common for one dark pattern to be grouped into several categories. The "roach motel" dark pattern, for example, in which a user finds it easy to subscribe to a service but very difficult to unsubscribe, fits under both obstruction and interface interference. That said, Gray and colleagues (2018) taxonomy proved effective in both Di Geronimo and colleagues' (2020) and Soe and colleagues' (2020) studies into the presence of dark patterns, and is, therefore, the taxonomy we have chosen to work with for our experiment. Both Di Geronimo and colleagues (2020) and Soe and colleagues (2020) note that they had to make small adjustments to the taxonomy to suit their specific testing scenarios, with both research groups calling for future studies that use Gray and colleagues' (2018) taxonomy to expand and adapt it for use in particular research scenarios.

To test the utility of Gray and colleagues' (2018) taxonomy and determine additional rules for the classification of dark patterns, the first author began by analyzing Brignull's (2010) live "Hall of Shame" Airtable document and coding all entries (*n* = 356 at the time of coding) using Gray and colleagues' (2018) taxonomy. Brignull's (2010) Airtable is an online repository for all dark patterns collected via #darkpatterns and @darkpatterns on the Twitter platform. As part of this process, the first author added some additional subclasses of dark patterns not included in the existing taxonomy—for example, "fake notification," or "ad delay." This produced our coding instrument, which we then used to categorize instances of dark patterns in our corpus of the 100 most popular New Zealand-based websites, see Figure 2. The additional subclasses of dark patterns are marked in red.



Dark pattern strategy	Sub-classes
Nagging	Upsell to premium
Obstruction	Roach motel
	Price comparison prevention
	Intermediate currency
	Distraction
	Misdirection
	Contact Zuckering
Sneaking	Forced continuity
	Hidden costs
	Sneak into basket
	Bait and switch
Interface interference	Toying with emotion
	False hierarchy
	Disguised ad
	Trick question
	Pre-selection
	Aesthetic manipulation
	Hidden information
	Confirm shaming
	Auto play
	Fake timer
	Fake 'low stock' notification
	Fake scarcity
	Activity notification
	Fake notification
	Ad drop-down delay
Forced action	Social Pyramid
	Brignull "Privacy Zuckering"
	Gamification
	Location tracking
	Pause (not permanently stop) notifications
	Forced registration

Figure 2. Our coding instrument (expanded and adapted from Gray et al., 2018). Our additions are marked in red text.

Determining Our Corpus

We chose to limit this study to websites only, rather than include apps. Apps constitute a unique digital environment and therefore warrant a dedicated study, as noted in Section 5. To determine the list of the most popular New Zealand websites, we used the Alexa ranking, which measures traffic to a site relative to all other sites on the Web over the past three months.[1] We filtered results by country and generated our list on June 8, 2021 (for the period March 8, 2021–June 8, 2021). After arriving at our list of the top 100 New Zealand websites, we filtered out the following: non-English sites (*n* = 1); business-to-business (B2B) sites (*n* = 2); and sites that redirected from an organization's old domain name to its new one (*n* = 2). We

[1] The rank is calculated using a proprietary methodology that combines a site's estimated average of daily unique visitors and its estimated number of page views over the past three months. They provide a similar country-specific ranking, which is a measurement of how a website ranks in a particular country relative to other sites over the past month. Alexa was also used by other studies into the prevalence of dark patterns (see Nouwens et al., 2020; Utz et al., 2019).

replaced these four websites with the next four on Alexa's ranking, arriving at our final list of the 100 most popular websites in New Zealand during a three-month period in 2021.

Defining Our User Journeys

To standardize our analysis of each website, we grouped user journeys into six common types.

1. Arrival: Landing on the website's homepage.
2. Registration: Signing up for a service.
3. Purchase: Purchasing a product or service. Note, we stopped each purchasing user journey after adding the item to cart because we did not have the research resources to complete shopping cart processes. We did, however, sign up to subscription services and donate a small amount of money to news organizations when asked, to test the cancellation process (see "cancel," below). In our conclusion, we discuss how stopping the shopping cart journey limited our findings.
4. Media content: Engaging in media content on a site—for example, reading a news story or watching a television show.
5. Contact: Noting how easy or difficult it was to find a contact number on the website.
6. Cancel: Following the off-boarding process to cancel a regular donation or subscription.

Data Analysis

As noted by Di Geronimo and colleagues (2020) and Soe and colleagues (2020), there are numerous aspects and provisions to dark patterns, many of which can be assessed only qualitatively. Our research builds on the work conducted by Di Geronimo and colleagues (2020) and on Soe and colleagues (2020), both of which used the walkthrough method developed by Light, Burgess, and Duguay (2016) to determine the presence of dark patterns. The walkthrough method is a qualitative approach that allows researchers to step through the various stages of interaction systematically and forensically, slowing down the mundane moments of use to consider the cultural meanings and power dynamics at each step. As Di Geronimo and colleagues (2020) argue, this approach is useful because, "in some instances . . . one can infer the presence of dark patterns only [by] interacting with the artefact" (p. 4). Furthermore, the walkthrough protocol ensures consistency in our method; however, it did not allow us to investigate websites with restricted access or high barriers of entry, such as government or social services, or banking and other financial services. We further discuss the limitations to our study in Section 5.

The first and second authors (media and communication studies and STS) worked together to manually analyze all 100 websites, using each website as it was intended to be used for five minutes—for example, to purchase a product on an e-commerce website, or to view a news story on a media website.[2] We classified any instances of dark patterns encountered using our coding instrument (Figure 2), taking screenshots to record each dark pattern we found during our walkthrough. Disagreements about what constituted a dark pattern and how a dark pattern should be categorized were noted for future discussion and comparison with the third author's findings. The third author (UX designer and

[2] These authors worked on a new HP laptop with cookies disabled and using the standard settings.

design researcher) performed another walkthrough of the websites, following the established protocol.[3] He hid the findings from the first walkthrough to ensure objectivity, and recorded any instances of dark patterns he encountered. We then discussed our findings as a research group, resolved any disagreements by majority vote, and arrived at our results. All three authors self-identifying as having high digital literacy (Dobson & Willinsky, 2009), with regular access to, and frequent use of, digital media technologies.

Results and Discussion: Users Are Most Likely to Encounter Dark Patterns When Completing a Purchase

High Level Results

Our data reveal that dark patterns tend to cluster around the purchasing journey, followed by arrival on the homepage, and when attempting to cancel a service or subscription (Figure 3). Users are most likely to experience some form of *interface interference* when purchasing a product or service—for example, a fake countdown timer to encourage immediate purchase. Users are also likely to encounter *forced action(s)* when browsing e-commerce sites, typically in the form of forced registration (i.e., requiring a user to register their personal details to use a site). Users are also likely to encounter *interface interference* in the form of interstitial, "pop-up" windows when first arriving on an e-commerce website, many of which direct users to sign up for notifications or newsletters.

