UNIVERSITY OF PADOVA

Department of General Psychology

Bachelor's Degree Course in Psychological Science

Final dissertation

Assessing Dark Patterns in Mindfulness Applications

Supervisor
Professor Anna Spagnolli

Candidate: Thu Phuong Nguyen
Student ID number: 2041318

Academic Year 2023-2024

Table of Contents

1. Abstract

Mindfulness applications are on the rise of popularity and are becoming a promising business. The applications promise to users that if they engage with the app, their stress and problems will be at ease. However, there are threats of dark patterns embedding in those mindfulness applications to gain benefit from users without their awareness. This literature review investigates whether dark patterns pose a threat in mindfulness applications. Fogg's Behavior Model and Seven Persuasive Technologies are used as a theoretical framework. It aims to provide insight into dark patterns' definition, classification, and describe how they are embedded in mindfulness applications, as well as their effects on individuals. The present review concluded that there is significant risk of dark patterns being embedded in mindfulness applications. Moreover, limitations and suggested possible future direction are discussed.

2. Introduction

In recent years, mindfulness applications have become extremely popular around the world. There are hundreds of apps dedicated to mindfulness and meditation available online, ready for users to download and use. These apps claim to bring a wide range of wellness benefits to their users, such as better stress management, increased productivity, and improved emotional resilience. The downloading and usage of mindfulness apps especially exploded during COVID-19 when people were under extreme stress. The biggest and most popular mindfulness app, Calm, has 80 million users and is valued at over 1 billion US dollars. It has become a multi-billion dollar industry, with the market size expected to reach USD 4,206.1 million by 2027 (Business Wire, 2021).

Mindfulness applications promote their modern digital environment with the ability to self monitor and tailor programs to users' needs and preferences, and deliver the most suitable solution to users, helping users improve their wellness and overcome personal obstacles like stress and sleeplessness. Many users are attracted to the beneficial promises of meditation apps and become engaged with them. However, along with the promising benefits, these applications are at risk to be manipulated and not put users' benefits as their top priority. The deceptive design strategies known as dark patterns are being embedded in those applications to manipulate users' behaviors and could lead to privacy violations and other harmful consequences. Dark patterns are defined as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something" (ww.deceptive.design). Those dark patterns are being increasingly embedded in various websites and applications.

With individuals spending significant time on websites and apps, serious privacy concerns have grown globally, leading regulatory authorities to closely monitor dark patterns (GPEN, 2024) Coordinated with the International Consumer Protection and Enforcement Network (ICPEN), Global Privacy Enforcement Network (GPEN) process annual global privacy sweep took place between January 29 and February 2, 2024. It involved participants, or "sweepers," from 26 privacy enforcement authorities from around the world. The sweep examined more than 1,000 websites and mobile applications and found that nearly all of them employed one or more deceptive design patterns that made it difficult for users to make privacy protective decisions (GPEN, 2024).

Recognizing the serious risk of dark patterns on privacy and user welfare, this paper aims to assess dark patterns embedded in mindfulness applications in detail.

Section 3 will describe the methodology used to collect the scientific papers for this literature review. Section 4 will present the theoretical framework. Section 5 will identify what dark patterns are in the modern technology world. Section 6 will discuss dark patterns in mindfulness applications. Section 7 will discuss the results and highlight future directions.

3. Methodology

The literature review screening process is guided by PRISMA 2009 Flow Diagram as in Figure 1, divided to 4 stages as follows:

1) Identification: Database research

The main resource in use is the "Scopus" database. The process of searching starts with the search within: "Article title, Abstract, Keywords". The literature search strategy focuses on the dark pattern, manipulation and their relationship in the mindfulness/digital health apps environment. The search terms are combined of keywords: "dark pattern, manipulation, mindfulness, mediation, digital health"

2) Screening

The screening process is start with assessing the research paper abstract and comply with the follow criteria

Inclusion criteria:

- the papers are in English language
- the papers are free access

Exclusion criteria:

- the papers are in other languages
- the papers are not free access

3) Eligibility

At this stage, the papers are in detailed inspection. All the replicated and unrelated papers are being removed. The selected papers need to be related to main elements: dark pattern and manipulation in the mindfulness/digital health apps environment.

Under instruction of the supervisor professor, the information in the papers are being retrieved as follows: name, the key benefit/purpose of Dark Pattern, domain target, action/operation, independent and dependent variables, effect/result.

4) Included

Following detailed examination and excluding irrelevant documents, the final selection includes 14 papers.

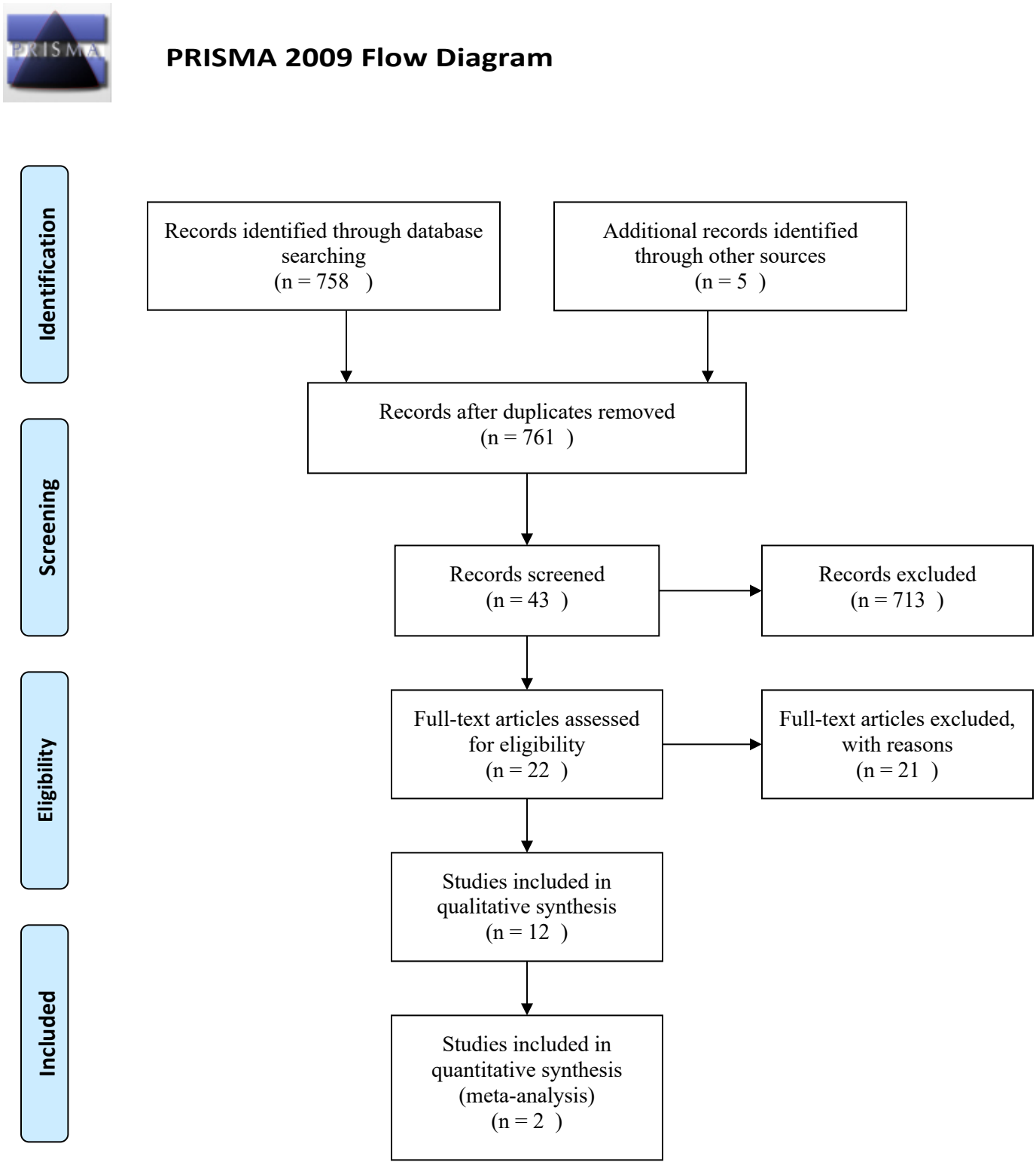


Figure 1. PRISMA Flow Diagram From Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009).

4. Theoretical framework

In order to understand how Dark Patterns function, it's essential to explore the factors influencing human behavior and how persuasive design techniques are applied. Understanding the psychological and behavioral principles is the key to recognizing the mechanism underlying deceptive designs. In this thesis, two major frameworks are discussed: Fogg's Behavior Model, which explain how motivation, ability and trigger shape behavior (Fogg, 2009) and Fogg's Seven Persuasive Technology, which outline the methods commonly used in digital design to manipulate user behavior (Fogg, 2003)

4.1 Fogg's Behavior Model (FBM)

Fogg's Behavior Model, illustrated in Figure 2, states that behavior is a product of three factors: Motivation, Ability and Triggers. In order for a person to perform a specific behavior, the person needs to be motivated and have the ability to perform the behavior, and be triggered to perform the behavior. All three factors need to be present simultaneously for the behavior to occur. If one of these elements is missing, the behavior is not carried out (Fogg, 2009).

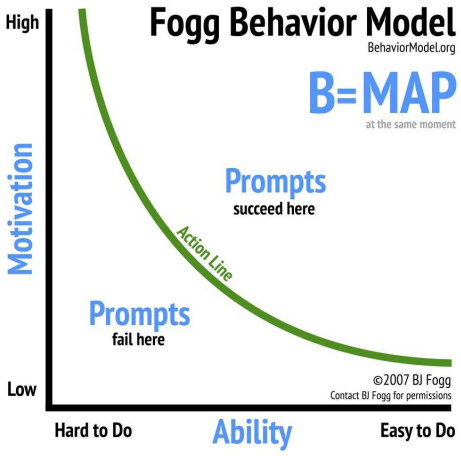


Figure 2: Fogg's Behavior Model

Motivation is the underlying drivers that motivate behavior. There are three core motivators with two sides of dimensions. The first core motivators are the dimension of pleasure and pain. This motivator elicits instant response with little thought or anticipation. The second motivator dimension is hope and fear. This dimension is all about expecting a certain result. Hope is the expectation of good outcome and fear is expectation of bad outcome. The third motivator dimension is social acceptance and social rejection. This dimension governs most of our social behavior. Individuals are driven to take actions that will get them acceptance in society. According to FBM, increased motivation is usually not the main focus, instead, increasing ability (make the behavior simpler) is the main path to target behavior. Even if the motivation is low, people can still perform the behavior if the behavior is simple and easy to perform. Simplicity changes behavior. Elements of ability are time, money, physical effort, cognitive effort, social norms and non-routine. Those elements vary by the individual and also context. Triggers are external factors that affect how a person carries out the desired behavior. Triggers could be understood as cues or calls to actions. There are three types of triggers: sparks, facilitator or signal. Spark could be used in situations that require leverage motivation. Facilior is to inform users that the behavior is easy to perform. Signal is simply a reminder (Fogg, 2009).

