IJIE (Indonesian Journal of Informatics Education)

Research Paper **ISSN: 2549-0389**

The Dark Side of Social Media: Analysing Dark Pattern Combinations and Their Impacts

[*1]Hansika Ukgoda
[1]Department of Information and Communication Technology, Faculty of Technological Studies,
Uwa Wellassa University of Sri Lanka, Sri Lanka
Corresponding Email: hansikauggoda@gmail.com

Abstract:

In today's digital era, technology is essential in daily life, transforming interactions and activities. However, the rise of "Dark Patterns - deceptive design practices in websites and apps raises significant ethical concerns. Originally defined by User Experience Designer Harry Bringull, dark patterns manipulate users into actions like involuntary purchases and subscriptions. This study explored dark patterns on social media networking sites (SNSs), focusing on two key questions: Do platforms use specific dark patterns in combination, and how do these combinations impact user interaction and experience? Utilizing cognitive walkthroughs with UI/UX experts, this research examined dark patterns on YouTube, LinkedIn, Telegram, and WhatsApp. Researchers conducted platform-specific evaluations to examine and understand the various combinations of manipulative design elements. The findings revealed prevalent combinations of dark patterns and evaluated their effect, addressing a critical gap concerning social media's ethical implications in the Human-Computer Interaction (HCI) field. The findings contribute to disclosing ethical design practices and promoting a more user-friendly approach to UI design that enhances user well-being and trust in digital environments.

Keywords: *dark pattern, ethical implications, interface designs, SNS, social media, user experience (UX)*

IJIE (Indonesian Journal of Informatics Education)
Vol 8 Issue 2 2024
DOI: http://dx.doi.org/10.20961/ijie.v8i2.91666
Received: 02/08/24 Revised: 26/12/24 Accepted: 28/12/24 Online: 31/12/24

Introduction

Modern digital innovations now play an essential role in how we conduct our lives. From communication to everyday activities, technology has profoundly transformed how people interact with the world. Amidst the technological revolution, a concerning trend has emerged the rise of "dark patterns". UX Designer Harry Bringull first coined the term dark patterns, describing them as "deceptive techniques that websites and applications employ to manipulate users into making unintended purchases or commitments." (Narayanan et al., 2020).

Contemporary academic research has extensively explored the phenomenon of dark patterns, uncovering various manifestations within Human-Computer Interaction (HCI). The growing body of research highlights the importance of understanding the attributes, distribution, and impact of dark patterns on user behaviour and mental state. These manipulative design techniques are consistently found across diverse online platforms, including social media, e-commerce websites, subscription services, and mobile applications. Ranging from subtle persuasion tactics that complicate subscription cancellations to more overt actions like automatic cart additions, dark patterns are prevalent in shaping user decisions. As digital interactions become more integrated into daily life, a comprehensive examination of the ethical considerations surrounding dark patterns is essential.

Mathur et al. (2022) laid the groundwork by developing an ontology that identifies and classifies 65 distinct dark patterns. Gunawan et al. (2022) further expanded this understanding by conducting comparative research on user interactions across mobile and web interfaces. Chaudhary et al. (2022) examined video streaming platforms, revealing how features such as autoplay and personalized content recommendations are strategically designed to maximize user engagement. Despite the extensive focus on HCI research, there remain significant gaps, particularly in understanding the influence of dark patterns on social media platforms and their effects on user behaviour. This study aims to address two key questions to bridge this gap:

Q1: Do platforms implement specific combinations of dark patterns strategically?

Q2: How do these combinations affect user engagement and experience?

To explore these questions, the research employs expert-led cognitive walkthroughs across four widely-used platforms: YouTube, LinkedIn, WhatsApp, and Telegram. UI/UX specialists perform targeted tasks to identify and analyse dark pattern combinations, enabling a deeper understanding of how multiple dark patterns interact to influence user behaviour. This study aims to accomplish two goals: examining common dark pattern combinations across platforms and evaluating how these patterns affect user behaviour and engagement. By examining the collective operation of these patterns, the study contributes to ongoing discussions about ethical design practices, ultimately promoting the development of more ethical and user-centered approaches to UI design.

Related Work

There has been growing interest in examining dark patterns within user interface design in recent years. Researchers examined diverse approaches, models, and classification systems to understand and combat deceptive interface patterns. This section integrates key scholarly findings, emphasizing core concepts, identification methods, defensive strategies, and contextual applications.

Gray et al. (2023) developed a comprehensive taxonomy to define dark pattern characteristics. This framework establishes a systematic classification of sixty-five dark patterns, delivering extensive taxonomic research. The researchers present evaluative frameworks for dark pattern analysis and recommend implementing evidence-based methodologies rooted in these frameworks. This comprehensive taxonomy aids research by providing a clear and detailed categorization of these deceptional practices. Mathur et al. (2021) also focus on problematic user interface designs and highlight the lack of consistent definition and conceptual foundation in dark patterns. They suggest applying empirical methods grounded in these perspectives. This research establishes conceptual frameworks and ethical principles for investigating manipulative interface designs.