Users are also likely to encounter dark patterns when accessing media content or when trying to cancel a subscription or donation to a media organization. When accessing media content, especially news content, websites are likely to use some form of *interface interference* to boost engagement metrics and drive advertising revenue. More frequently, however, users are most likely to encounter some form of *obstruction* when attempting to cancel a service, donation, or subscription ("roach motel"). Our results also show that the users are likely to encounter a form of *obstruction* when trying to find an organization's contact telephone number. This constitutes a new subclass of dark pattern we have dubbed "contact Zuckering."[4] We discuss the implications of these findings in detail below.

[3] This author worked on an Apple MacOS Big Sur (11.5.1), using the Chrome browser (Version 92.0.4515.131 [Official Build] [x86_64]). He signed out of all accounts associated with the laptop and cleared cookies after each unique website visit.

[4] The phrase "contact Zuckering" is inspired by the dark pattern known as "Privacy Zuckering," where users are "suckered" to give away more privacy. We wish to imply that users are similarly "suckered" by a dark pattern into contacting a business via a means that the business prefers and in a way that requires users to hand over personal data.

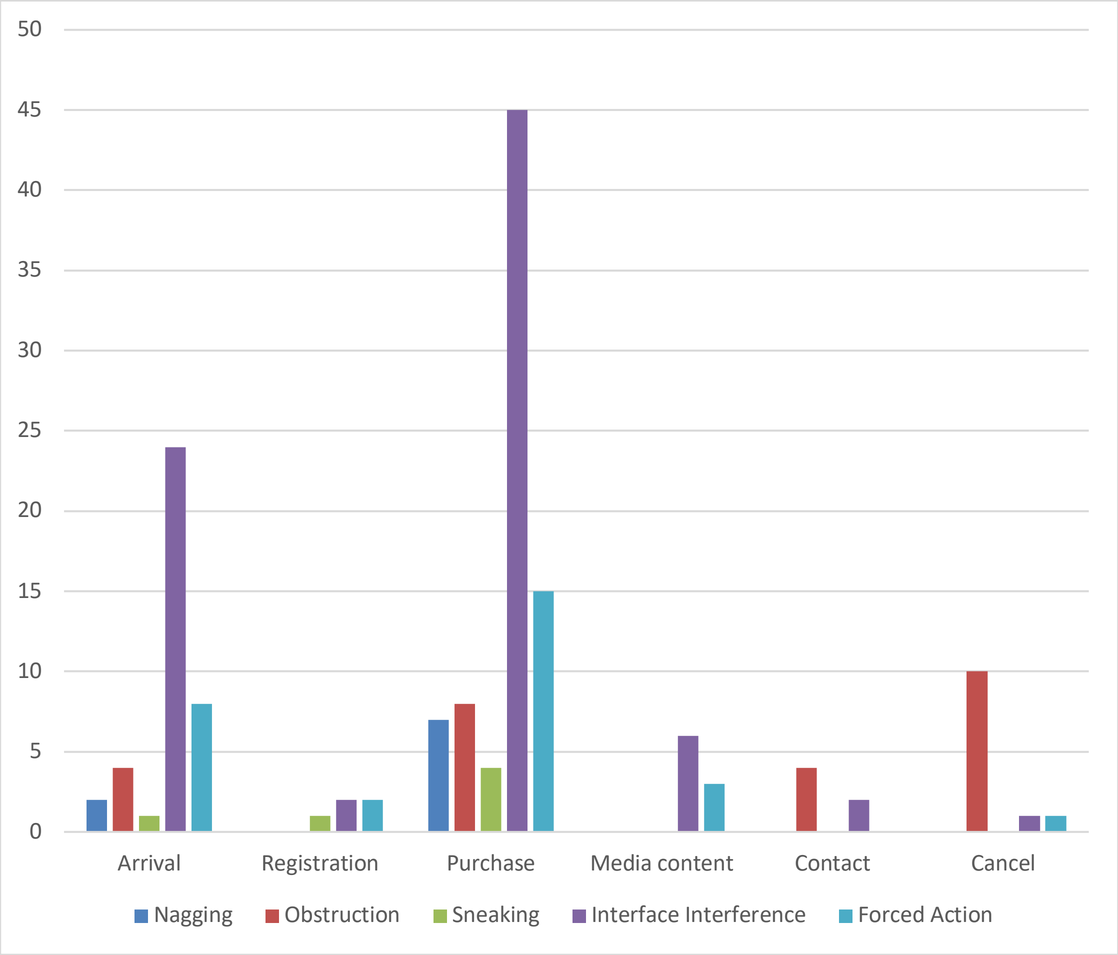


Figure 3. Clusters of dark patterns by user journey.

Across all 100 websites, the most common type of dark-pattern strategy was *interface interference* (52%), followed by *forced action* (19%), *obstruction* (15%), *nagging* (9%), and *sneaking* (5%; Figure 4). We detected dark patterns in at least 54% of the 100 most popular websites in New Zealand over the three-month period of our study. We present the table that documents our findings as an Appendix (Table 1).[5]