In the persuasive design's context, motivation could be our desire to get social connection or social acceptance, which initially leads us to start engaging in an app. Ability could be how easy it is to perform a task on an app. Triggers could be simply notifications or reminders at the right moment to engage a behavior. Together, motivation, ability, and trigger form the foundation of persuasive design strategies.

4.2 Fogg's Seven Persuasive Technologies

Further from the FBM and specific in the digital environment context, persuasive designs have been utilized to steer users' behaviours. According to Fogg, persuasive design is defined as "any interactive product designed to change attitudes or behaviours by making desired outcomes easier to achieve" (Fogg, 2003). Aligned with the ability aspect of FBM, increasing users' ability by simplifying actions is key to achieving target behaviors. Simplicity is a powerful driver of behavior change. Fogg identifies seven strategies often used in persuasive technologies, which are:

Reduction, Tunneling, Customization/tailoring, Suggestion, Self-monitoring, Surveillance and *Conditioning*. Each technology applies a different strategy to change attitudes or behaviors and in reality, a persuasive product is often the result of two or more technologies combined (Fogg, 2003).

Reduction technology eliminates some steps to simplify tasks , making it easier to achieve target goals. Based on psychological and economic theories, humans usually seek to minimize costs and maximize gains. Therefore, reduction technology works on the principle that simplifying a behavior improves its benefit/ cost ratio and increases motivation to repeat those behaviors (Fogg, 2003).

Tunneling technology is designed to reduce uncertainty or confusion by leading users through a clear, step-by-step process to achieve a particular behaviour. Tunneling technologies are effective because people value consistency. Once they commit to a process, they tend to follow through, even when faced with contradictory information (Fogg, 2003).

As studies show that people tend to pay more attention to the personalized information, *customization/tailoring* technologies designed products tailored to users' information, encouraging changes in attitudes or behaviours. Customization/tailoring technology makes it easier for users to find relevant content without dealing with irrelevant information. This is effective because personalized messages attract more attention, leading to deeper thinking, and if convincing, create greater persuasion (Fogg, 2003).

Suggestion technology identifies the “Right Time" to intervene, since people are more motivated to perform some actions during certain moments, and deliver reminders to prompt users' behaviour. Suggestion technologies build on existing motivations, like financial stability, health, or admiration from others. They work by cueing relevant actions with prompts like, ‘Now would be a good time to do X.’(Fogg, 2003)

Self-monitoring technology allows individuals to monitor themself, enabling them to modify certain attitudes or behaviours to achieve desired goals. The goal is to remove the burden of measuring and tracking performance. This makes it easier for people to understand how they are doing, increasing the likelihood of continuing the behavior. In addition, self-monitoring

technologies feed the natural human drive for self-understanding, like personality or aptitude tests (Fogg, 2003).

Knowing that people behave differently under observation, *surveillance* technologies allow one party to observe and modify the other party's behaviour. Surveillance has long been an active research topic in social psychology, with consistent findings that observation has strongly affected how people behave. When people know they're being watched, they behave differently. According to the research, if one party can observe and can reward or punish another party's actions, the observed party is likely to make their actions align with the observer's expectations (Fogg, 2003)

Conditioning technology is using operant conditioning, often in the form of positive reinforcement, to reinforce target behaviours when they occur. Operant conditioning can be used not just to reinforce behavior but to shape complex behaviors. Shaping is a process of reinforcing behaviors that approximate the target behavior (Fogg, 2003).

Fogg's Seven Persuasive Technologies are tools that could apply to influence users' behavior. *Reduction* could simplify or hide key information, leading users to accidentally agree to a subscription or purchase that they don't want. *Tunneling* can complicate the process, making it harder for users to unsubscribe or delete accounts. *Customization/tailoring* can be used to present personalized options to users, encourage engagement and benefit the platform more than users. Through *Suggestion*, designers create a false sense of urgency, pressuring users to purchase with warning about miss out discounts. *Self-monitoring* has been applied in gamification to misrepresent achievement, making users stay engaged or purchase upgraded features. *Surveillance* can be applied to give negative feedback or remind users to continue using the program. *Conditioning* appears as a free trial with false compliments or rewards given to users , nudging users into purchasing after trial ends.

5. What is Dark Patterns

5.1 The definition of Dark Patterns

The term Dark Pattern was coined by Harry Bignull via his website Darkpattern.org in 2010. He defined Dark Pattern as *"a user interface that has been carefully crafted to trick users into doing things...they are not mistakes, they are carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind"*. Recently, in 2022, Bignull has updated the definition and referred to it also as deceptive pattern design: *"Deceptive patterns (also known as "dark patterns") are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."* Based on Bignull's original definition, other scholars and user experience practitioners extend it further with specific and clear aspects. Gray et al.(2018), defined Dark Patterns as "*define instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest"* (Gray et al., 2018). Maier and Harr describe Dark Patterns as "*functionality, drawing on psychological insights, implemented within user interfaces that is deceptive to users and in not in their best interests*".

Marthur proposed that there is no single definition of Dark Patterns but rather common components that can be used to describe or categorize Dark Patterns. According to Marthur et al.(2021), Dark Patterns can be defined by four facets: characteristics of the user interface that can affect users, mechanism of effect for influencing users, the role of the user interface designer and benefits and harms resulting from a user interface design (Marthur et al., 2021). The first facet focuses on characteristics of the user interface that can affect users like trick or misleading interfaces. Some definitions feature alternative characteristics as "coercing, steering, or deceiving" (Marthur et al., 2019) or "obnoxious, coercive, or deceitful" (Gray et al., 2018). The second facet of definitions is the mechanism of effect for influencing users such as subverting user intent or preference, tricking users or undermining autonomy. Many definitions specify multiple mechanisms of effect on users like manipulation, exploitation, or attack (Marthur et al., 2021). The third facet is the role of the user interface designer. Several definitions focus on how designers abuse their knowledge of human behavior or intentionally deploy dark patterns to achieve a goal (Marthur et al., 2021). The fourth facet of dark pattern definitions is the benefits and harms

resulting from a user interface design such as aiming to benefit an online service or involve harm to users (Marthur et al., 2021). As shown in Figure 3, Marthur et al., 2021 presents a classification of various Dark Patterns' definitions in academic, literature, law and policy based on the four facets.

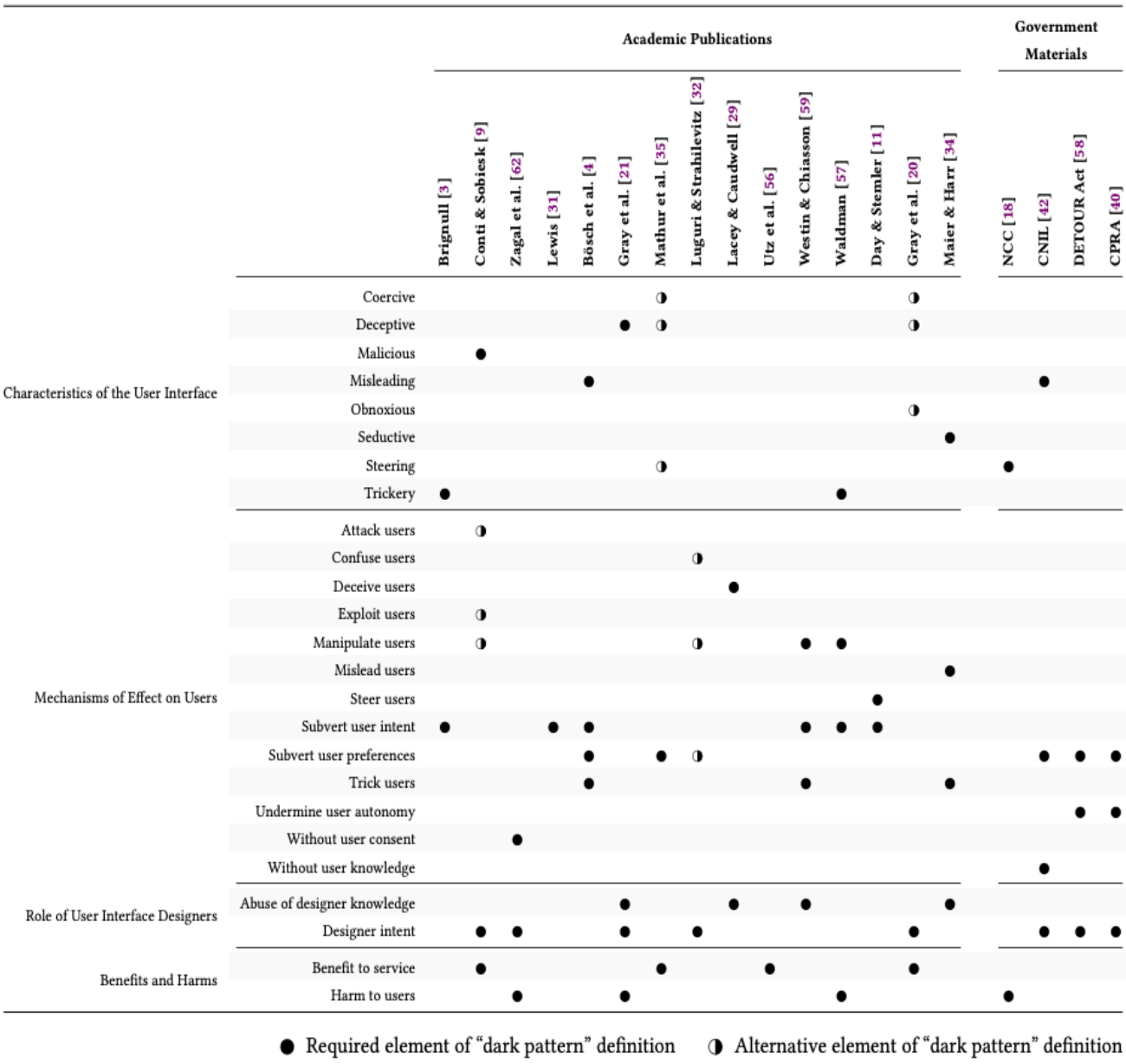


Figure 3. A classification of various "dark pattern" definitions in academic literature, law, and policy from Marthur et al., 2021

5.2 The classification of Dark Patterns

Based on Bignull's initial 12 types of Dark Patterns, Gray came up with five primary categories of Dark Patterns that appeared to serve as strategic motivators for designers: Nagging, Obstruction, Sneaking, Interface Interference, and Forced Action (Gray et al., 2018) as in Figure 4.