Researchers actively explore the diverse manifestations of dark patterns as they emerge across platforms and environments. Delving deeper into the dark patterns, Understanding Account Deletion and Relevant Dark Patterns on social media (Scaffner et al., 2022) study investigates account deletion and user perception of social media. The paper analyses 490 account deletion interfaces across America's leading twenty social media platforms to uncover manipulative design techniques. They expose strategies like complex account removal procedures and partial data erasures. In their analysis of video streaming services, Chaudhary et al. (2022) investigated user manipulation techniques and dark pattern implementations. Researchers examined how UI elements such as Autoplay and Recommendations shape user interactions. They introduce a comprehensive classification of video streaming dark patterns and explore interface design principles that promote digital wellness. Research by Hidaka et al. (2023) highlights how cultural contexts influence dark pattern manifestations. Their investigation of Japanese mobile applications revealed a distinct category of dark patterns termed "Linguistic Dead Ends," which encompasses "Untranslation" and "Alphabet Soup." This research emphasizes the critical nature of design methodologies and investigative approaches, particularly when conducting cross-cultural studies on dark patterns. Gunawan et al. (2021) compared dark pattern implementations across multiple interaction modalities. Through a large-scale analysis of user interfaces and interaction platforms, they unveil variations in dark patterns between platforms. Researchers created a comprehensive codebook of dark patterns and identified fifty distinct types through service analysis. The research paper "About Engaging and Governing Strategies: A Thematic Analysis of Dark" extends dark pattern studies to social networking sites, examining Facebook, Instagram, TikTok, and Twitter. The research revealed five novel dark patterns by analysing engagement and governance approaches. They reveal SNS specific dark patterns and their impacts using thematic analysis (Mildner et al., 2023). Schafer et al. (2023) aim to provide a common reference for designers and policymakers by creating a typology that proposed eleven attention-capture damaging patterns (ACDPs).

To identify these ACDPs systematic literature was conducted. The authors also discuss the impact and opportunities for addressing attentional harm. Research by Blanchy et al. (2021) found that while consumers understand manipulative design tactics exist, they remain uncertain about the specific harm dark patterns cause them.

Gray et al. (2020) and Schafer et al. (2023) identified research gaps in investigating countermeasures against dark patterns so, they led their research into the detection and classification of dark patterns. However, they only evaluated six countermeasures for three dark patterns. To reduce these impacts the authors have proposed developing browser plugins for visual countermeasures. They conducted a workshop that aimed to connect research with the legal and regulatory communities. For engagement and collaboration in the workshops, they used Slack and Google Docs. Mildner et al. (2023) also proposed a methodology for assessing interfaces based on five dimensions of dark patterns. Furthermore, they addressed unethical design in CUIs through manipulations and cognitive biases and emphasized distinguishing between persuasive and manipulative e-design in HCI. Himawan et al (2017) highlights the negative impacts of social media, such as distractions during learning and potential exposure to harmful content, which can be exacerbated by dark patterns designed to prioritize user engagement over user well-being. They implied that understanding the that understanding the ethical implications of social media usage is crucial, as dark patterns can undermine the educational potential of these platforms, leading to a need for more ethical design practices in educational technologies. Similarly, Rosy (2018) suggested that dark patterns designed to maximize user engagement can distract students from their studies, ultimately lowering their achievement levels. Kelehar et al. (2022) also conducted an online survey to assess end users' perceptions of manipulative patterns. The survey participants evaluated the interfaces through semantic scales and identified manipulative patterns. Their findings indicated that the experts recognized more manipulative patterns but overestimated end users 'perceptions.

Focusing on privacy, Bosch et al. (2016) introduced privacy dark strategies and privacy dark patterns. They explored how actors manipulate personal data against user interest and provided a framework to analyse malicious concepts and develop countermeasures. Gunawan et al. (2022) investigated whether dark patterns can lead to the redress of individuals. This research examines how studies in the dataset evaluate adverse impacts and explores GDPR consent standards as a case study. This review categorizes prior work by Mathur et al., harms taxonomy, and discusses linking privacy dark patterns harms to user recourse. Gray et al. (2023) conducted a comprehensive analysis of seventy-nine literary works from 2014 to 2022 on dark patterns, highlighting crucial aspects of their context, presence, and influence. The Authors described common disciplinary perspectives and framing concepts by characterizing dominant methodologies used in studying dark patterns. They described common disciplinary perspectives, and methodologies and highlighted gaps and future opportunities for dark patterns research.

Research Method

This research aims to examine how platforms combine specific dark patterns and analyse how these combinations affect users' interactions and their overall experience. Therefore, considering four popular platforms (YouTube, LinkedIn, WhatsApp, Telegram) this study conducted a series of cognitive walkthroughs conducted by four UI/UX engineers with substantial expertise in HCI and UX research and design. Each expert reviewed potential dark pattern combinations by completing twelve comprehensive tasks that explored how users navigate through the mobile applications on each platform.

Sampling and Selection

This study selected four major social media platforms based on their global popularity and diverse user demographics: YouTube, Telegram, WhatsApp, and LinkedIn. These platforms were chosen to ensure a comprehensive analysis of different types of social media interactions. The focus was placed on user interaction features such as content creation and engagement and account creation and termination due to their relevance to known dark patterns. To mitigate selection bias, the chosen platforms represented a broad spectrum of social media experiences. However, it is acknowledged that platforms that are not included in this study, such as Facebook or Instagram, might exhibit different dark pattern combinations.

Pilot Testing

Before conducting the full analysis, a pilot test was performed on two platforms. The pilot test involved two evaluators performing cognitive walkthroughs and recording their observations. This phase helps to identify and refine the analysis procedures, ensuring that the criteria of evaluators are consistently applied. The pilot test revealed some inconsistencies in feature categorization (notifications, content recommendations, etc.), which were addressed by revising the feature definitions and improving the evaluators' guidelines. This process helped enhance the reliability of the findings and ensure a robust methodology.

Reviewers

To conduct this experiment, Four UI/UX engineers (3 male, 1 Female mean age = 25.4 years) with multiple years of experience varied from Two to Four years. Professionals from various companies in Sri Lanka, Australia, and the United States worked as reviewers during the execution of this research study. The recruitment process begins by compiling a list of potential reviewers from the professional network, focusing on individuals with a proven track record in HCI and UX research. Using preliminary screening the candidates were identified based on their contribution to industry conferences and professional experience in interface design and user experience. Participation in the study was voluntary, and all reviewers were assured of the confidentiality of their contribution

Preparation

Once consent was obtained, each reviewer received a Smartphone device (Android 11) preinstalled with the necessary applications: YouTube, WhatsApp, Telegram, and LinkedIn. The devices are factory reset to ensure uniform conditions throughout the process. The research team assigned each participant a unique email account and phone number to establish fresh user profiles on their designated platforms. This approach protected user privacy and eliminated any influence from previous customizations on the research results. The team also preloaded specific media content onto each device to help complete tasks.