[5] Table 1 is available via the Open Science Framework: https://osf.io/d8qrs

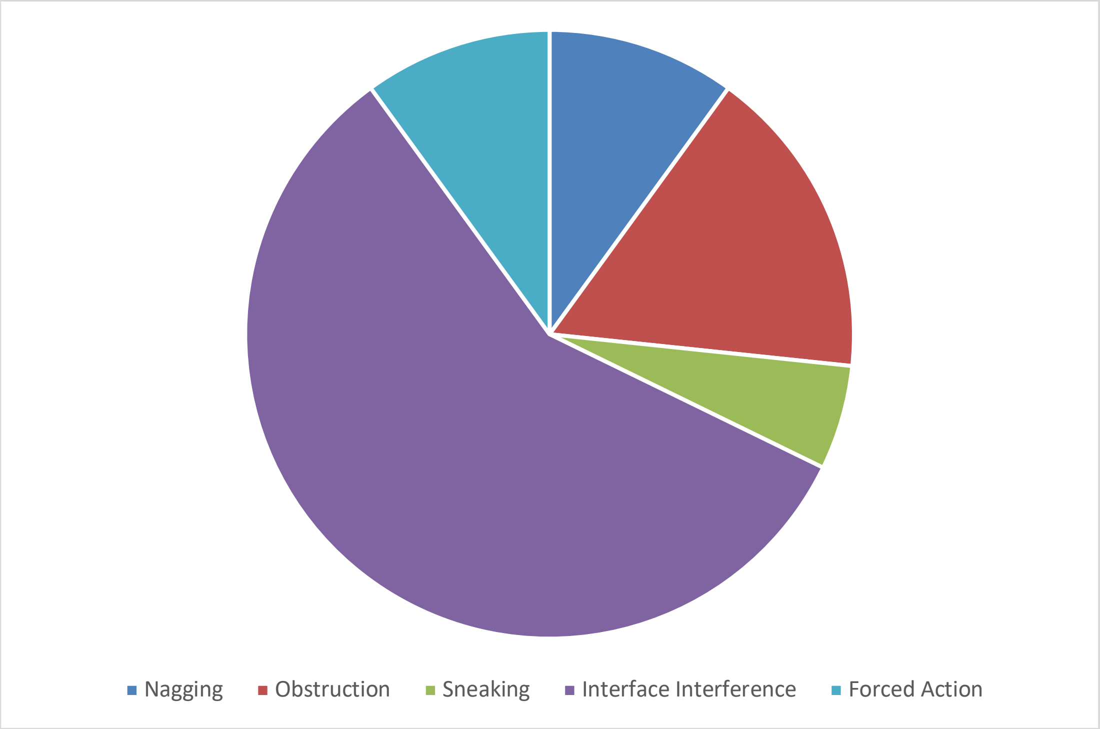
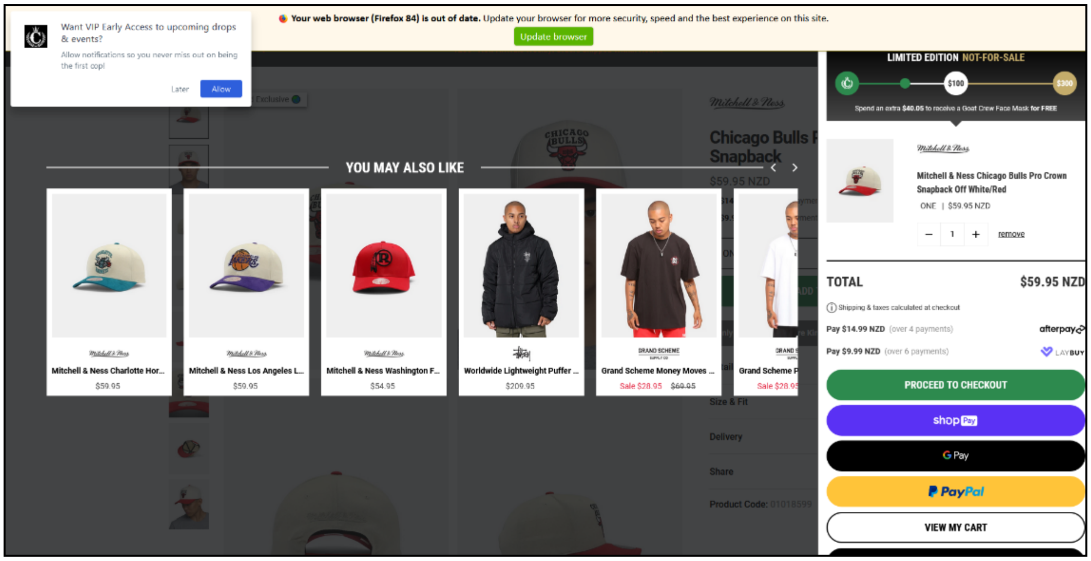


Figure 4. Percentage of dark-pattern strategies by type.

Mechanisms to Drive Sales and the Disclosure of Personal Information

A key finding of this research is that dark patterns are deployed to maximize or drive sales. As noted, the most common dark-pattern strategy—interface interference—was often found during the purchasing journey to encourage the user to purchase a product, or, upon arrival on the homepage, to advertise deals or encourage membership or subscription to a service. Common examples of interface interference included design features that encouraged impulse buying, such as the countdown timer, fake scarcity, or price comparison prevention. One of the biggest culprits was Vodafone New Zealand (telecommunication company), on whose site we encountered four qualitatively different instances of interface interference during the purchasing journey. Dark patterns included the purchase options defaulting to monthly plans, plan details hidden when narrowing purchasing decisions, small UI text used when informing users of one-off fees, and multiple instances of fake scarcity or "surprise free options." The streetwear brand Culture Kings was also notable, with four of the seven dark patterns on their site encountered occurring during the purchasing journey—for example, the inability to opt out of "VIP notifications" from the site, default opt-in to the newsletter, multiple instances of fake scarcity, and pushing other items for sale while underemphasizing the "proceed to checkout" button (Figure 5).



Want VIP Early Access to upcoming drops & events?

Allow notifications so you never miss out on being the first cop!

Your web browser (Firefox 84) is out of date. Update your browser for more security, speed and the best experience on this site.

Spend an extra **$40.05** to receive a Goat Crew Face Mask **for FREE**

Product	Price
Mitchell & Ness Charlotte Hor...	$59.95
Mitchell & Ness Los Angeles L...	$59.95
Mitchell & Ness Washington F...	$54.95
Worldwide Lightweight Puffer ...	$209.95
Grand Scheme Money Moves ...	Sale $28.95 ~~$60.95~~
Grand Scheme P	Sale $28.95

Mitchell & Ness Chicago Bulls Pro Crown Snapback Off White/Red

ONE | $59.95 NZD

TOTAL $59.95 NZD

Shipping & taxes calculated at checkout

Pay $14.99 NZD (over 4 payments)

Pay $9.99 NZD (over 6 payments)

Figure 5. The Culture Kings website uses multiple instances of interface interference to guide user behavior. Screenshot by the author.

There were numerous other examples of dark patterns in e-commerce sites to encourage instant purchasing behavior. Many retail sites used countdown timers to create a sense of urgency in the user. Other sites used notifications such as "in stock, ships today!" to leverage consumers' bias toward instant gratification. This was especially deceptive in the case of Fishpond and Mighty Ape (online-only books and gift stores), and Dick Smith (electronics store), where the websites make it difficult or impossible to find out where a product ships from and therefore how long it will take to arrive (items can take up to 10 weeks to arrive in New Zealand from the United States, China, or Europe). Several websites also used dark patterns to overstate a "sale" price or to suggest that the price of an item is cheaper than normal or when compared with other sites. Harvey Norman (technology and furniture store), for example, adds red text to items, such as "Price Matched!" or "Hot Price!" (Figure 6). However, when the researchers tried to compare the "Price Matched!" item with other New Zealand websites, we could not find the item for sale anywhere else. Statements such as "Hot Price" suggested the item was available at a reduced price; however, when returning to the site in ensuing weeks and months, the price remained the same.