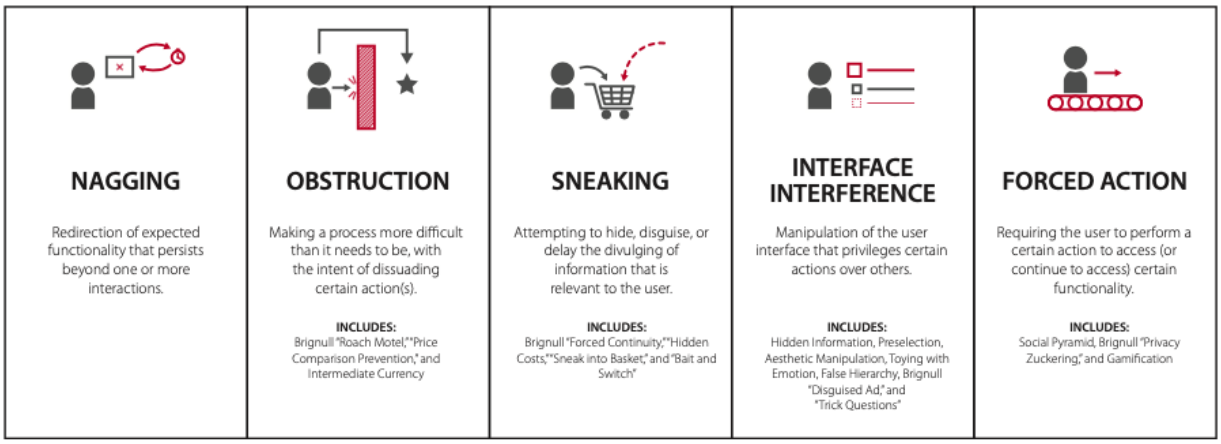


Figure 4. Summary of dark pattern strategies from Gray et al., 2018.

Nagging: redirection of expected functionality that persists beyond one or more interactions 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 (Gray et al., 2018). Nagging usually serves as an interruption to users' way of approaching a goal. Examples are pop-ups that obscure the interface, auto play video or audio that is not desired.

Obstruction: making a process more difficult than it needs to be, with the intent of dissuading certain actions (Gray et al., 2018). An example is how applications make it difficult to cancel membership or subscription. Obstruction comes up with 3 subtypes: Roach Motel, Price Comparison Prevention, Intermediate Currency.

Sneaking: attempting to hide, disguise, or delay the divulging of information that is relevant to the user (Gray et al., 2018). An example is the X button on the interface that does not close the window but leads to another unexpected action. Subtypes are Forced Continuity, Hidden Cost, Sneak into Basket and Bait and Switch

Interface Interference: manipulation of the user interface that privileges certain actions over others (Gray et al., 2018). Interface Interference's subtypes include Hidden Information,

Preselection and Aesthetic Manipulation. Aesthetic Manipulation also comes up with four specific instantiations: Toying with Emotion, False Hierarchy, Disguised ad, and Trick Questions.

Forced action: requiring the user to perform a certain action to access (or continue to access) certain functionality (Gray et al., 2018). Forced Action has subtypes which are Social Pyramid, Privacy Zuckering and Gamification.

The following table shows details of 5 main types of Dark Patterns with subtypes and examples in user interface.

Dark Pattern	Subtypes	Description	Action in apps
Nagging		Redirection of expected functionality that persists beyond one or more interactions	Messages that asking users to turn on notifications for the app Only two options are present, "Not Now" and "OK"
Obstruction	Roach Motel	Make it difficult to close an account	Apps creates many layers or steps making it's complicated and difficult to close account
	Price Comparison Prevention	making direct price comparisons between products and services difficult	Making important product information (product ID, price) uncopyable
	Intermediate Currency	users spend real money to purchase a virtual currency which is then spent on a good or service	In-app purchase for mobile games
Sneaking	Forced Continuity	continues to charge the user after the service they have purchased expires	continue the paid service or upgrade to the paid version of the free trial and charge the user.
	Hidden Costs	provides users with a late disclosure of certain costs	a certain price is advertised for a good or service, only to later be changed due to the addition of taxes and fees, limited time conditions, or unusually high shipping costs
	Sneak into Basket	adds items not chosen by the user to their online shopping cart, often claiming to be a suggestion based on other purchased items	adds an unwanted item into the cart
	Bait and Switch	a certain action will cause a certain result, only to have it cause a different, likely undesired result	A button to buy more moves is positioned in the same location where a button to start a new game is normally positioned,
Interface Interference	Hidden Information	options or actions relevant to the user but not made immediately or readily accessible	options or content hidden in fine print, discolored text, or a product's terms and conditions statement When a user registers for an account, they are given an option to accept the terms and conditions above a long list of small text. Hidden within this text is a small

			checkbox to opt out of the bank selling the user's information.
	Preselection	an option is selected by default prior to user interaction.	preselects the option for information sharing and email subscription when register
	Aesthetic Manipulation	any manipulation of the user interface that deals more directly with form than function	design choices that focus the user's attention on one thing to distract them from or convince them of something
	Toying with Emotion	any use of language, style, color, or other similar elements to evoke an emotion in order to persuade the user into a particular action	cute or scary images, or as enticing or frightening language
	False Hierarchy	gives one or more options visual or interactive precedence over others, particularly where items should be in parallel rather than hierarchical	The "custom" option in the app is designed in a way that gives the user the false impression that the option is disabled.
	Disguised ad	ads disguised as interactive games, or ads disguised as a download button or other salient interaction the user is looking for.	a click on any part of the site loads another page, effectively rendering the entire site an ad
	Trick Questions	includes a question that appears to be one thing but is actually another, or uses confusing wording, double negatives, or otherwise leading language to manipulate user interactions.	checkboxes to opt out rather than opt in, often paired with confusing double negatives
Forced action	Social Pyramid	requires users to recruit other users to use the service.	The game incentivizes users to invite their friends to the game by making some features or goals inaccessible without online connections that also play the game
	Privacy Zuckering	tricks users into sharing more information about themselves than they intend to or would agree to	in-apps questions that collect excessive data
	Gamification	situations in which certain aspects of a service can only be "earned" through repeated (and perhaps undesired) use of aspects of the service	If the player doesn't purchase anything from the game, they will have to play the game for a longer period of time in order to achieve the same result they would have from paying.

Table 1. Details of dark pattern strategies with its subtypes and examples from Gray et al., 2018.

5.3 The concern of Dark Patterns' effect

Several cautions have been raised about what Dark Patterns' potential negative impact on individuals, business and society at large. According to Marthur et al. (2021), he discussed that there are four normative perspectives that Dark Patterns have affected on which are: Individual

Welfare, Collective Welfare, Regulatory Objectives and Individual Autonomy. This thesis will focus on Individual Welfare. The Individual Welfare normative lens focuses on the adverse effect of Dark Pattern on individual consumer welfare. Marthur et al discussed that there are three kinds of individual welfare that are being diminished by Dark Patterns: Financial loss, Invasion or Privacy and Cognitive Burden. Financial Loss is the most straightforward consequence of Dark Patterns on individual consumers. Businesses often apply Dark Patterns on their interfaces pushing consumers to spend more than they mean to. Examples of such interfaces include those that profit from users by adding products into shopping carts without users' consent (Sneak into Basket) and those that mislead users into believing they are signing up for a one-time offer or free trial when in reality they are signing up for recurring fees (Marthur et al., 2021). Cognitive Welfare is when Dark Patterns on various interfaces cause users to spend unnecessary time, energy and attention. Examples of such interfaces include those that obstruct users from canceling subscription or delete accounts by complicating the process (Roach Motel).

Invasion of Privacy is when the Dark Pattern alters privacy of users. Examples of such interfaces include privacy-invasive defaults that expose user data (Preselection), privacy-respecting choices that are hard to access (Privacy Zuckering, Interface Interference, and Obstruction) (Marthur et al., 2021). Invasion of Privacy is a serious concern and being mainly focused by many researchers and regulatories. GPEN Report stated that many websites and apps employ techniques that interfere with individuals' ability to make choices that best protect their privacy or consumer rights. GPEN specifically found that more than 89% of privacy policies were found to be long or use complex language suited for those with a university education. When asking users to make privacy choices, 42% of websites and apps used emotionally charged language to influence decisions, while 57% made the least privacy protective option the easiest to select. Additionally, 35% of websites and apps repeatedly asked users to reconsider deleting their account, and in nearly 40% of cases, users faced obstacles accessing privacy options. Finally, 9% of websites and apps required more personal information for account deletion than for account creation. In line with the GPEN's report, Iwaya et al. (2023) investigated 27 popular mental health apps and discovered significant privacy concerns. They found out that most apps expose users to privacy threats as 3rd parties can link, identify, and detect users' actions and data. Moreover, the majority of apps' privacy policies were identified to require at least college-level education to fully understand them, leading users

unaware about the nature of the data processing activities in mental health apps, data controllers, and service providers.

5.4 Dark Patterns in mobile modality

Recent studies have found Dark Patterns in different platforms, including desktop websites, mobile websites and mobile apps. Between modalities, mobile apps are found to be the most affected from Dark Patterns. Genorimo et al. (2020) analyzed 240 apps belonging to 8 different categories on the Google Play Store and manually identified and classified dark patterns they included, finding that 95% of the analyzed apps contain one or more Dark Patterns. The research identifies 1,787 Dark Patterns across all apps, and nearly half (49%) of the apps were found to contain 7 Dark Patterns on average. Gunawan et al., (2021)'s findings are consistent with the Genorimo's work, but goes further, showing that dark pattern usage frequently differs across the versions of a given service. According to Gunawan et al., (2021), apps tend to have more unique dark patterns than their web counterparts, and apps tend to include different patterns than the corresponding websites. The research also highlight that popular apps tend to include slightly more types of dark patterns overall. Figure 5 illustrates the percentage of Dark Patterns across various categories and modalites, which apps have highest rates.

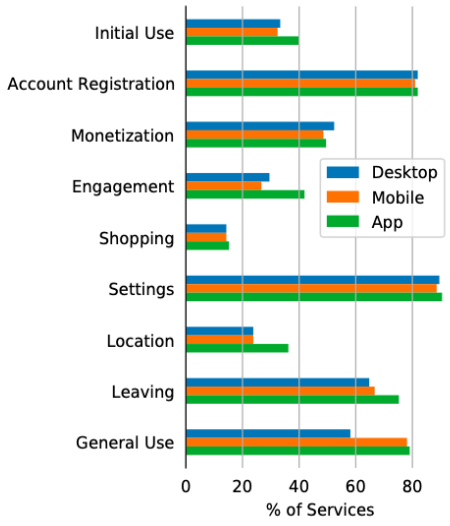


Figure 5. Bar chart of the percentage of services that contain at least one dark pattern from different categories, broken down by modality from Gunawan et al., 2021.