Procedure

This study was conducted based on the dark pattern taxonomy derived from Marthur et al.'s work which encompasses sixty-nine distinct types of dark patterns. The research incorporated three dark patterns from the study "Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps": Linguistic Dead-Ends, Untranslation, and Alphabet Soup (Table 1). Each reviewer participated in an introductory session on the topic followed by 1 hour dedicated to addressing any questions, ensuring uniform understanding. After the session, reviewers received informational material that contained the definitions of each dark pattern that they should observe (This information material can be found in supplementary materials). After the introductory session, the group discussed questions to ensure uniform understanding. The evaluators completed twelve tasks during their cognitive walkthroughs. Di Geronimo et al.'s research paper (2020) on popular Google Play Store platforms contributed to five of these assessment tasks. These tasks are designed to cover a broad range of user interactions, providing a comprehensive view of potential dark patterns in each platform. Inspired by his methodology, each platform was investigated for one hour and each session was recorded to get a deep observation of the platforms. The recordings were automatically saved on each device and accessed upon the reviewer's return to the smartphones. Five example of dark patterns categories can be seen in Table 1, while the complete data can be seen in the Appendix section.

Table 1. Categorization of dark patterns

Deceptive Information	**Obstruction & Restriction**	**Sneaky & Hidden Practices**	**Manipulation & Exploitation**	**Obfuscation**	**….**
Trick Questions (Brignull 2010)	Obstruction (Gray et al. 2018-2019)	Sneak Into Basket (Brignull 2010)	Attention Grabber (Conti & Sobiesk 2010)	Distraction (Conti & Sobiesk 2010)	….
Privacy Zuckering (Brignull 2010)	Restricting Functionality (Zagal et al. 2013)	Hidden Subscriptions (Gray et al. 2018-2019)	Exploiting Interruption (Zagal et al. 2013)	Errors (Zagal et al. 2013)	….
Misdirection (Zagal et al. 2013)	Manipulating Navigation (Zagal et al. 2013)	Hidden Legalese Stipulations (Bösch et al. 2016)	Entrapping (Hidaka et al. 2023)	The Milk Factor (Zagal et al. 2013)	….
Misrepresenting (Hidaka et al. 2023)	Immortal Accounts (Bösch et al. 2016)	Disguised Data Collection (Zagal et al. 2013)	Alphabet Soup (Hidaka et al. 2023)	Visual Interference (Gray et al. 2018-2019)	….
Social Pyramid Schemes (Zagal et al. 2013)	Hidden Costs (Zagal et al. 2013)	Disguised Ads (Zagal et al. 2013)	Grinding (Conti & Sobiesk 2010)	Confusion (Zagal et al. 2013)	….
Testimonials of Uncertain Origins (Gray et al. 2018-2019)	Low-stock Messages (Gray et al. 2018-2019)	Shadow User Profiles (Bösch et al. 2016)	Playing by Appointment (Zagal et al. 2013)	Linguistic Deadends (Hidaka et al. 2023)	….

Each task was selected for its relevance to identifying dark pattern combinations as mentioned. The following were performed,

1. Enable screen recording on the device.
2. Launch each platform, register your credentials, sign in, and complete your session. (Examines onboarding processes and potential manipulative combinations during setup)

3. Close and reopen each application. (observes persistence of state)
4. Create, post, and delete content. (Observe manipulative combinations in content creation and deletion processes)
5. Follow and unfollow other accounts or join and leave groups. (Investigates interaction manipulations)
6. Like and dislike posts or content. (Investigates engagement manipulation through feedback mechanism)
7. Subscribe and unsubscribe to channels or accounts. (Examines the pressure applied to retain or acquire subscriptions)
8. Navigate to personal settings. (Observes ease of access and potential manipulations in settings)
9. Navigate to the ad-related settings. (Examine privacy and advertisement preference)
10. Dedicate a minimum of five minutes to explore each application's core functionality: (Ensure comprehensive observation by mimicking regular user behaviour)
    a. Describe the natural flow of the application.
    b. Identify any features that 'guided' interactions.
    c. Note any distractions encountered and their sources.
11. Delete the account. (Checks for dark pattern combinations that hinder account termination)
12. Deactivate the screen recording and save the recording. (Ensure complete data capture for analysis)

During each task, reviewers are requested to look for any instance of dark pattern combinations. Observations are documents immediately after each task, with reviewers noting the combination they observed, the context, and the potential impact on the user. After completing all the tasks, reviewers discuss their observations to ensure consistency and completeness.

Result and Discussion

This section presents findings from cognitive walkthroughs on YouTube, LinkedIn, WhatsApp, and Telegram, focusing on identifying and analysing combined dark patterns. Screen recordings and audio notes were transcribed using Otter.ai for detailed analysis. Each platform exhibits distinct yet interrelated dark pattern combinations designed to influence users. The researchers analysed one-hour recordings to obtain data for addressing both research questions. The screen recordings captured the visual elements of manipulative design combinations, while the audio provided complementary material, offering a detailed expression of the user's experience in real-time.

Answering the first research question, the following section presents the identified combinations on each platform separately (Table 2).