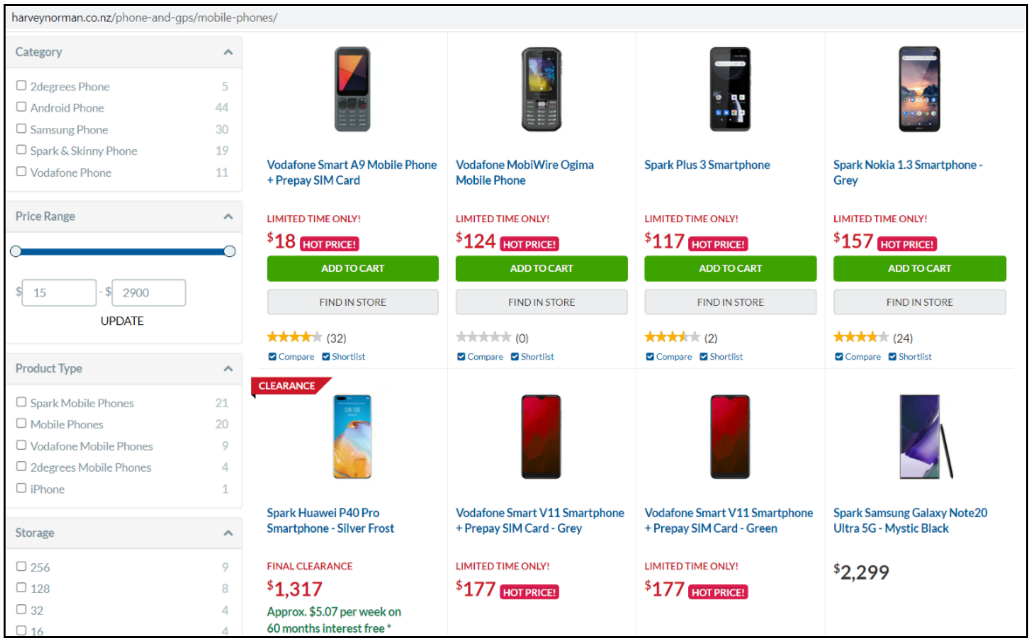
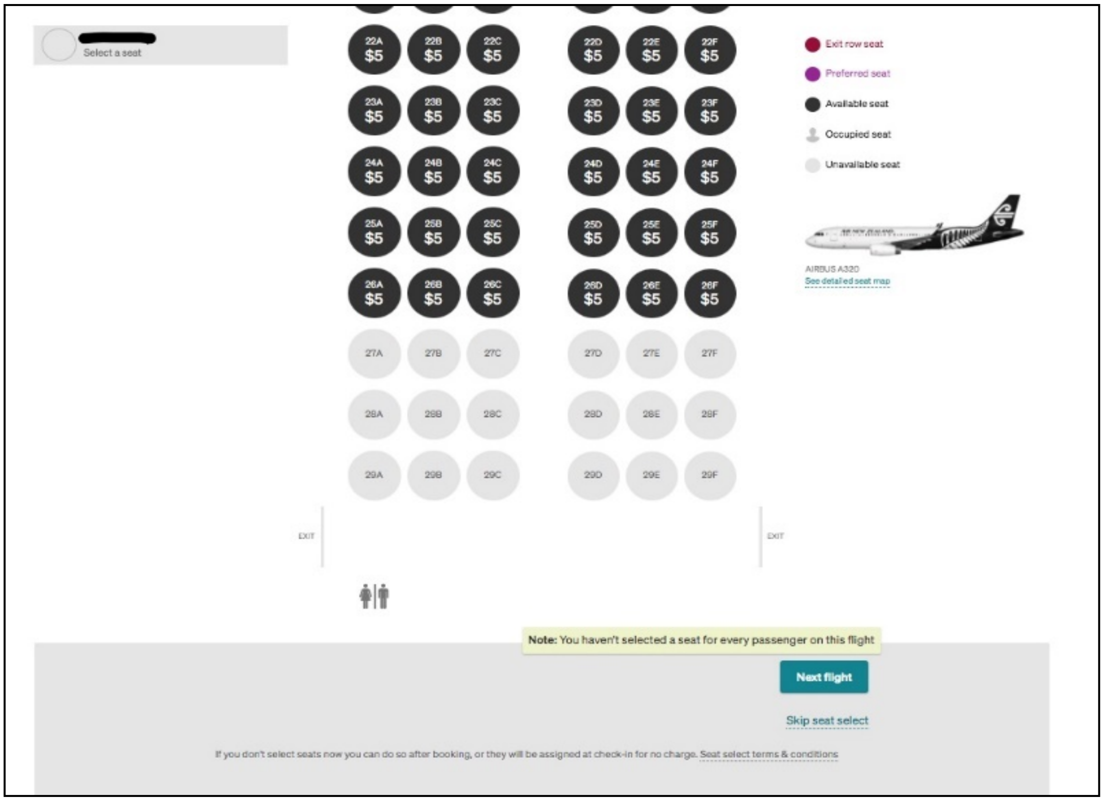


Figure 6. Harvey Norman’s use of interface design to encourage impulse purchasing. Screenshot by the author.

E-commerce websites also deployed dark patterns to upsell to users. Air New Zealand (national airline carrier), for example, makes it difficult for users to skip premium “add-ons,” such as seat selection. In this case, the user is required to scroll down to find a small, undistinguished button to skip this step, while also encountering a button that effectively “warns” users they have not selected a seat—when, in fact, there is no requirement to do so (Figure 7). Air New Zealand also preselects insurance for the user and requires them to opt out of receiving the newsletter. Almost all e-commerce websites in our corpus used mild forms of dark patterns to try to sell users more items before completing the purchase. In the case of Chemist Warehouse—a notably busy website—the final “purchase” button is difficult to find among all the other items the user is asked to consider before completing the purchase.


[redacted]
Select a seat
22A $5 22B $5 22C $5 22D $5 22E $5 22F $5
23A $5 23B $5 23C $5 23D $5 23E $5 23F $5
24A $5 24B $5 24C $5 24D $5 24E $5 24F $5
25A $5 25B $5 25C $5 25D $5 25E $5 25F $5
26A $5 26B $5 26C $5 26D $5 26E $5 26F $5
27A 27B 27C 27D 27E 27F
28A 28B 28C 28D 28E 28F
29A 29B 29C 29D 29E 29F
EXIT
EXIT
Exit row seat
Preferred seat
Available seat
Occupied seat
Unavailable seat
AIRBUS A320
See detailed seat map
Next flight
Skip seat select
Seat select terms & conditions

Note: You haven't selected a seat for every passenger on this flight

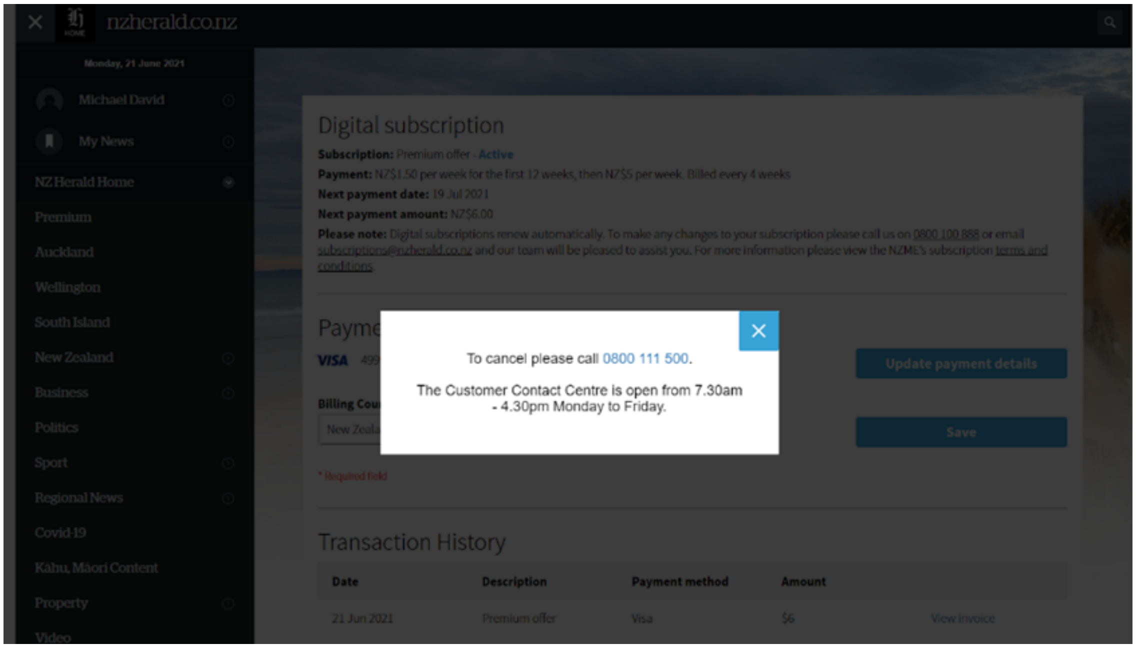
If you don't select seats now you can do so after booking, or they will be assigned at check-in for no charge.