Findings also revealed that users are often unaware of the presence of Dark Patterns embedded in apps. Geronimo et al conducted an online experiment with 584 participants to examine Dark Pattern blindness. The outcome highlighted that most of the time users could not perceive the presence of deceptive designs or not be sure about it. Some participants even stated that Dark Patterns are so widely spread and common among modern applications that they become part of the normal interaction flow when using apps (Geronimo et al., 2020). Consistent with the findings of Geronimo et al, Maier and Harr discover that users are partially aware of the existence of deceptive designs, but unaware of the total number and frequency of them. Moreover, despite being aware of persuasive and manipulative techniques, users keep using these services, making excuses why it still has benefits for them (Maier & Harr, 2020). This is concerning because individuals and societies are gradually accepting and normalizing deceptive designs.

6. Dark Patterns in Mindfulness Applications

6.1 Balance app as case study

In this section, Dark Patterns in mindfulness applications will be assessed. With the growing popularity of mindfulness applications, there are several critical works addressing the deceptive designs in those applications. In their report, Paterson and Ananthapadmanaban identified Dark Patterns such as Nagging, Forced to continue, Toying with emotion in Headspace, Calm and other popular mindfulness applications. This study employs a focused case study approach, providing an in-depth and detailed analysis of an chosen app. The chosen case study is the Balance app, a modern mindfulness application that claims to offer multiple personalized meditation sessions tailored to users' needs. Balance app advertises it is "*created an innovative, personalized meditation experience that helps people improve their stress, sleep, focus, mood, and more"* (Balance app). Balance app specifically highlights its personalization experience to users, promoting with the personalization and time spent on Balance app, the meditation will be more effective *"The more you share with the Balance app over time, the more personalized and effective your meditations become."* (Balance app). In the Dark Patterns' framework, Balance app presents an extreme case of Privacy Zuckering and Hidden Information, as it gathers significant personal information under the disguise of "Personalization". Figure 6 presents the Balance app's website, where "Personalization" is prominently featured in its advertising strategy.

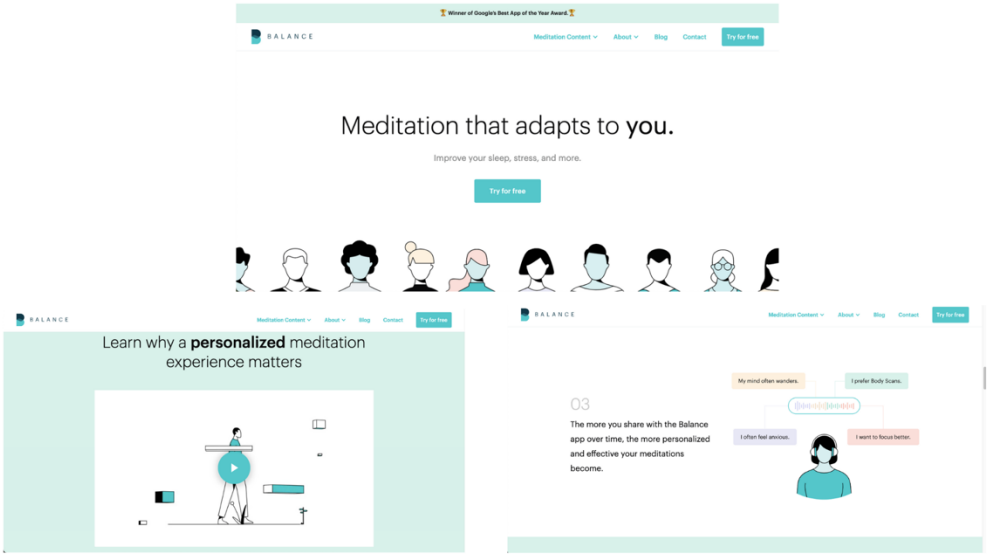


Figure 6. Balance app website and introduction www.balanceapp.com

6.2 Assessing Dark Patterns embedded in Balance app

6.2.1 Nagging

During the registration process, Balance app repeatedly requests users to enable notifications as in Figure 7. If users choose “Don’t Allow", the request will keep appearing.

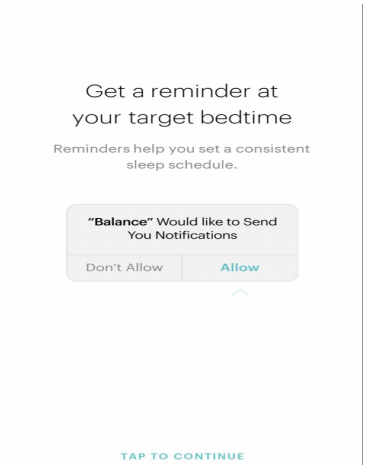


Figure 7. Balance app asking to allow notifications

Before starting any meditation session, users are obligated to complete information retrieval questions as in Figure 8, even if the user already answered similar ones in prior sessions. There is no skipping option, users have to choose one of the answers.

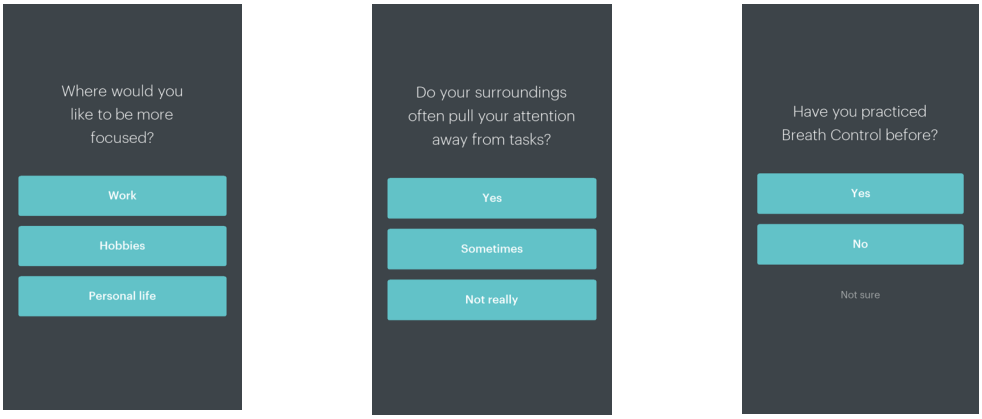


Figure 8. Balance app asking user to answer questions before mediation sessions

Balance constantly sending promotion emails, creating an illusion of users will miss out offers if not purchased intermediately, as shown in Figure 9.

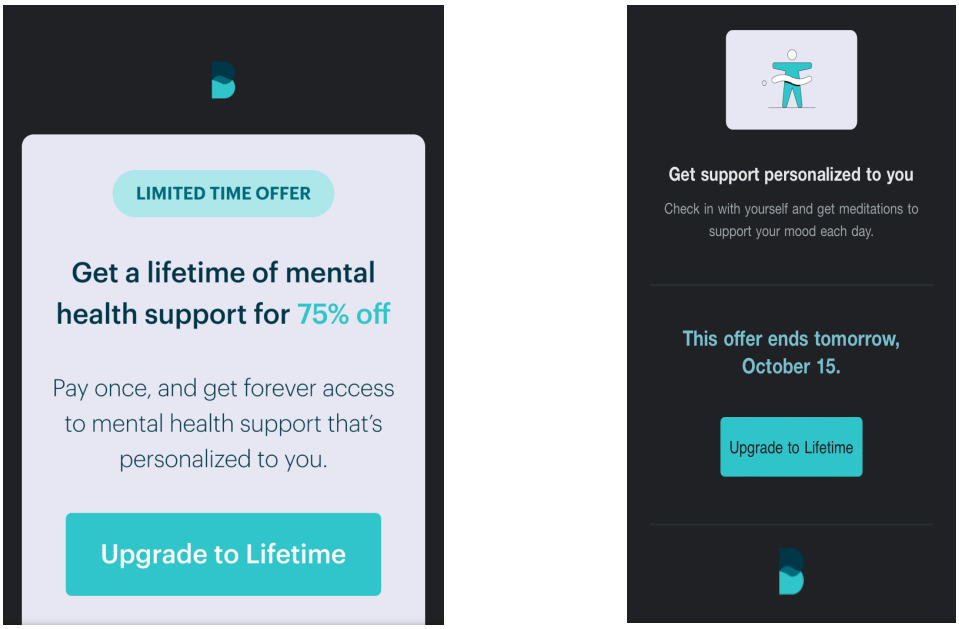


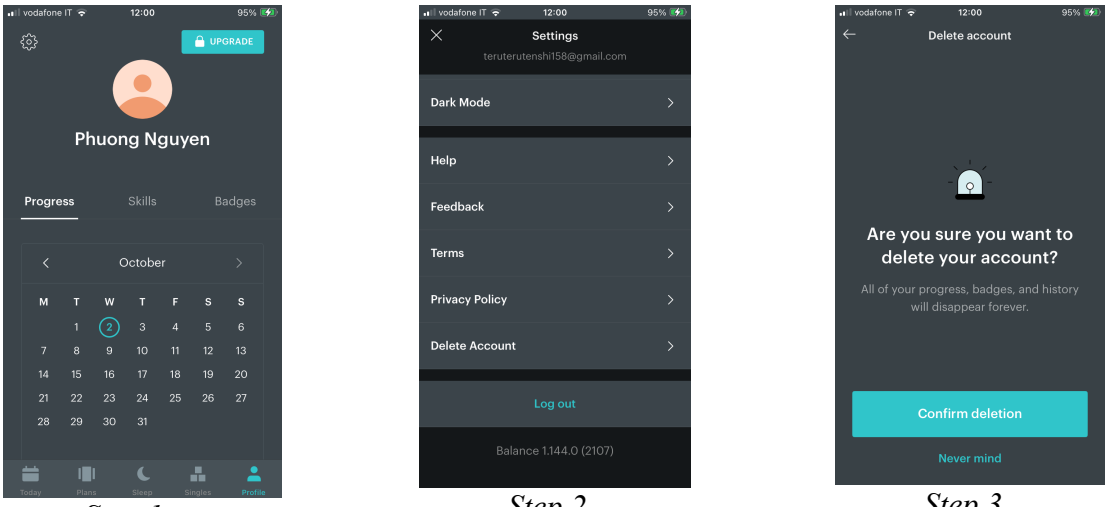
Figure 9. Balance app constantly send promotion to users

6.2.2 Obstruction

Roach Motel

A. Delete account

When users want to delete their account, they must go through multiple steps as shown in Figure 10. First, users have to go to the profile section at the bottom right of the app. Second, users have to navigate the setting button which is the tiny gear icon at the top left of the app. Next users must click the gear icon and need to scroll to the bottom of the menu to find the delete option. After selecting the delete option, they need to confirm the deletion one final time.