Table 2. Identified Dark Patterns Combinations in Platforms

Platform	Combinations	Abbreviations
YouTube	Misdirection + Roach Model	Misdirection + RM
	Disguised Ads + Trick Questions	DA + TQ
	Nagging + Controlling	Nagging + Controlling
	Manipulating Navigation + Confusion	MN + Confusion
	Limited-time Messages + High Demand Messages	LM + HM
	Forced Action + Manipulating Navigation	FA + MN
	Confusion + Countdown Timers	Confusion + CT
WhatsApp	Hidden Legalese Stipulations + Privacy Zuckering	HLS + PZ
	Forced Action + Restricting Functionality	FA + RF
Telegram	Disguised Ads + Manipulating Navigation	DA + MN
	Misdirection + Controlling	Misdirection + Controlling
LinkedIn	Roach Motel + Confusion	RM + Confusion
	Pressured Selling + Controlling	PS + Controlling
	Obfuscation + Nagging	Obfuscation + Nagging
	We Never Forget + Sneaking	WNF + Sneaking
	Forced Action + Social Brokering	FA + SB
	Disguised ads + Entrapping	DA + Entrapping

Before delving into the detailed dark pattern combinations observed on each platform, it is essential to highlight the frequency of these combinations, as illustrated in Figure 1. This figure provides insights into how often these combinations appeared across the platforms during the one-hour observation period. On YouTube, the combinations of Disguised Ads + Trick questions were the most appeared combination, appearing four times. This was followed by several other combinations such as Misdirection + Roach Model, Limited-time Messages + High Demand Messages, and Manipulating Navigation + Confusion, each appearing three times. On LinkedIn, instances of dark pattern combinations such as Pressured Selling + Controlling and Obfuscation + Nagging are observed three times each. Other combinations like Roach Model + Confusion and We Never Forget + Sneaking were less frequent but still noticeable. WhatsApp is Known for its reliability and user trust, exhibited fewer combinations, also the instance appearance is also less than compared to LinkedIn and YouTube. These findings suggest that while WhatsApp generally maintains a good user experience, it still employs certain dark pattern combinations to influence user behaviour. Telegram also showed a lower frequency of manipulative design than other platforms. The instance frequencies of these combinations highlight the varying degrees to which each platform employs dark patterns. These insights provide the stage for a deeper exploration of how these combinations manifest in each platform.

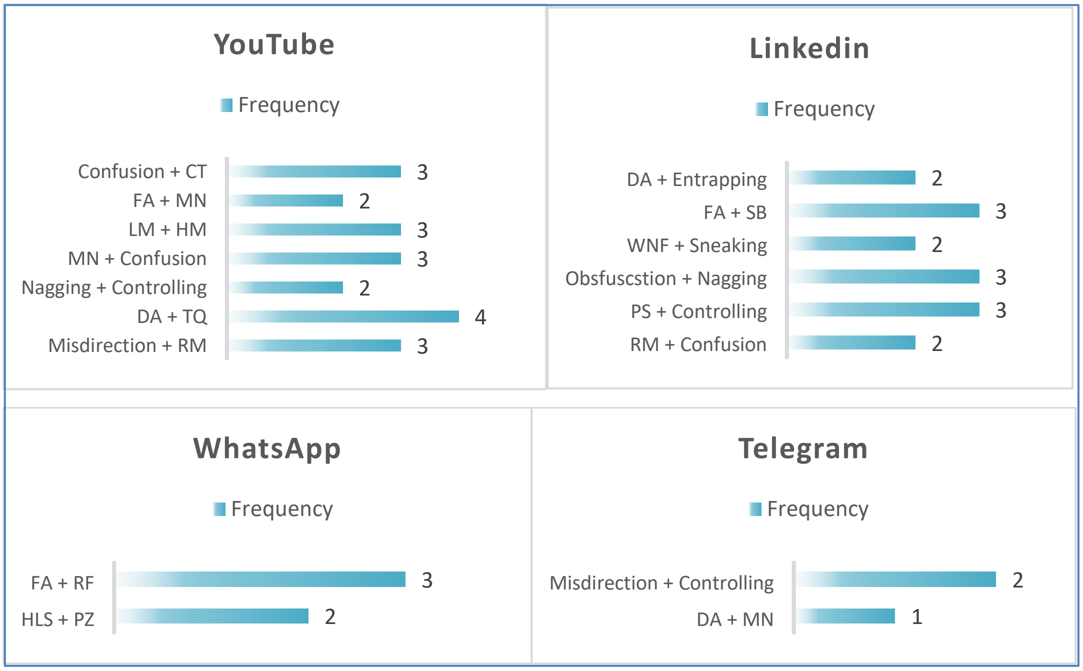
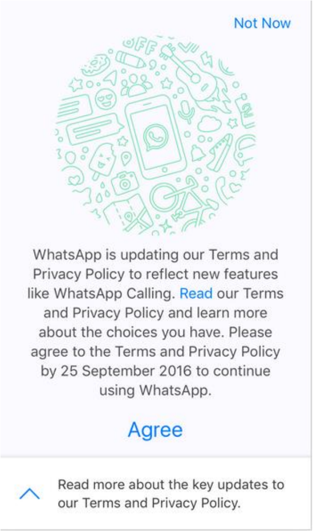


Figure 1. Frequency of Dark Pattern Combinations Observed Across Different Platforms

WhatsApp

WhatsApp stands as a highly dependable platform that has established strong credibility with its users through continuous enhancements in functionality and accessibility features throughout recent years. The application remains free and will maintain its cost-free status while delivering superior user experience. However, several combinations were found through the analysis. Forced Action + restricting Functionality is one of the combinations identified in WhatsApp. WhatsApp prompts users to accept new terms (Forced Action) forcing them to restrict the platform's functionality (Restricting Functionality).