Figure 7. Air New Zealand encourages users to use pay extra to select their seat. Screenshot by the author.

Dark patterns also commonly appeared on media websites to facilitate sales, whether in the form of advertising dollars or individual user subscriptions. For example, *Stuff* (2021), a popular news site that works on a donation model,[6] used emotional appeals to encourage user donations—such as, "you've read 20 articles for free this month . . ." *Stuff* (2021) uses footers that block over half of the landing page to encourage donations, with no option for "no" (only "I'd like to contribute," "I've already donated," or "maybe later"). The researchers donated a small amount to the site to test the cancellation process, finding themselves caught up in a difficult off-boarding process. Donations to *Stuff* are run by an organization called Press Patron, which operates on a separate login system. There is nowhere to log into Press Patron from the *Stuff* website, which makes it difficult to cancel or manage donations. Furthermore, after arriving at the correct site to manage donations, there is no "cancellation" button; rather, the user needs to input "0" into the amount field to cancel his or her financial contribution, which may confuse some users. *The New Zealand Herald* operates on a "premium" subscription business model. When trying to cancel our subscription, we found that we could not do so online; rather, we were directed

[6] Users are asked to set up a regular, automatic payment to donate to the site. However, all content on the site is free to access regardless of whether a user donates.

to call a number where an operator asked us to provide a reason for the cancellation (Figure 8).[7] In addition, at Sky Sport, a user cannot, technically speaking, cancel his or her account; rather, cancellation is framed as a "suspension." Users cannot cancel their Sky TV accounts online and are required to phone a number to speak to an operator.



Digital subscription

Subscription: Premium offer - Active
Payment: NZ$1.50 per week for the first 12 weeks, then NZ$5 per week. Billed every 4 weeks
Next payment date: 19 Jul 2021
Next payment amount: NZ$6.00
Please note: Digital subscriptions renew automatically. To make any changes to your subscription please call us on 0800 100 888 or email subscriptions@nzherald.co.nz and our team will be pleased to assist you. For more information please view the NZME's subscription terms and conditions.

Payme

VISA 499

Billing Cou

New Zeala

* Required field

To cancel please call 0800 111 500.

The Customer Contact Centre is open from 7.30am - 4.30pm Monday to Friday.

Transaction History

Date	Description	Payment method	Amount	
21 Jun 2021	Premium offer	Visa	$6	View invoice

Figure 8. The New Zealand Herald requires users to phone a number and offer a reason to cancel their subscription. Screenshot by the author.

Media sites also deployed dark patterns to drive engagement metrics. Both *Stuff* and *The New Zealand Herald* made constant use of the red, "breaking news" banners at the top of their sites even for the most banal stories to encourage users to repeatedly check the website throughout the day. *Stuff*, *The New Zealand Herald*, ThreeNow, and NewsHub all used the auto-play function for embedded video content. In all cases, the websites made it very difficult—at times impossible—to either disable this function or pause the video. On *Stuff*, a video cannot be paused until it has started to play. On *The New Zealand Herald*, a delayed ad drop-down in addition to a five-second auto-play countdown makes it very difficult for a user to locate and click the "pause" button in time (Figure 9). This is likely a tactic to drive advertising sales, in which higher engagement metrics can be used to secure advertising revenue.

[7] When we offered "we can no longer afford it" as our reason, there was no attempt to dissuade us.

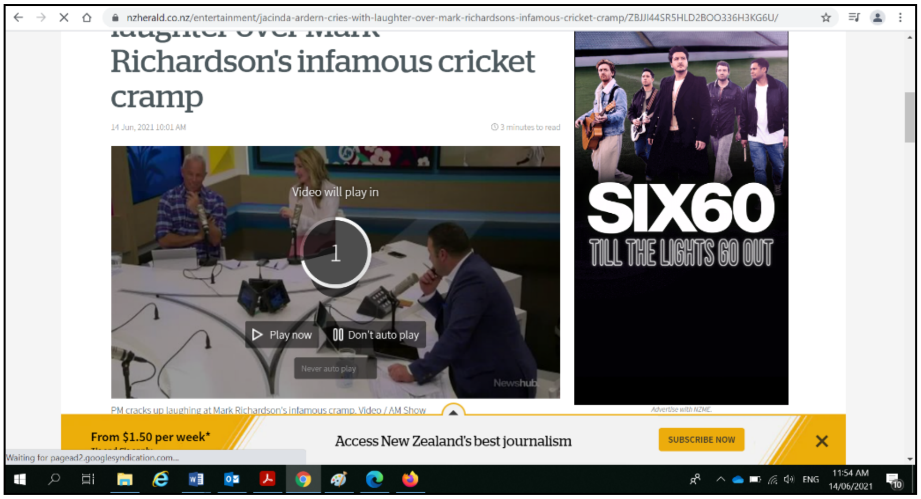

nzherald.co.nz/entertainment/jacinda-ardern-cries-with-laughter-over-mark-richardsons-infamous-cricket-cramp/ZBJJI44SR5HLD2BOO336H3KG6U/
Richardson's infamous cricket cramp
14 Jun, 2021 10:01 AM
3 minutes to read
Video will play in
1
Play now
Don't auto play
Never auto play
Newshub
PM cracks up laughing at Mark Richardson's infamous cramp. Video / AM Show
SIX60
TILL THE LIGHTS GO OUT
Advertise with NZME.
From $1.50 per week*
Access New Zealand's best journalism
SUBSCRIBE NOW
Waiting for pagead2.googlesyndication.com...
ENG
11:54 AM
14/06/2021

Figure 9. The New Zealand Herald makes it difficult to find and click the "don't auto-play" button in time. Screenshot by the author.

The few instances of "sneaking" or "nagging" that we encountered in our walkthroughs also related to sales. We classified as "nagging" instances where websites repeatedly (i.e., three or more times) used interstitial windows to prompt the user to sign up for a newsletter or register their details, such as when navigating through the Countdown website or the Culture Kings website. Vodafone used the dark strategy of sneaking when signing up for one of their phone plans. The Vodafone website advertises plans at an initial (lower) price, only to add costs near the end of the lengthy purchasing journey once the user has already invested time in the process. This exploits the cognitive bias known as "hyperbolic discounting," or the likelihood to overvalue the present consequences of a decision over future decisions (Waldman, 2020, p. 106).