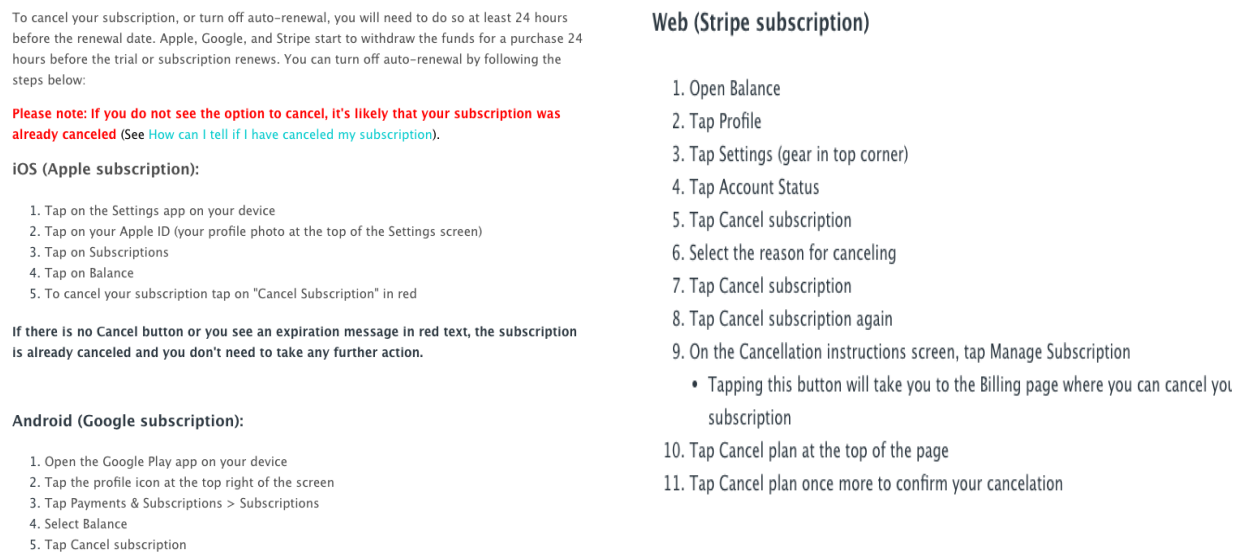


Step.1 *Step.2* *Step.3*

Figure 10. Delete account steps

B. Unsubscribe

As in Figure 11, each modality has a different process for unsubscribing from the Balance service, which can be confusing. For each modality, there's a minimum 5 steps to cancel the subscription. There’s another important point that users may not realize that deleting the app or account doesn’t stop the subscription, and they may continue to be charged.



To cancel your subscription, or turn off auto-renewal, you will need to do so at least 24 hours before the renewal date. Apple, Google, and Stripe start to withdraw the funds for a purchase 24 hours before the trial or subscription renews. You can turn off auto-renewal by following the steps below:

Please note: If you do not see the option to cancel, it's likely that your subscription was already canceled (See How can I tell if I have canceled my subscription).

iOS (Apple subscription):

1. Tap on the Settings app on your device
2. Tap on your Apple ID (your profile photo at the top of the Settings screen)
3. Tap on Subscriptions
4. Tap on Balance
5. To cancel your subscription tap on "Cancel Subscription" in red

If there is no Cancel button or you see an expiration message in red text, the subscription is already canceled and you don't need to take any further action.

Android (Google subscription):

1. Open the Google Play app on your device
2. Tap the profile icon at the top right of the screen
3. Tap Payments & Subscriptions > Subscriptions
4. Select Balance
5. Tap Cancel subscription

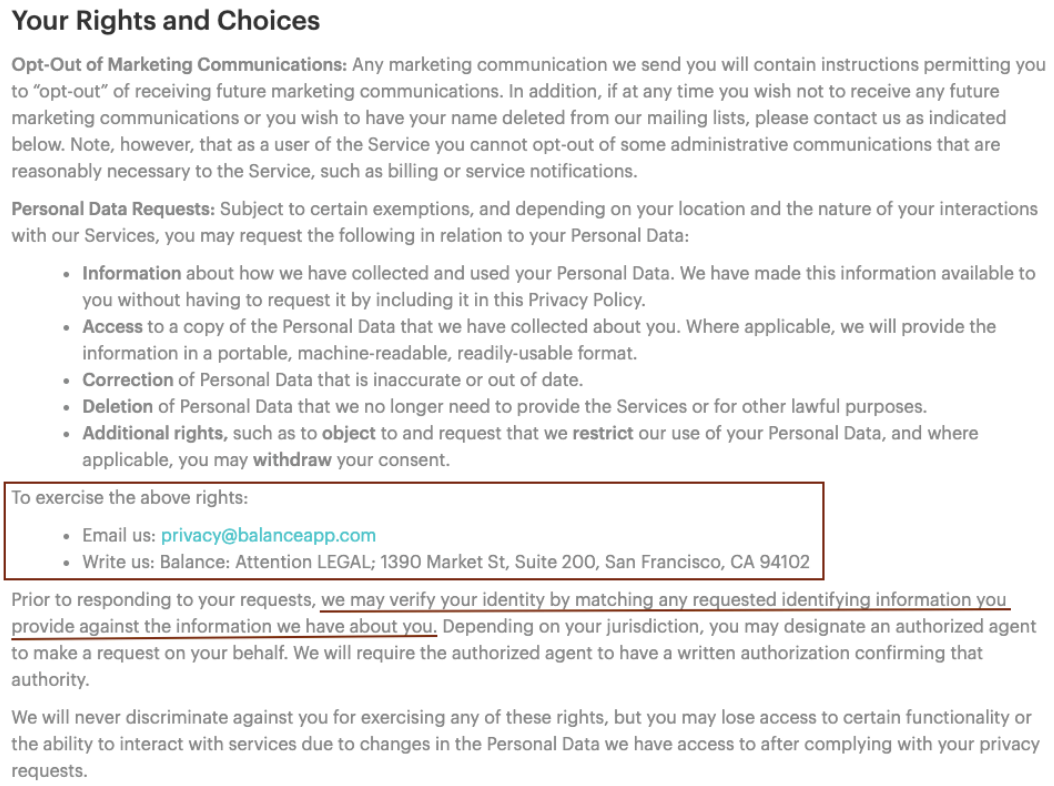
Web (Stripe subscription)

1. Open Balance
2. Tap Profile
3. Tap Settings (gear in top corner)
4. Tap Account Status
5. Tap Cancel subscription
6. Select the reason for canceling
7. Tap Cancel subscription
8. Tap Cancel subscription again
9. On the Cancellation instructions screen, tap Manage Subscription
   - Tapping this button will take you to the Billing page where you can cancel you subscription
10. Tap Cancel plan at the top of the page
11. Tap Cancel plan once more to confirm your cancelation

Figure 11. Instruction to unsubscribe for differents modalities

C. Personal Data Deletion

Even after users delete their accounts or unsubscribe, the Balance app retains and uses their private information. In order to completely delete their data, users need to send a request email to Balance, as the app doesn't have an auto delete option. Additionally, Balance app intentionally complicates the process further by requiring users to verify their identity before proceeding. The challenges users face when exercising their rights over personal information strikingly contrast with the simplicity of Balance's account registration. Figure 12 shows the delete data instruction.



Your Rights and Choices

Opt-Out of Marketing Communications: Any marketing communication we send you will contain instructions permitting you to "opt-out" of receiving future marketing communications. In addition, if at any time you wish not to receive any future marketing communications or you wish to have your name deleted from our mailing lists, please contact us as indicated below. Note, however, that as a user of the Service you cannot opt-out of some administrative communications that are reasonably necessary to the Service, such as billing or service notifications.

Personal Data Requests: Subject to certain exemptions, and depending on your location and the nature of your interactions with our Services, you may request the following in relation to your Personal Data:

- **Information** about how we have collected and used your Personal Data. We have made this information available to you without having to request it by including it in this Privacy Policy.
- **Access** to a copy of the Personal Data that we have collected about you. Where applicable, we will provide the information in a portable, machine-readable, readily-usable format.
- **Correction** of Personal Data that is inaccurate or out of date.
- **Deletion** of Personal Data that we no longer need to provide the Services or for other lawful purposes.
- **Additional rights,** such as to **object** to and request that we **restrict** our use of your Personal Data, and where applicable, you may **withdraw** your consent.

To exercise the above rights:

- Email us: privacy@balanceapp.com
- Write us: Balance: Attention LEGAL; 1390 Market St, Suite 200, San Francisco, CA 94102

Prior to responding to your requests, we may verify your identity by matching any requested identifying information you provide against the information we have about you. Depending on your jurisdiction, you may designate an authorized agent to make a request on your behalf. We will require the authorized agent to have a written authorization confirming that authority.

We will never discriminate against you for exercising any of these rights, but you may lose access to certain functionality or the ability to interact with services due to changes in the Personal Data we have access to after complying with your privacy requests.

Figure 12. Instruction for user to control data

6.2.3 Sneaking

Force continue

When signing up for a trial account, users must provide a payment method—usually a credit card—and agree to automatic subscription renewal as illustrated in Figure 13. If they don't cancel before the trial expires, they'll be charged automatically.

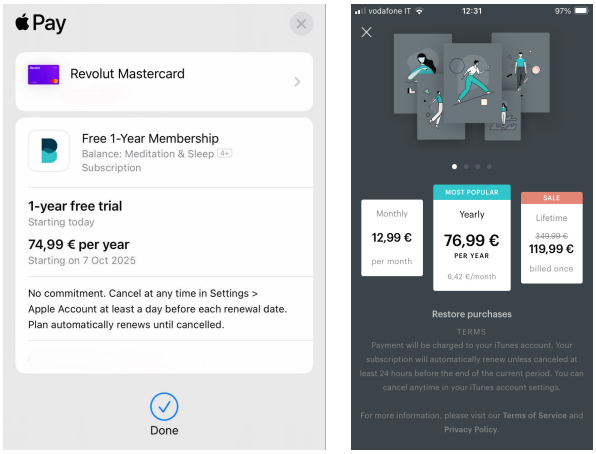


Figure 13. Subscription renewal agreement

6.2.4 Interface interference

Hidden Information

A. Registration process

In the Balance app, during the registration process, the app does not provide consent checkboxes to confirm agreement with the Terms of Service and Privacy Policy. When assessing the registration process for both website and mobile phone, users first answer information retrieval questions, create an account, agree to a trial period and subscribe to membership without agreeing to terms and conditions. Users get distracted by an aesthetic and mesmerizing visual process combined with the advertising of personalization programs. This results in users not recognizing there are no checkbox options for terms of service as well as privacy policy and go straight to giving payment information and subscription. The registration process is displayed at Figure 14, same process for both website and mobile app.