Another combination found is the combination of Obfuscation and Interface interferences. The app effectively hides options, making it a very proactive choice for users to opt out of relinquishing information and ultimately not being transparent concerning some critical privacy options. Consider WhatsApp's policy updates, where users face a single choice: clicking "Agree and Continue," without any option to decline the terms (see Figure 2). WhatsApp also buries important privacy-related information within lengthy terms of service or privacy policies, prompting users to accept it while subtly adjusting privacy settings (Hidden Legalese Stipulations + Privacy Zuckering). This leads to more information being made public than users might realize. People depend extensively on these applications, making them susceptible to deceptive marketing strategies.



WhatsApp is updating our Terms and Privacy Policy to reflect new features like WhatsApp Calling. Read our Terms and Privacy Policy and learn more about the choices you have. Please agree to the Terms and Privacy Policy by 25 September 2016 to continue using WhatsApp.

Read more about the key updates to our Terms and Privacy Policy.

Figure 2. WhatsApp's policy update prompt

YouTube

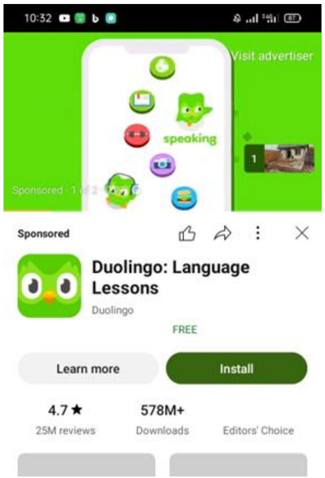


Figure 3. YouTube advertisement with two countdown timers

Although YouTube offers numerous free resources and a platform for connecting with friends, it often requires users to hand over personal information. YouTube heavily relies on ad revenue and employs subtle dark pattern combinations of Confusion and Countdown Timers. The pattern in question involves using various ad implementations. The skip button can consist of a countdown or some other call to action, or it can simply be a countdown without any call to action associated with it. Another thing that YouTube does is add multiple counters to their ads (see Figure 3). One counter will count down the duration of the ad then the other will count down the seconds until the user skips the ad.

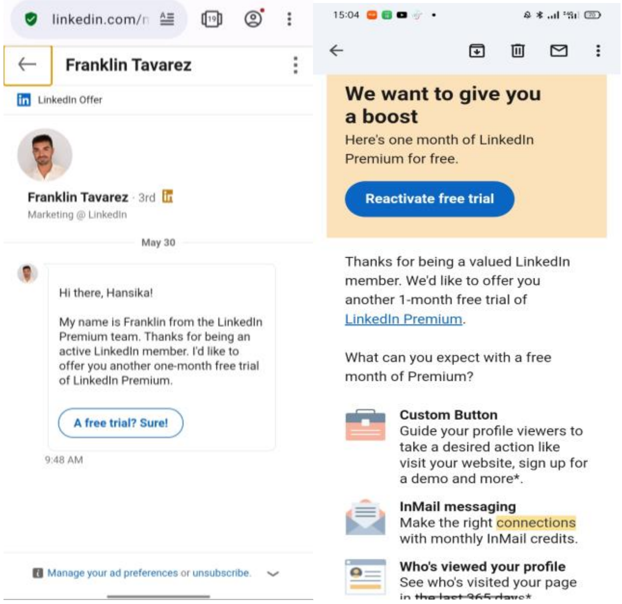
This is a somewhat underhanded technique whose sole purpose is to confuse viewers, and while it is not exactly illegal, it will frustrate YouTube subscribers. After close attention to the countdown on the skip ad button, noticed that the duration of each number is variable and doesn't correlate to seconds. Some are longer than a second. This means that what the user thinks is 5 seconds is slightly longer. This increases the actual time an ad is displayed relative to a user's perception of the time elapsed. (Confusion + Manipulated Navigation)

Also, YouTube's recommendation algorithm (misdirection) perpetuates video consumption and keeps users engaged (Roach Model). Autoplay features and personalized recommendations entice users to consume more media, extending their platform engagement time. These recommendations seem to be suggestions based on watch history rather than the current video, perpetuating continuous viewing. Autoplay (forced action) ensures continuous viewing by automatically playing the next video. The platform's intricate navigation (manipulating navigation) discourages users from leaving, making it challenging to exit. Furthermore, advertisements presented by YouTube are sometimes disguised as legitimate content or questions/ surveys aimed at tricking users into engaging with them. (Disguised Ads + Trick Questions)Another identified combination is Limited-time Messages + High Demand Messages. As a video streaming platform, YouTube occasionally displays limited-time messages like "Watch now before it's gone!" alongside high-demand messages (e.g., "Trending video!"). This generates immediate action by compelling users to engage promptly. Furthermore, YouTube continuously prompts users to upgrade to premium services for enhanced experiences, including ad-free viewing (Nagging + Controlling).

LinkedIn

Dark patterns might initially resemble design errors, but designers create these elements intentionally by leveraging deep insights into human psychology. Experts widely consider these dark patterns as unethical design techniques that significantly damage user experience and destroy users' confidence in products, websites, or brands.

LinkedIn is the main platform for professional networking that allows people to connect collaborate and network within their industries. Although it allows users to build strong networks that are crucial to career advancement, LinkedIn employs several hidden dark pattern combinations to exploit its users. LinkedIn makes it easy to sign up for their platform and subscribe to the premium features, however, once they're in, it becomes a challenge to delete or unsubscribe their accounts. For instance, when users try to cancel their premium subscription, LinkedIn switches the primary and secondary buttons. So, at a glance, the user may be confused that they are performing the opposite action. (Confusion + Roach Model). LinkedIn also bombarded users with notifications and direct messages, pressuring users to purchase premium memberships and promoting extra features (see Figure 4). This creates a coercive environment through pressured selling and feature limitations (Pressured selling + Controlling).



Hi there, Hansika!