Our results indicate, then, that dark patterns predominantly emerge at the point of, and are intertwined with sales or financial transactions. Many of the top New Zealand websites use manipulative design tactics to facilitate or continue a sale or transaction. In this sense, dark patterns represent an exaggeration of "market manipulation" (Calo, 2013; Hanson & Kysar, 1999), in which companies use their knowledge of human psychology and cognitive biases to steer purchasing behaviors and increase profits.[8] It is, therefore, crucial for future research to consider the market contexts in which dark patterns arise. Existing literature on dark patterns has largely been silent about the market logics of dark patterns (for exceptions, see Mathur et al., 2019; Mulligan, Regan, & King, 2020), focusing instead on the ethics of dark patterns and the threats they pose to user autonomy. From our research, it is clear that considerations of the industry contexts in which dark patterns emerge is fundamental to understanding the ways users are subject to manipulation in everyday life because conclusions that the designers behind dark patterns are unethical or "assholes" (Chivukula et al., 2019) ignores the importance of the economic contexts of manipulative interface design. Further explorations into the market

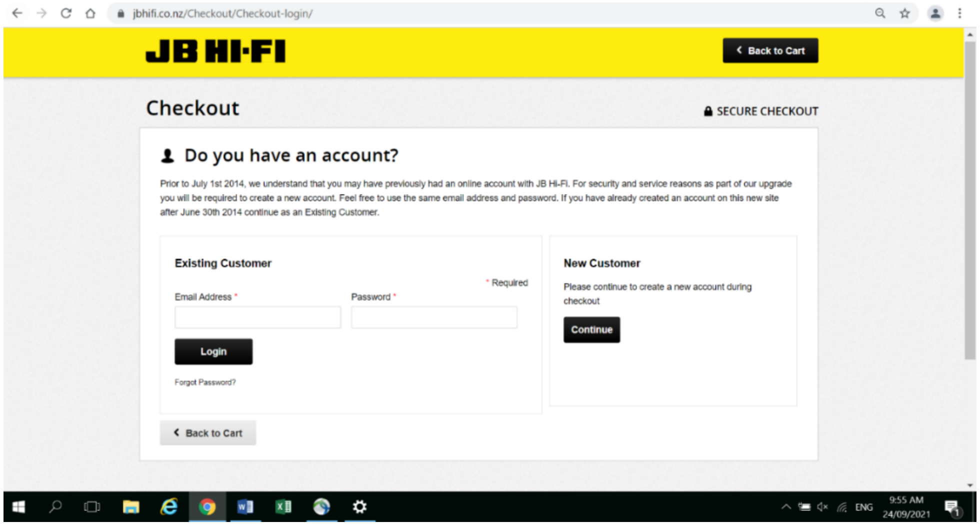
[8] Market manipulation should be distinguished from classical sales strategies. The former describes how businesses exploit the cognitive limits of consumers (Hanson & Kysar, 1999), while the latter are sales techniques that predate the Internet and target uninformed, uncertain and undecided consumers (Pourmasoundi et al., 2022).

logics of dark patterns may contribute toward greater understanding of why the market and politics fail to reign in egregious digital practices, despite collective outrage or frustration (Acquisti, Brandimarte, & Loewenstein, 2020; see also Mulligan et al., 2020).

Surveillance Capitalism and the New Zealand Internet

Dark patterns are also deployed to create and continue contact with a potential customer and to gather valuable behavioral data about consumer habits. As noted, common examples of forced action include requiring individuals to register their personal details to use a site, even in the most casual encounter. Many e-commerce sites ask or require users to give over valuable personal data such as names, locations, ages, genders, and shopping or media preferences. Often, registration is compulsory to complete a purchase (Figure 10). Other sites make so many repeated appeals for user data (i.e., through the use of interstitials) that the site becomes functionally unusable unless the user complies with the request. On some sites, for instance on the Farmers (department store) website, the option to complete a purchase as a guest is hidden by interaction elements (light gray text against a white background) and requires a user to navigate away from the initial notice to select this option. Forced registration therefore appears to be an increasingly common practice among e-commerce sites in New Zealand and constitutes a clear attempt to harvest valuable behavioral data from consumers.

The logic underpinning forced registration is to create a channel of communication whereby the customer can be contacted and learn of future sales and discounts, and for the organization to maintain a record of a user's consumer habits. In this sense, dark patterns constitute an important mechanism of surveillance capitalism (Zuboff, 2019), in which personal data are used to pattern, predict, and modify human behavior for the data-driven economy. Given that personal information is now "raw material in the political economy of informational capitalism" (Cohen, 2019, p. 48), there is clear motivation for websites to extract as much user data as possible through design patterns that force registration.



Do you have an account?

Prior to July 1st 2014, we understand that you may have previously had an online account with JB Hi-Fi. For security and service reasons as part of our upgrade you will be required to create a new account. Feel free to use the same email address and password. If you have already created an account on this new site after June 30th 2014 continue as an Existing Customer.

Existing Customer

* Required

Email Address *

Password *

New Customer

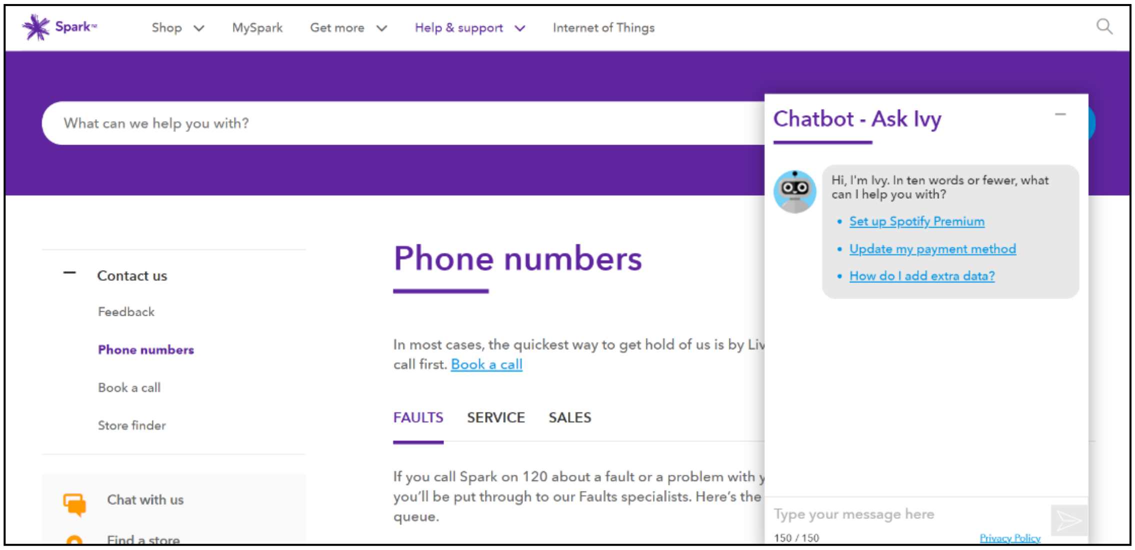
Please continue to create a new account during checkout

Figure 10. It is common for e-commerce sites to require customers to register before completing a purchase. Screenshot by the author.