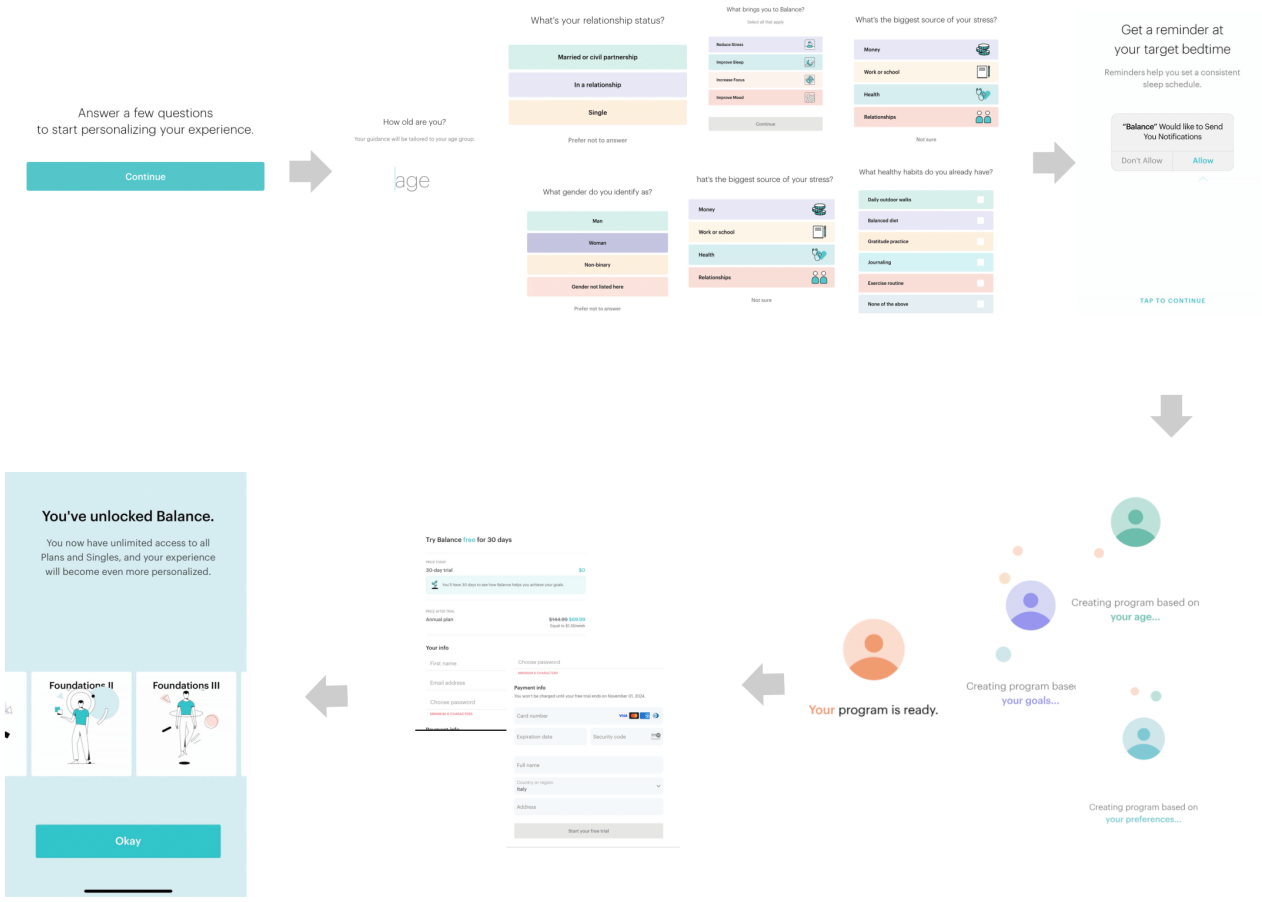


Figure 14. Registration process

B. Terms of Service navigate

Before subscribing and installing the app, Balance app makes it difficult to find the Terms of Services and Privacy Policy. To find the Terms of Service, users click on the 'About' section, then go to the 'Help' section, and scroll to the bottom right to find the Terms of Service. Clicking on this link opens a page that includes 'Where can I find the Balance Terms of Service?' After clicking that link, it directs users to another site where users must again click on 'You can find the Balance Terms of Service on our website by clicking here,' before finally seeing the terms. The process is illustrated in Figure 15. Once users register an account and subscribe to membership, users can go to profile, then click to the gear icon, scroll down and find the Terms of

Service as well as Privacy Policy. This is problematic because the Terms of Service and Privacy Policy should be transparently presented for users to review before agreeing.

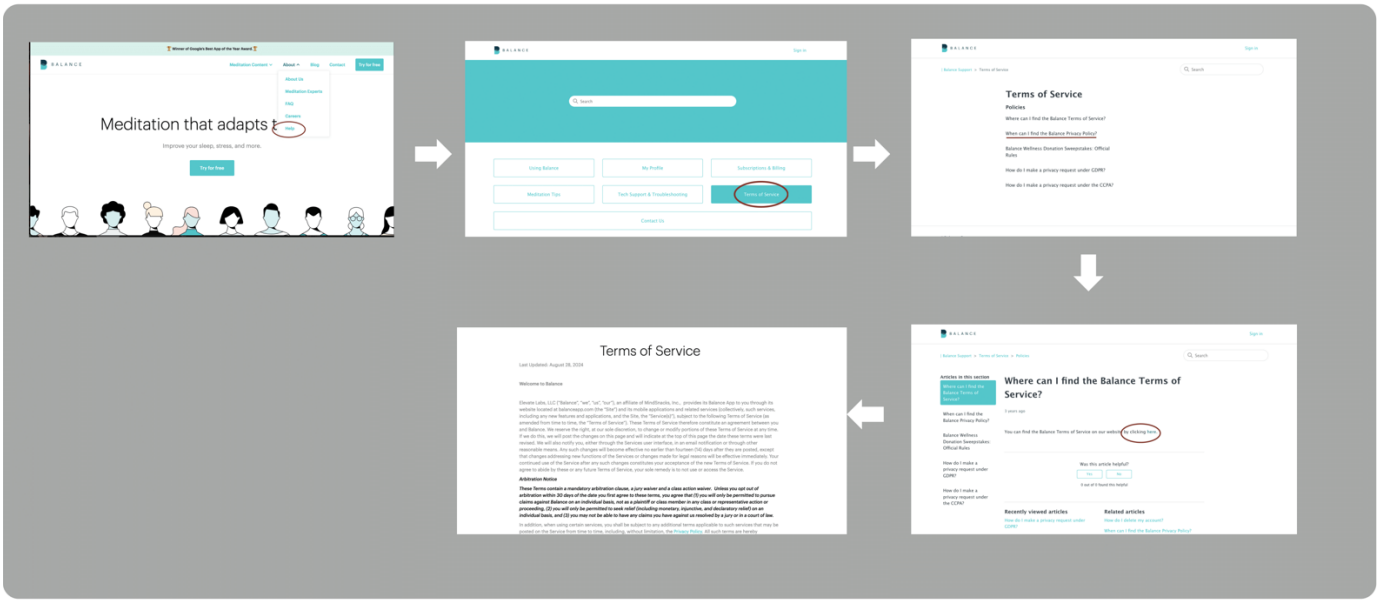


Figure 15. Terms & Service location process

C. Data control section navigate

As discussed in the Nagging session, users need to send a request email to Balance to control or delete their personal data. However, this information is hard to locate. The process for locating this information is similar to finding the Terms of Service, as illustrated in Figure 16. First, users click on the 'About' section, then go to the 'Help' section, and scroll to the bottom right to find the Terms of Service. Clicking on this link opens a page that includes 'Where can I find the Balance Privacy Policy?' After clicking that link, it directs users to another site where users must click on 'You can find the Balance Policy on our website by clicking here,'. When the Privacy Policy finally appears, users need to scroll down and carefully search to find the data control and deletion session and the email address. This is the only way to control or delete data, as it cannot be done in the app.

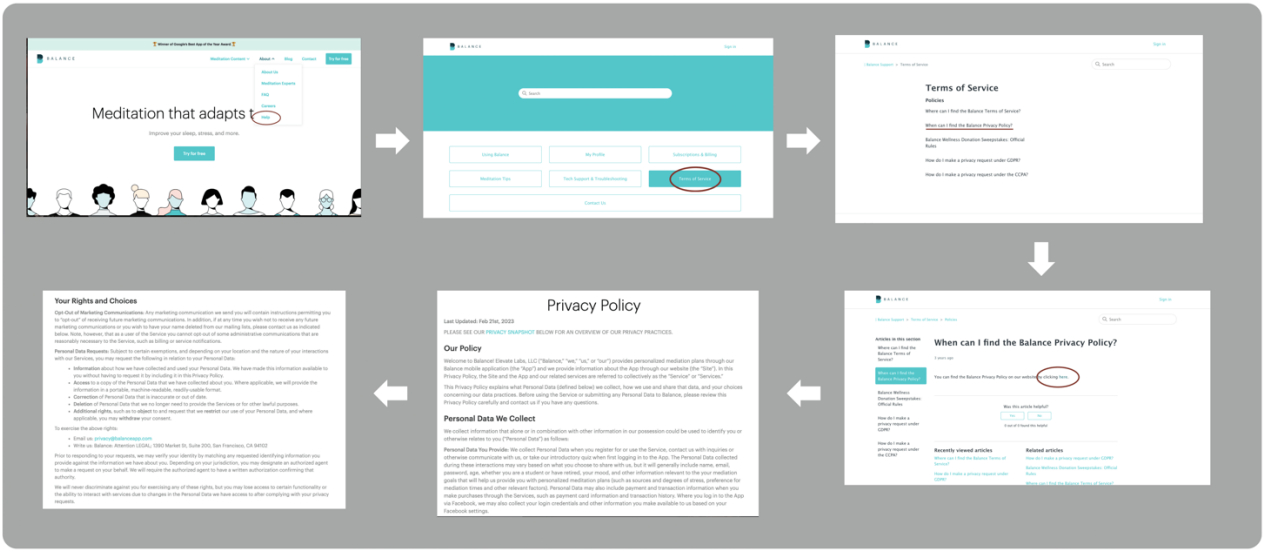
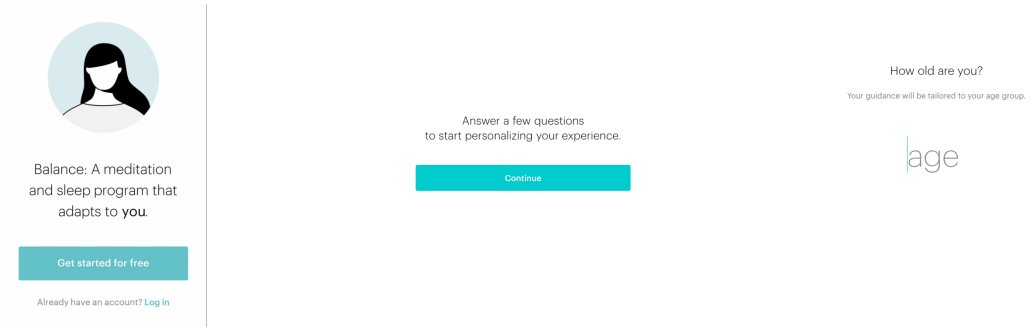


Figure 16. Data control and deletion process

6.2.5 Forced action

Privacy Zuckering

Balance app is a strong example of Privacy Zuckering collecting users' data through the “Personalization" starting from the registration step. Figure 17 displays the data required by Balance to create a “Personalization" plan adapted to each user. The required information varies from age, gender, relationship status, student status, stress related to healthy habits etc.