My name is Franklin from the LinkedIn Premium team. Thanks for being an active LinkedIn member. I'd like to offer you another one-month free trial of LinkedIn Premium.

We want to give you a boost

Here's one month of LinkedIn Premium for free.

Thanks for being a valued LinkedIn member. We'd like to offer you another 1-month free trial of LinkedIn Premium.

What can you expect with a free month of Premium?

Custom Button
Guide your profile viewers to take a desired action like visit your website, sign up for a demo and more*.

InMail messaging
Make the right connections with monthly InMail credits.

Who's viewed your profile
See who's visited your page in the last 365 days*

Figure 4. LinkedIn notifications and direct messages urging users to purchase premium memberships

Another Combination LinkedIn employs is a combination of Obfuscation + Nagging. LinkedIn conceals multiple configuration options, which prevents users from effectively managing their privacy settings and controlling their profile's visibility to others. Moreover, the platform nags' users with persistent notifications to complete their profiles to improve their experiences. When observing it was discovered that user privacy has been greatly affected by the platform. LinkedIn stores user data indefinitely, retaining information such as profile details, connections, and browsing history without explicit consent, employing sneaky tactics like background data collection (we never forget + Sneaking).

Further analysis revealed disguised ads, and entrapping strategies were also hidden inside the platform, which tricked users into certain actions. Advertisements on LinkedIn are disguised as regular content within the user's feed, making it challenging to differentiate between normal content. Platforms also spam users with emails about job opportunities and profile views to sustain engagement. LinkedIn engages in social brokering by leveraging users' data to facilitate connections and endorsements without transparent consent and coerces users into making new connections.

Telegram

The final Social Media platform analysed in this paper is Telegram. Telegram is the perfect tool to host online communities and coordinate teamwork. Telegram uses dark patterns similar to other platforms. Users cannot block these ads, which are often placed within the app as regular content. Users struggle to differentiate between promotional content and authentic communication in this context. Ads can be strategically placed within the platform’s navigation, leading users to unintentionally click them while trying to navigate through their chats or channels. As a result, the Distinguished ads + Manipulating Navigation dark pattern is manifested. Apart from being a social media platform, Telegram also serves as a marketing tool. Although Telegram is free to use there is an optional subscription service that unlocks additional exclusive features. These extra features include an integrated audio-to-text message converter, no ads in public channels telegram, and many others. The platform encourages users to subscribe to these premium features to gain these extra benefits, potentially manipulating the experience of users by misdirecting and controlling them. (Misdirecting + Controlling dark pattern combination)

Impact on User Interaction and Experience

Dark patterns significantly affect how users interact with and experience digital interfaces. These deceptive designs leverage psychological biases to influence users into making unfavourable choices, including impulsive purchases or unwarranted sharing of private data. Having explored the various facets of the first research question, which delved into the dark pattern combinations, the focus now shifts to the second research question: How do these combinations impact user interaction and overall experience? This question attempts to understand the broader implications of how dark patterns impact user experience and behaviour. Companies implement these deceptive design techniques to maximize their commercial advantages. Dark patterns are not merely nefarious by design: they come with tangible consequences. The manipulation of user’s data happens all over the internet. This research identifies various combinations that manipulate users into performing specific actions that contradict their genuine intentions or preferences. Dark patterns employ deceptive language, complex interfaces, and hidden options to manipulate users into taking actions that benefit the platform rather than themselves. Social media platforms, for instance, often implement convoluted privacy agreements and terms of service that obscure transparency, leading to user manipulation and diminishing trust in these platforms. The strategic combination of dark patterns profoundly impacts user autonomy, raising significant ethical concerns. These patterns exploit cognitive biases and limit users' ability to make informed decisions, effectively stripping them of their freedom of choice. This is especially troubling when users face crucial decisions regarding personal data management, where deceptive practices can lead to serious consequences. Repeated exposure to dark patterns causes user frustration and damages platform credibility. LinkedIn provides a prime example through persistent notifications that urge users to expand their network and improve their profiles, creating user annoyance. The platform also uses tactics like obscuring cancellation options for premium subscriptions (e.g., LinkedIn Subscription) or complicating service opt-outs, fostering feelings of helplessness and dissatisfaction. When users are repeatedly deceived by these patterns, their engagement with the platform decreases in future interactions. This deteriorates the relationship between companies and customers, damaging trust that extends beyond immediate consequences. The resulting distrust may erode the legitimacy of the digital economy and undermine broader societal confidence in technology.

YouTube's misleading pop-ups and advertisements obstruct user activities and may trigger accidental purchases, leading to financial strain, buyer's remorse, frustration, anger, or regret. While dark pattern combinations affect all users, certain vulnerable groups such as those with lower digital literacy, younger users, or individuals from disadvantaged socioeconomic backgrounds are more susceptible to manipulation. Social media dark pattern combinations also infringe on privacy, as platforms exploit user data through unauthorized collection or sharing. Companies design pre-selected options and default privacy configurations to encourage unintentional disclosure of confidential data.

These manipulative interface designs actively obstruct users from exercising informed decision-making, potentially triggering negative consequences including overspending, compromised data security, or automatic subscription renewals. This unclear approach creates a power differential, keeping users ignorant about their actions' complete ramifications. Although these dark pattern combinations may provide short-term benefits for social networking services (SNS) platforms, the long-term consequences are negative. Users who experience manipulation or deception demonstrate reduced loyalty to the platform, hesitate to recommend services to their networks, and exhibit less positive engagement. These effects directly impact user retention and hinder platform growth.

The analysis of dark pattern combinations reveals significant implications for user interactions and overall experiences on social media platforms. Understanding these ethical concerns can guide stakeholders toward creating more transparent, user-respecting digital environments that foster authentic engagement and trust.