Furthermore, forced registration has significant implications for users' data privacy. As noted by Acquisti and colleagues (2020), consumers do care about privacy but find it increasingly difficult to manage it in the online environment. From our data, we found that interface design downplays the risks of data sharing, frames data sharing as a positive act or social good, and normalizes the disclosure of increasingly personal data. For example, the Countdown website frames its use of personal data as way of offering an "enhanced" service to customers, allowing them a more "personalized and tailored" experience. Factors such as present bias (overweighting the immediate gain and underweighting the long-term consequences) and informational asymmetry (websites make their privacy policies very difficult to read and comprehend) contribute to users giving over personal data and allowing organizations to track their consumer habits (Acquisti et al., 2020). For example, the benefits of signing up to a supermarket reward scheme, such as accessing sale prices for items, often distract from the long-term privacy implications of allowing supermarkets access to a user's behavioral data—the value of which far outweighs the minimal savings on offer. This renders the true costs of privacy intangible, delayed, and uncertain (Acquisti, 2004).

Automating Customer-Business Relations

Our data also suggest that dark patterns are used to reduce business-operating costs. Another common dark pattern we identified is what we call "contact Zuckering," or the use of design to obfuscate means of communication that are costly to businesses (e.g., speaking to a customer service representative) and steer the user to a more cost-effective means of communication (e.g., frequently answered questions, online forms, or an automated Web chat) (Figure 11). The high prevalence of contact Zuckering in our corpus suggests that the interface between the business and consumer is designed to triage customer queries and drive down business costs associated with dealing with them. This may disadvantage users who prefer to speak with the business over the phone but have low digital literacy, such as the elderly population. Future research could investigate whether dark patterns affect different types of users' disproportionality. As noted above, in many ways, dark patterns represent a continuation of market manipulation, and contact Zuckering is no exception. In this case, dark patterns follow a history of businesses designing customer experiences to encourage certain choices. The introduction of free-to-call (0800) numbers in New Zealand in the 1990s was an attempt to direct callers to outsourced, cost-effective customer inquiry businesses. Contact Zuckering represents a further step in automating the customer-business interface and further limits the choices available to users.



Phone numbers

In most cases, the quickest way to get hold of us is by Liv
call first. Book a call

If you call Spark on 120 about a fault or a problem with y
you'll be put through to our Faults specialists. Here's the
queue.

Chatbot - Ask Ivy

Hi, I'm Ivy. In ten words or fewer, what can I help you with?

- Set up Spotify Premium
- Update my payment method
- How do I add extra data?

Figure 11. An example of contact Zuckering from the Spark website. Screenshot by the author.

Imported and Homegrown

Another key finding is that a significant batch of dark patterns are not being made in New Zealand but are imported from elsewhere. Some dark patterns in user journeys (e.g., e-commerce processes) were built on near-identical Web templates (see Figure 12), suggesting New Zealand businesses are purchasing software that designs the shopping cart user journey for them. This suggests that certain dark patterns are designed by third-party software providers, with little or no awareness by UX designers or product owners in New Zealand. For example, JB Hi-Fi and Harvey Norman are both trans-Tasman companies, operating out of both New Zealand and Australia. The JB Hi-Fi website appears to be custom-made, but their development team is incognito. The Harvey Norman sites appears to be built on a mix of purchased and custom-made technology, with the development team primarily based in Sydney, with only a handful of New Zealand-based developers working to localize the site.

Our previous research into the UX design industry in New Zealand supports our suggestion that many dark-pattern libraries are being imported. Our research found that UX designers had very little awareness or understanding of dark patterns and, when they did, perceived them to be the result of “asshole design” on fringe websites (Beattie et al., forthcoming). Research into the genealogies of the dark-pattern libraries being imported for use in the New Zealand Web environment, alongside interviews with bespoke interface developers in New Zealand, would contribute a great deal to understanding the industry contexts in which dark patterns emerge. It further legitimizes the arguments made by Chivukula and colleagues (2019) and Gray and colleagues (2018) that there is a need for progressive UX design education to be incorporated into tertiary institutions, perhaps in the form of design ethics courses. Relevant design ethics material could include the work of technology philosopher Peter Paul Verbeek (2011) who demonstrates how designers can mitigate unforeseen user manipulation by anticipating and incorporating a range of usages and effects of their persuasive creations into the design process. Ethical design education would help to boost the capacity for UX designers to advocate for users during the course of a workflow and introduce a new layer of accountability between users and product owners.

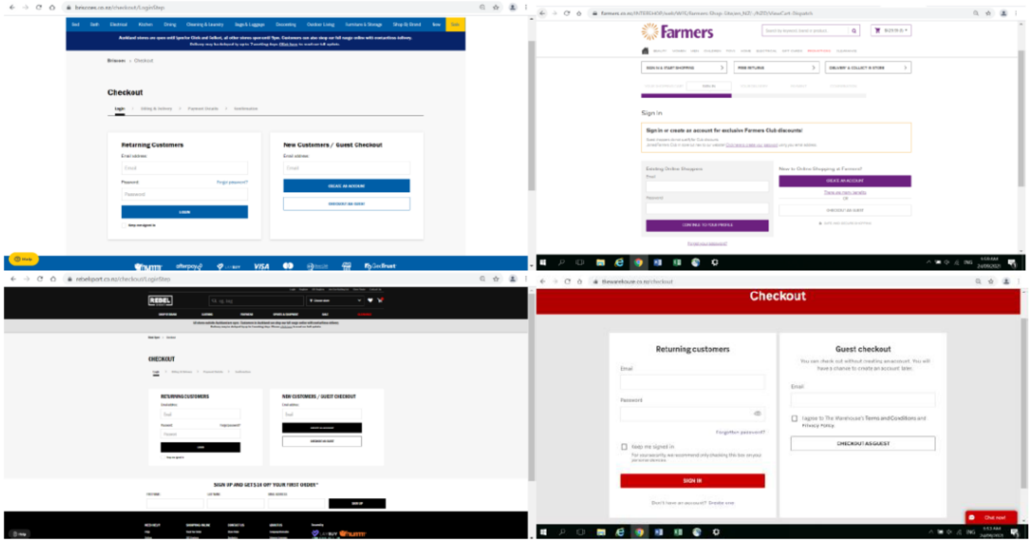


Figure 12. A comparison of four shopping cart processes to demonstrate similarities across pattern libraries. Screenshots by the author.

Our study has shown that dark patterns cluster wherever an organization has a financial stake in the outcome. Websites use dark patterns to steer purchasing behaviors, obtain valuable personal data about consumer habits, drive advertising revenue, or when simply trying to reduce business-operating costs. The congregation of dark patterns on e-commerce sites during the purchasing journey, in particular, warrants further investigation. A recent report into New Zealanders' consumer habits claims that the COVID-19 lockdowns have produced a "transformational shift" in spending behaviors, as online retail becomes normalized (Anthony, 2021). Furthermore, artificial intelligence is increasingly being used to direct the formation of user experiences based on users' individual data profiles and their histories of behavior in mediated spaces. This means that users are highly likely to be increasingly subjected to individualized and targeted online manipulation as they conduct online retail.

Our study is not a comprehensive diagnosis of dark patterns across the New Zealand Internet. That our study focused on e-commerce and media sites may be a reflection of how easy these sites are to access, for the general population at least. We did not access websites that had restricted access, including financial services, government services, and education websites. In addition, because of limited research resources, we also did not complete certain shopping cart processes or request refunds on all retail websites. There are, no doubt, many forms of malicious website design that we missed in our walkthroughs, whether that is because we simply could not access the site, because we did not follow a particular user journey, or the dark patterns occurred in a trans-media context (i.e., on the organization's app).