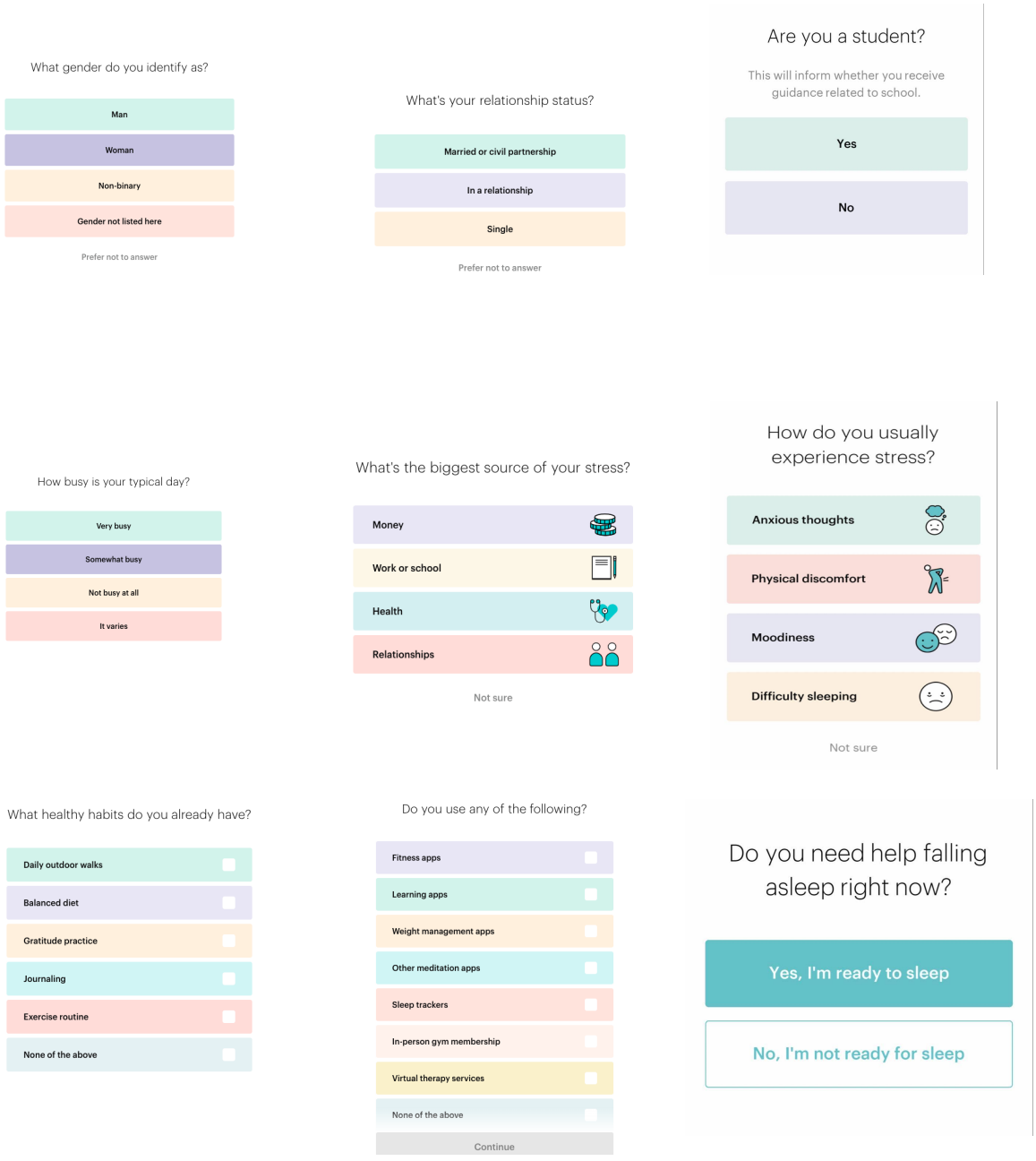


Figure 17. Balance App registration retrieval information questions

However, not just the registration, for each mediation session, Balance constantly asks users to answer retrieval information questions to continue using it. Users are obligated to answer those questions to start the meditation sessions and cannot skip them. The questions include stress levels, meditation frequency, sleep quality, lifestyles and similar topics. Figure 18 illustrates the process and Figure 19 displays some examples of the questions.

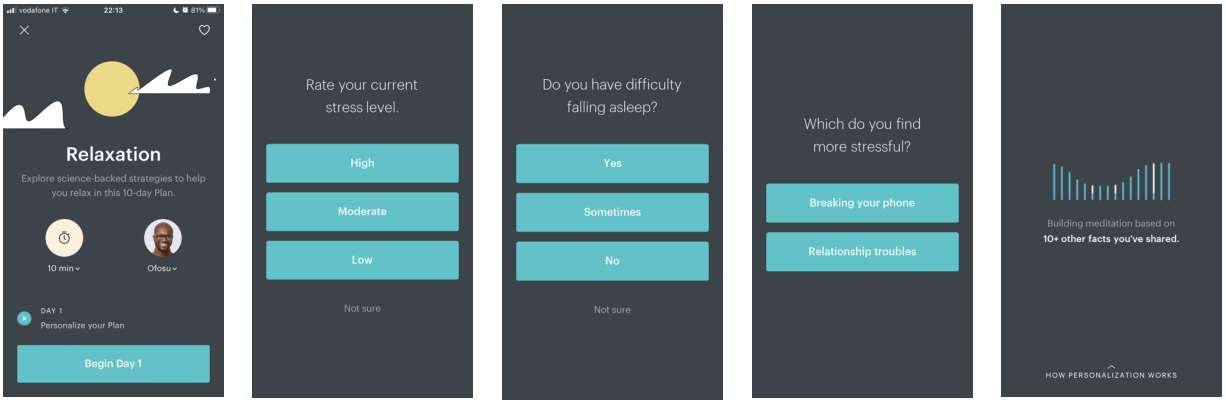
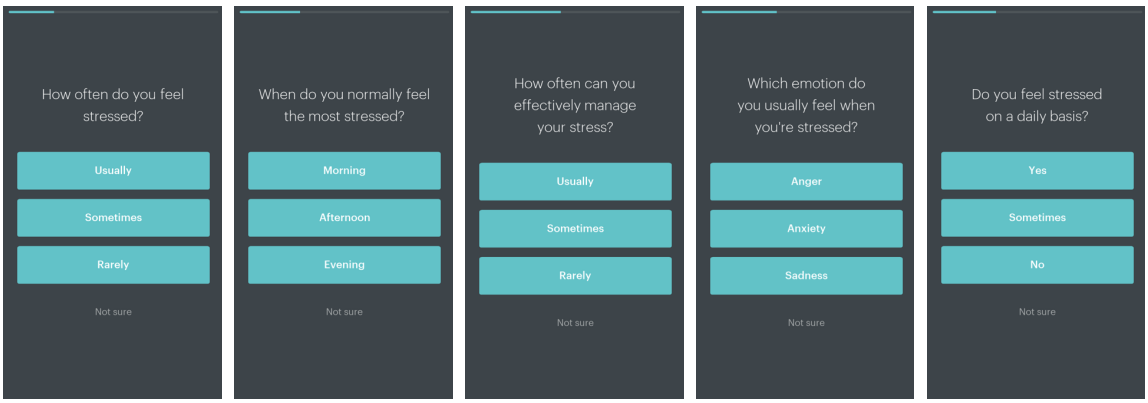


Figure 18. Meditation session process. User start from choosing a session, answering three-four questions then access to session

At first glance, the questions seem ordinary and harmless. By answering these questions, users believe it will result in a meditation plan adapted to help solve their problems. However, on a closer examination, the amount of collected information is significant. A user engaging with the Balance app every day would answer a minimum three questions per session, leading to a total of 1,095 questions in a year. Although the questions may appear benign, over time, the data gathered builds a detailed profile of each user, including sensitive information about lifestyles, habits, stress levels, emotional state or even daily struggles.



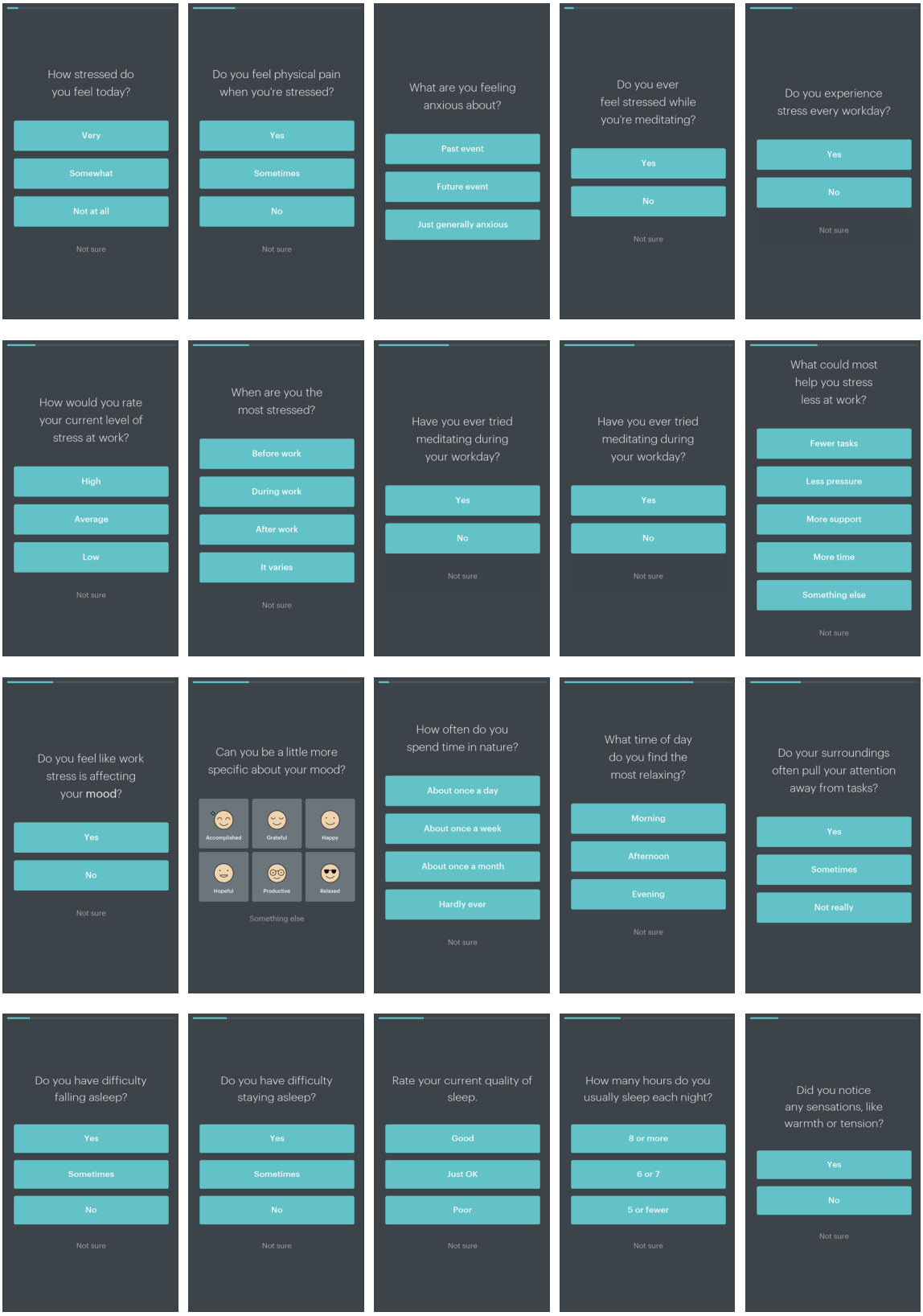


Figure 19. Sample question

7. Limitations, Discussion and Conclusion

The purpose of this thesis is to explore Dark Patterns in detail, including their definitions, classifications and effects on individuals, and how they are embedded in mindfulness applications. The work begins by searching and collecting relevant literature from the Scopus platform, followed by a detailed screening and inspection process. During the inspection, all the replicated and unrelated papers are being removed. The selected papers are related to main elements: dark pattern and manipulation in the mindfulness/digital health apps environment.