Future Work

The findings from this study reveal essential pathways to enhance digital ethics scholarship and advance user interface design principles. This research has identified several constraints that researchers must address in future studies. Notably, the investigation concentrated solely on mobile platform applications. This narrow focus might overlook important differences in dark pattern implementations across various interfaces like web browsers or desktop software. Different modalities exhibit distinct interface designs, which shape how users interact and perceive manipulative elements. Researchers must expand their investigations across diverse platform modalities to develop a comprehensive understanding of dark patterns in digital interfaces. External dynamics, including shifting user expectations and technological innovations, can impact study outcomes.

Consequently, researchers need to evaluate these contextual elements when analysing the results. These insights and recognized constraints lead to multiple promising directions for future investigations.

1. Exploring Multimodal Interfaces: Comparative across multiple modalities could highlight how interface modality influences the prevalence and impact of manipulative design tactics on user experience and behaviour.
2. Longitudinal Studies: Researchers must implement long-term tracking studies to examine how dark patterns evolve across SNSs and digital platforms. These investigations will illuminate emerging trends in manipulative design strategies, user coping mechanisms, and policy responses.
3. Cultural and Contextual Analysis: Cross-cultural comparative research will reveal how different societal norms, and regulatory frameworks shape the implementation and impact of dark patterns across digital interfaces.
4. Advanced Analytical Techniques: Researchers should utilize sophisticated methods including machine learning algorithms, natural language processing, and structural equation modelling. These approaches will generate comprehensive insights into dark pattern effectiveness mechanisms.

The integration of these research directions will enable scholars to expand dark pattern knowledge significantly. This scientific progress will promote ethical design principles and strengthen user confidence and psychological wellness in digital spaces.

Conclusion

The study acknowledges that its findings may be influenced by external factors such as evolving user expectations and technological advancements. It offers a comprehensive analysis of dark pattern combinations present in the mobile applications of selected social networking sites (SNSs). Through a cognitive walkthrough conducted with six Human-Computer Interaction (HCI) experts, the study identifies and categorizes prevalent dark patterns based on established taxonomies in the field. The results highlight how these patterns manipulate user behaviour and influence decision-making processes, raising significant ethical concerns related to user autonomy, privacy, and transparency in digital interactions. Design professionals can leverage these insights to eliminate dark patterns, maintain ethical principles, and build credibility in digital interface development through collaborative efforts.

References

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). ”i am definitely manipulated, even when i am aware of it. It’s ridiculous! ”—Dark patterns from the end-user perspective. *Designing Interactive Systems Conference 2021*, 763–776. https://doi.org/10.1145/3461778.3462086

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*. https://petsymposium.org/popets/2016/popets-2016-0038.php

Chaudhary, A., Saroha, J., Monteiro, K., Forbes, A. G., & Parnami, A. (2022). “Are you still watching? ”: Exploring unintended user behaviors and dark patterns on video streaming platforms. *Designing Interactive Systems Conference*, 776–791. https://doi.org/10.1145/3532106.3533562

Conti, G., & Sobiesk, E. (2010). Malicious interface design: Exploiting the user. *Proceedings of the 19th International Conference on World Wide Web*, 271–280. https://doi.org/10.1145/1772690.1772719

Deceptive Patterns (Aka dark patterns)—Spreading awareness since 2010. (n.d.). Retrieved 26 December 2024, from https://www.deceptive.design/

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. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3313831.3376600

Gray, C. M., Chivukula, S. S., & Lee, A. (2020). What kind of work do ‘asshole designers’ create? Describing properties of ethical concern on reddit. *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 61–73. https://doi.org/10.1145/3357236.3395486

Gray, C. M., Gunawan, J. T., Schäfer, R., Bielova, N., Sanchez Chamorro, L., Seaborn, K., Mildner, T., & Sandhaus, H. (2024). Mobilizing research and regulatory action on dark patterns and deceptive design practices. *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3613905.3636310

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (Patterns) side of ux design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3173574.3174108

Gray, C. M., Sanchez Chamorro, L., Obi, I., & Duane, J.-N. (2023). Mapping the landscape of dark patterns scholarship: A systematic literature review. *Designing Interactive Systems Conference*, 188–193. https://doi.org/10.1145/3563703.3596635

Greenberg, S., Boring, S., Vermeulen, J., & Dostal, J. (2014). Dark patterns in proxemic interactions: A critical perspective. *Proceedings of the 2014 Conference on Designing Interactive Systems*, 523–532. https://doi.org/10.1145/2598510.2598541

Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., & Wilson, C. (2021). A comparative study of dark patterns across web and mobile modalities. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–29. https://doi.org/10.1145/3479521

Gunawan, J., Santos, C., & Kamara, I. (2022). Redress for dark patterns privacy harms? A case study on consent interactions. *Proceedings of the 2022 Symposium on Computer Science and Law*, 181–194. https://doi.org/10.1145/3511265.3550448

Hidaka, S., Kobuki, S., Watanabe, M., & Seaborn, K. (2023). Linguistic dead-ends and alphabet soup: Finding dark patterns in japanese apps. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3544548.3580942

Himawan, A. A., Basori, B., & Adi Sucipto, T. L. (2017). Social media influence and intensity of watching television drama on achievement of students. *IJIE (Indonesian Journal of Informatics Education)*, 1(2), 95. https://doi.org/10.20961/ijie.v1i2.11334

Keleher, M., Westin, F., Nagabandi, P., & Chiasson, S. (2022). How well do experts understand end-users’ perceptions of manipulative patterns? *Nordic Human-Computer Interaction Conference*, 1–21. https://doi.org/10.1145/3546155.3546656

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

Mildner, T., Doyle, P., Savino, G.-L., & Malaka, R. (2022). Rules of engagement: Levelling up to combat unethical cui design. *Proceedings of the 4th Conference on Conversational User Interfaces*, 1–5. https://doi.org/10.1145/3543829.3544528