However, there are good reasons to take a snapshot of New Zealand’s digital environment to discover where dark patterns might constellate and what users are most likely to be doing when they encounter a dark pattern. First, understanding the presence of dark patterns in the digital environment may contribute to regulatory interventions in consumer protection and data privacy in New Zealand. Second, determining where users might encounter dark patterns is an important step if we are to understand the industry and market contexts of dark patterns and the digital ecosystems in which they arise. The work undertaken in this study opens the door to future empirical research into the design genealogies of dark patterns, especially for the Global South. Finally, as Di Geronimo and colleagues (2020) demonstrate, users perform better in recognizing deceptive or malicious designs if they are informed of the issues. Therefore, determining clusters of dark patterns in the most-used New Zealand websites may help bring the issue to the attention of the wider public. Our hope is that this study establishes the ground for work to be done toward developing greater data literacy in this region.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of instant gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21–29). New York, NY: Association for Computing Machinery. doi:10.1145/988772.988777

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758. doi:10.1002/jcpy.1191

Anthony, J. (2021, September 1). ‘Lockdown culture marks transformational shift in New Zealanders’ spending habits as online sales boom. *Stuff*. Retrieved from https://www.stuff.co.nz/business/industries/126246704/lockdown-culture-marks-transformational-shift-in-new-zealanders-spending-habits-as-online-sales-boom

Beattie, A., Lacey, C., & Caudwell, C. (forthcoming). ‘It’s like the wild west’: User Experience (UX) designers on ethics and privacy in Aotearoa New Zealand. *Design and Culture*.

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies 2016, 4*, 237–254. doi:10.1515/popets-2016-0038

Brignull, H. (2010). *What are dark patterns?* Retrieved from https://www.deceptive.design/

Calo, R. (2013). *Digital market manipulation* (University of Washington School of Law Research Paper No. 2013-27). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703

Chivukula, S., Watkins, C., McKay, L., & Gray, C. (2019). "Nothing comes before profit": Asshole design in the wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–6). Glasgow, Scotland: Association for Computing Machinery. doi:10.1145/3290607.3312863

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford, UK: Oxford University Press.

Commerce Commission New Zealand. (2021). *Market study into the grocery retail sector (draft report—executive summary)*. Wellington. Retrieved from https://comcom.govt.nz/__data/assets/pdf_file/0024/260376/Market-study-into-the-retail-grocery-sector-Draft-report-Executive-summary-29-July-2021.pdf

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)* (pp. 1–14). New York, NY: Association for Computing Machinery. doi:10.1145/3313831.3376600

Dieter, M. (2015). Dark patterns: Interface design, augmentation and crisis. In D. M. Berry & M. Dieter (Eds.), *Postdigital aesthetics* (pp. 163–179). London, UK: Palgrave Macmillan.

Dobson, T., & Willinsky, J. (2009). Digital literacy. In D. R. Olson & N. Torrance (Eds.), *The Cambridge handbook of literacy* (pp. 286–312). Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511609664

Frobrukerrådet. (2018). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Oslo, Norway: The Norwegian Consumer Council. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Gray, C., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). Montreal, QC: Association for Computing Machinery. doi:10.1145/3173574.3174108

Gray, C., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *CHI Conference on Human Factors in Computing Systems* (pp. 1–18). Yokohama, Japan: Association for Computing Machinery. doi:10.1145/3411764.3445779

Hanson, J. D., & Kysar, D. A. (1999). Taking behavioralism seriously: The problem of market manipulation. *NYU Law Review, 74*(3), 630–749. Retrieved from https://www.nyulawreview.org/issues/volume-74-number-3/taking-behavioralism-seriously-the-problem-of-market-manipulation/

Hootsuite. (2021). *The global state of digital 2021*. *Datareportal*. Retrieved from https://datareportal.com/reports/digital-2021-new-zealand

Light, B., Burgess, J., & Duguay, S. (2016). The walkthrough method: An approach to the study of apps. *New Media & Society, 20*(3), 881–900. doi:10.1177/1461444816675438

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *The Journal of Legal Analysis, 13*(1), 43–109. doi:10.1093/jla/laaa006

Maier, M., & Harr, R. (2020). Dark design patterns: An end-user perspective. *Human Technology, 16*(2), 170–199. doi:10.17011/ht/urn.202008245641

Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. In *Proceedings of the ACM Conference on Human-Computer Interaction* (pp. 1–32). New York, NY: Association for Computing Machinery. doi:10.1145/3359183

Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What makes a dark pattern . . . dark? Design attributes, normative considerations, and measurement methods. In *CHI Conference on Human Factors in Computing Systems* (pp. 1–18). Yokohama, Japan: Association for Computing Machinery. doi:10.1145/3411764.3445610

Mulligan, D., Regan, P., & King, J. (2020). The fertile dark matter of privacy takes on the dark patterns of surveillance. *Journal of Consumer Psychology, 30*(4), 767–773. doi:10.1002/jcpy.1190

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing* (pp. 1–13). Honolulu, HI: Association for Computing Machinery. doi:10.1145/3313831.3376321

Paternoster, L. (2018, August 12). Getting round GDPR with dark patterns. A case study: Techradar. *Leon Paternoster*. Retrieved from https://www.leonpaternoster.com/posts/techradar-gdpr/

Preston, N. (2021, August 24). Square eyes: Half of Kiwis addicted to devices, many blame Covid pandemic. *The New Zealand Herald*. Retrieved from https://www.nzherald.co.nz/technology/square-eyes-half-of-kiwis-addicted-to-devices-many-blame-covid-pandemic/MQRQ453EXSB36J5B3LGBNABQUM/

Rossi, A., Ducato, R., Haapio, H., Passera, S., & Palmirani, M. (2019, February 21). Legal design patterns: Towards a new language for legal information design. *JUSLetter IT: Internet of Things—Digital Edition of Proceedings of the 22nd International Legal Informatics Symposium 2019*. Retrieved from https://stefaniapassera.com/wp-content/uploads/2019/03/preprint_LEGAL-DESIGN-PATTERNS.pdf

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design—dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping experiences, shaping society* (pp. 1–12). Tallinn, Estonia: Association for Computing Machinery. doi:10.1145/3419249.3420132

Stock, R. (2021, August 13). Dark arts of supermarket 'loyalty' schemes laid bare. *Stuff*. Retrieved from https://www.stuff.co.nz/business/opinion-analysis/126028294/dark-arts-of-supermarket-loyalty-schemes-laid-bare

Stuff. (2021). *Homepage*. Retrieved from https://www.stuff.co.nz

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)Informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973–990). London, UK: Association for Computing Machinery. doi:10.1145/3319535.3354212

Verbeek, P.-P. (2011). *Moralizing technology: Understanding and designing the morality of things*. Chicago, IL: University of Chicago Press.

Waldman, A. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology, 31*, 105–109. doi:10.1016/j.copsyc.2019.08.025

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London, UK: Profile Books.