In order to understand how Dark Patterns function, it's essential to explore the factors influencing human behavior and how persuasive design techniques are applied. In this thesis, two major frameworks are discussed: Fogg's Behavior Model and Fogg's Seven Persuasive Technologies. Fogg's Behavior Model explains how Motivation, Ability and Trigger shape behavior. In order for a person to perform a specific behavior, the person needs to be motivated and have the ability to perform the behavior, and be triggered to perform the behavior. All three factors need to be present simultaneously for the behavior to occur (Fogg, 2009). Fogg's Seven Persuasive Technologies including Reduction, Tunneling, Customization/Tailoring, Suggestion, Self-monitoring, Surveillance and Conditioning, which outline the methods commonly used in digital design to manipulate user behavior (Fogg, 2003).

In terms of definition, Dark Patterns have various interpretations rather than one universal definition. From the initial definition coined by Bignull: "*a user interface that has been carefully crafted to trick users into doing things...they are not mistakes, they are carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind*", other scholars and user experience practitioners extend it further with specific and clear aspects. Marthur proposed that there is no single definition of Dark Patterns but rather common components that can be used to describe or categorize Dark Patterns. According to Marthur et al, Dark Patterns can be defined by four facets: characteristics of the user interface that can affect users, mechanism of effect for influencing users, the role of the user interface designer and benefits and harms resulting from a user interface design. The first facet focuses on characteristics of the user interface that can affect users like trick or misleading interfaces. The second facet of definitions is the mechanism

of effect for influencing users such as subverting user intent or preference, tricking users or undermining autonomy. The third facet is the role of the user interface designer. The fourth facet of dark pattern definitions is the benefits and harms resulting from a user interface design such as aiming to benefit an online service or involve harm to users (Marthur et al., 2021).

Regarding the classification of Dark Patterns, based on Bignull's initial 12 types, Gray came up with five primary categories of Dark Patterns that appeared to serve as strategic motivators for designers: Nagging, Obstruction, Sneaking, Interface Interference, and Forced Action (Gray et al., 2018). Nagging is redirection of expected functionality that persists beyond one or more interactions 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 (Gray et al., 2018). Nagging usually serves as an interruption to users' way of approaching a goal. Obstruction is making a process more difficult than it needs to be, with the intent of dissuading certain actions (Gray et al., 2018). Obstruction comes up with 3 subtypes: Roach Motel, Price Comparison Prevention, Intermediate Currency. Sneaking is attempting to hide, disguise, or delay the divulging of information that is relevant to the user (Gray et al., 2018). Subtypes are Forced Continuity, Hidden Cost, Sneak into Basket and Bait and Switch. Interface Interference is the manipulation of the user interface that privileges certain actions over others (Gray et al., 2018). Interface Interference's subtypes include Hidden Information, Preselection and Aesthetic Manipulation. Aesthetic Manipulation also comes up with four specific instantiations: Toying With Emotion, False Hierarchy, Disguised Ad, and Trick Questions. Forced action is requiring the user to perform a certain action to access (or continue to access) certain functionality (Gray et al., 2018). Forced Action has subtypes which are Social Pyramid, Privacy Zuckering and Gamification.

Several cautions have been raised about what Dark Patterns' potential negative impact on individuals, business and society at large. This thesis focuses on Individual Welfare. Marthur et al discussed that there are three kinds of individual welfare that are being diminished by Dark Patterns: Financial loss, Invasion or Privacy and Cognitive Burden. Financial Loss is the most straightforward consequence of Dark Patterns on individual consumers. Businesses often apply Dark Patterns on their interfaces pushing consumers to spend more than they mean to. Cognitive Welfare is when Dark Patterns on various interfaces cause users to spend unnecessary time, energy

and attention. Invasion of Privacy is when the Dark Pattern alters privacy of users. Invasion of Privacy is a serious concern and being mainly focused by many researchers and regulatories. In addition, between modalities, mobile apps are found to be the most affected from Dark Patterns. According to Gunawan et al., apps tend to have more unique dark patterns than their web counterparts, and apps tend to include different patterns than the corresponding websites. Findings also revealed that users are often unaware of the presence of Dark Patterns embedded in apps. Most of the time users could not perceive the presence of deceptive designs or not be sure about it.

To assess how Dark Patterns operate in mindfulness applications, this study employs a focused case study approach, providing an in-depth and detailed analysis of an chosen app. The chosen case study is the Balance app, a modern mindfulness application that claims to offer multiple personalized meditation sessions tailored to users' needs. As detailed in Section 6, all five main Dark Pattern strategies are presented in the Balance app. For the Nagging category, the app constantly pops up notification permission registration and requires users to answer information questions before each meditation session. In the Obstruction category, Balance app sets up complicated processes for users to delete accounts, unsubscriptions and delete users' data. When it comes to data control, Balance app intentionally complicates the process by making the data control information difficult to access, requesting users to send email and also have to verify their identity before proceeding. The challenges users face when exercising their rights over personal information strikingly contrast with the simplicity of Balance's account registration. Related to the Sneaking category, the app employs Force continue pattern, where users will be auto-charged once trials end.

The Balance app is an extreme example of using Hidden Information (Interface Aesthetic) and Private Zuckering (Forced Action). Balance app demonstrates serious concerns related to transparency and user consent as important information like terms of services, privacy policy and data control are being difficult to locate as analyzed in the Hidden Information section. In particular, there is no consent checkbox for users to agree to the terms during installing and subscribing process. Especially, Balance app uses 'personalization' to distract users through an appealing registration process to answer tailored questions. The process ultimately leads users to

a subscription without fully understanding that they've automatically agreed to the terms of service. This lack of disclosure is violating consumer rights. The promise of "Personalization" also misleads users into answering a large number of personal questions without full awareness. In the trial period or even after subscriptions, to start a meditation session, users have to answer retrieved questions. If a user used the app every day with one session each time, that user would answer at least three questions per session, leading to a total of 1,095 questions in a year. The questions appear to help users to develop a 'Personalization' program to solve their problems. Still, the amount of information that Balance app gathers is significant. Over time, the data gathered builds a detailed profile of each user, including sensitive information about lifestyles, habits, stress levels, emotional state or even daily struggles. The lack of transparency, combined with excessive data collection, exposes users to potential exploitation.

In conclusion, Dark Patterns present clear risks in the Balance app. The Dark Patterns in mindfulness applications keep users engaging to the app and not aware of financial loss and data extraction.This is particularly concerning as businesses exploit people's pursuit of wellness, to improve their mental and emotional health. Mindfulness applications' users are vulnerable targets since they're dealing with mental problems like stress, anxiety or insomnia. While users hope to solve their problems through mindfulness apps, the platforms use this need to promote purchases, increase engagement, and collect data. It's no doubt that these platforms gain great benefits from users' engagement.

When discussing limitations, this work is an observation-based evaluation of mindfulness applications integrating with knowledge of Persuasive designs and Dark Patterns literature. Therefore, this work does not include technical analysis of how Dark Patterns operate within the app, and how user data is collected and shared with the parent company and third parties. There may be further Dark Patterns present but not detected due to the app's intentionally deceptive user interface design. There is significant potential for future investigation and in-depth research into Dark Patterns in Mindfulness as well as other digital health applications.

8. References

Balance app. (n.d.). www.balanceapp.com. Accessed 2 Sep 2024.

Brignull, H. (2010). Dark patterns: User interfaces designed to trick people. UX Brighton 2010.

Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). Deceptive patterns – user interfaces designed to trick you. Deceptive.design. Retrieved April 25, 2023, from https://www.deceptive.design/

Business Wire. (2021, March 5). Global mindfulness meditation apps market outlook to 2027 - A USD 420.6 million market by 2027. Retrieved from https://www.businesswire.com/news/home/20210305005147/en

Colin, M. G., 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. Association for Computing Machinery, New York, USA, 1–14.

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). Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376600

Fogg, B. J. (2003). Persuasive technology: Using computers to change what we think and do. Morgan Kaufmann Publishers.

Fogg, B. J. (2009). A behavior model for persuasive design. www.bjfogg.com

Global Privacy Enforcement Network (GPEN). (2024). 2024 GPEN Sweep on deceptive design patterns. Retrieved from https://www.privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns

Gunawan, J., Pradeep, A., Chofnes, D., Hartzog, W., & Wilson, C. (2021). A comparative study of dark patterns across mobile and web modalities. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 377, 29 pages. https://doi.org/10.1145/3479521

Iwaya, L. H., Babar, M. A., Rashid, A., & Wijayarathna, C. (2023). On the privacy of mental health apps: An empirical investigation and its implications for app development. Empirical Software Engineering, 28(1), 2. https://doi.org/10.1007/s10664-022-10236-0

Khaled, R., James, N., & Biddle, R. (2005). An analysis of persuasive technology tool strategies. https://www.researchgate.net/publication/221253988_An_Analysis_of_Persuasive_Technology_Tool_Strategies. Accessed 16 Nov 2017.

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

Marijn, S. (2021). Optimization of what? For-profit health apps as manipulative digital environments. Ethics and Information Technology, 23(3), 345–361. https://doi.org/10.1007/s10676-020-09576-6

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proc. ACM Hum.-Comput. Interact., 3(CSCW), Article 81, 32 pages. https://doi.org/10.1145/3359183

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. In CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1–18). Association for Computing Machinery. https://doi.org/10.1145/3411764.3445610

Paterson, J. M., & Ananthapadmanaban, S. (2023). Data privacy and consumer protection practices of automated mental health, wellbeing, and mindfulness apps. Centre for AI and Digital Ethics, University of Melbourne.