Mildner, T., Freye, M., Savino, G.-L., Doyle, P. R., Cowan, B. R., & Malaka, R. (2023). Defending against the dark arts: Recognising dark patterns in social media. *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, 2362–2374. https://doi.org/10.1145/3563657.3595964

Monge Roffarello, A., Lukoff, K., & De Russis, L. (2023). Defining and identifying attention capture deceptive designs in digital interfaces. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–19. https://doi.org/10.1145/3544548.3580729

Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: Past, present, and future: the evolution of tricky user interfaces, 18(2), 67–92. https://doi.org/10.1145/3400899.3400901

Rosy, B. (2018). Schoology, changing a negative thinking pattern about use of social media. *IJIE (Indonesian Journal of Informatics Education)*, 2(1), 1. https://doi.org/10.20961/ijie.v2i1.21612

Schäfer, R., Preuschoff, P. M., & Borchers, J. (2023). Investigating visual countermeasures against dark patterns in user interfaces. *Mensch Und Computer 2023*, 161–172. https://doi.org/10.1145/3603555.3603563

Schaffner, B., Lingareddy, N. A., & Chetty, M. (2022). Understanding account deletion and relevant dark patterns on social media. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), 1–43. https://doi.org/10.1145/3555142

Zagal, J., Björk, S., & Lewis, C. (2013). Dark patterns in the design of games. *International Conference on Foundations of Digital Games*. https://www.semanticscholar.org/paper/Dark-patterns-in-the-design-of-games-Zagal-Bj%C3%B6rk/19a241378b06d868eb5f6b76027172c3aaca86f4

Appendix: Categorization of Dark Patterns

Deceptive Information	Obstruction & Restriction	Sneaky & Hidden Practices	Manipulation & Exploitation	Obfuscation	Coercion & Pressure	Misuse of Social Dynamics	Unfair Financial Practices	Aggressive Marketing	Control and Automation	Data Exploitation	Interface Design Exploits	Emotional Manipulation	Complex Social Relationships	Translation Barriers
Trick Questions (Brignull 2010)	Obstruction (Gray et al. 2018-2019)	Sneak Into Basket (Brignull 2010)	Attention Grabber (Conti & Sobiesk 2010)	Distraction (Conti & Sobiesk 2010)	Coercion (Conti & Sobiesk 2010)	Friend Spam (Zagal et al. 2013)	Nickling-And-Diming (Hidaka et al. 2023)	Pay to Skip (Zagal et al. 2013)	Automating the User (Hidaka et al. 2023)	Information Milking (Bösch et al. 2016)	Interface Interference (Gray et al. 2018-2019)	Confirmshaming (Zagal et al. 2013)	The Social Network of Proxemic Contracts or Unintended Relationships (Greenberg et al. 2014)	Untranslation (Hidaka et al. 2023)
Privacy Zuckering (Brignull 2010)	Restricting Functionality (Zagal et al. 2013)	Hidden Subscriptions (Gray et al. 2018-2019)	Exploiting Interruption (Zagal et al. 2013)	Errors (Zagal et al. 2013)	Forced Work (Zagal et al. 2013)	Address Book Leeching (Bösch et al. 2016)	Monetized Rivalries (Zagal et al. 2013)	Pay to Skip (Zagal et al. 2013)	Controlling (Hidaka et al. 2023)		Address Book Leeching (Bösch et al. 2016)	Nagging (Gray et al. 2018-2019)		
Misdirection (Zagal et al. 2013)	Manipulating Navigation (Zagal et al. 2013)	Hidden Legalese Stipulations (Bösch et al. 2016)	Entrapping (Hidaka et al. 2023)	The Milk Factor (Zagal et al. 2013)	Forced Registration (Bösch et al. 2016)	Making Personal Information Public (Zagal et al. 2013)	Price Comparison Prevention (Zagal et al. 2013, Bösch et al. 2016)	Pre-Delivered Content (Zagal et al. 2013)	Two-Faced (Hidaka et al. 2023)		Making Personal Information Public (Zagal et al. 2013)	Price Comparison Prevention (Zagal et al. 2013, Bösch et al. 2016)		
Misrepresenting (Hidaka et al. 2023)	Immortal Accounts (Bösch et al. 2016)	Disguised Data Collection (Zagal et al. 2013)	Alphabet Soup (Hidaka et al. 2023)	Visual Interference (Gray et al. 2018-2019)	Forced Action (Gray et al. 2018-2019)		Bait and Switch (Brignull 2010, Zagal et al. 2013)	Shock (Zagal et al. 2013)				Bait and Switch (Brignull 2010, Zagal et al. 2013)		
Social Pyramid Schemes (Zagal et al. 2013)	Hidden Costs (Zagal et al. 2013)	Disguised Ads (Zagal et al. 2013)	Grinding (Conti & Sobiesk 2010)	Confusion (Zagal et al. 2013)	Forced Continuity (Zagal et al. 2013)					Data Exploitation	Interface Design Exploits	Emotional Manipulation	Complex Social Relationships	Translation Barriers
Testimonials of Uncertain Origins (Gray et al. 2018-2019)	Low-stock Messages (Gray et al. 2018-2019)	Shadow User Profiles (Bösch et al. 2016)	Playing by Appointment (Zagal et al. 2013)	Linguistic Deadends (Hidaka et al. 2023)	Pressured Selling (Gray et al. 2018-2019)					Information Milking (Bösch et al. 2016)	Interface Interference (Gray et al. 2018-2019)	Confirmshaming (Zagal et al. 2013)	The Social Network of Proxemic Contracts or Unintended Relationships (Greenberg et al. 2014)	Untranslation (Hidaka et al. 2023)