Differences in Misleading Data Collection and Financial Dishonesty in Social Media Creating Dark Patterning

DOMINIC STREEB, Colorado State University, USA

Additional Key Words and Phrases: Dark Patterning, Financial Dishonesty, Data Collection

ACM Reference Format:

Dominic Streeb. 2024. Differences in Misleading Data Collection and Financial Dishonesty in Social Media Creating Dark Patterning. 1, 1 (May 2024), 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Almost every individual around the United States uses social media platforms on a daily basis for news, profile updates, and even online shopping. With the platforms growing popularity, companies are finding different ways to collect more information about users, increasing paid services with hidden fees, and misleading free trials[4]. A new interest in unethical design strategies, known as dark patterns, helps users understand how and why companies are creating misdirection when many are drawn into the adverse effects[6]. Dark patterning is the inherited problem of many social media platforms and websites aimed at collecting data of consumers unknowingly, dishonest financial transactions, and malicious user agreements. Dark patterns are deceptive elements planted into web applications tricking users into giving up personal information, money, and valuable data[7]. Many outlets are used to derive information from their users such as persistent ads, deceiving cookie banners, misleading user agreements, and a multitude of user agreements aimed to have users auto agree to information unknowingly. Not only are malicious methods used to collect data unknowingly, but some web services are collecting more revenue by adding hidden fees or other expenses to online shopping transactions, often going unnoticed by the consumer[5].

Two commonly utilized dark patterns are misleading data collection and financial dishonesty. Unfortunately, many of these practices are low priorities of law enforcement which leaves the consumers responsible for there online safety concerning these marketing and financial schemes[1]. For example, a commonly used concocted financial scheme is whats called a "Bait and Switch" which refers to a company advertising for a bargained price of a good when it may not be on sale or may be aimed at bringing customers to the location. Another example of dark patterning in media when concerning financial dishonesty is when a company implements hidden fees or misleading convenience fees to gather more revenue without providing more to the customer[8]. With the decrease in time spent on online transactions, payments and shopping totals are not scrutinized to a high degree creating a more complaisant interaction between consumers and online shops often advertised through social media. While financial dishonesty is becoming a popular method for companies to gain more financially, misleading data collection can be observed in almost every social media platform from lengthy user agreements to ambiguous cookie banners. Specifically focusing on the unethical design of

Author's address: Dominic Streeb, dstreeb@colostate.edu, Colorado State University, Fort Collins, Colorado, USA, 80524.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2024 Association for Computing Machinery.
Manuscript submitted to ACM

the data collection tools, they are created to instate the user to read less and agree more[6]. The two most common dark patterns are misleading data collection and financial dishonesty. The study aims to determine if there are significant differences in individuals likelihood to detect these financial dishonest transactions or misleading data collections. The end goal of the experiment is to observe how susceptible individuals ages 19-29 are to dark patterning in social media, if people in the age group are perceptive to dark patterning and the difference between misdirection in data collection and financial dishonesty.

2 RELATED WORKS

Many institutions use the term dark patterns to define instances where designers use their knowledge of human behavior and the desires of the end users to implement deceptive attributes not in the users best interest[3]. Web applications and social media platforms are decreasing users involvement in the data they provide and take away the ability to have honesty user agreements. This has quickly led to users becoming fatigued with privacy notifications and contributed to the rise of both browser extensions that block these banners and demands for a solution to come from the designers[9].

2.1 User Interaction with Web Influences

Observing the relative ability for HCI (Human Computer Interaction) users to determine the presence of dark patterning in media has been an effective method for visualizing how users are effected by dark patterning. Gathered a group of individuals familiar with dark patterning and getting these participants familiarized them with methods to recognizing its presence relieved that the users were unable to detect most or all dark patterns presented to them[2]. These studies were often constructed by giving a list of tasks to complete in a timed manor as to create an environment where the individuals were not actively searching for misleading data but using the application as intended[7]. Participants were given surveys after running the experiments on the mobile device to gauge the user functionality and if they perceived any of the dark patterning scenarios described to them before the experiment. Even though the participants were made aware of the 82 possible malicious patterns in the software only 22 were found and discussed[7]. Most account setups and social media interaction demonstrated Hidden-Legalese Stipulations, Misdirection, Interface Interference, Visual Interference, Privacy Zuckering, and Address Book Leeching[6]. Other studies focused on specific design elements that may be malicious or deceiving in nature to determine the effects of users aptitude to be persuaded or manipulated. For example, Uber utilised a A/B patterning strategy that makes the user interface more attractive to persuade drivers to continue driving rather than ending there work[1]. Often this involves the utilization of dark patterning on websites and social media creating the illusion that one option is better than another. Something as simple as button color or style can easily persuade in individual who may not be fully informed of the action they are making.

2.2 Misleading Data Collection

With the multitude of possibilities of dark patterning in social media, many studies have focused on the overall effects of dark patterns and how companies are effecting users interaction, while other specifically look at falsifying records and information. Several papers discussed the underlying correlation of users and how likely they are to believe information given to them on a media platform. This can include falsifying news stories and financial transactions the user may make online[10]. It can often be difficult and time consuming to verify content a user is consuming in social media, and sometimes is impossible to certify every button and link does not have malicious intent. Inspired by recent work, some web interfaces are moving forward with generating user reports on the likelihood of individuals willingly giving more personal information than necessary, but this is not widely utilized as many companies use user information for profit. Companies are moving towards more confusing agreements and fewer options to opt out of data collection[9]. Not only are users agreeing to give more data to companies, but some organizations are focused specifically on how much information a user is willing to give up in order to receive better perks like coupons or other incentives in the web application. They found that over 50 percent of users would give emails, phone numbers, and credit card information[10]. With the growing use of dark patterning in online platforms, more research and information needs to be implemented so users are aware of there online impact.

3 METHODOLOGY

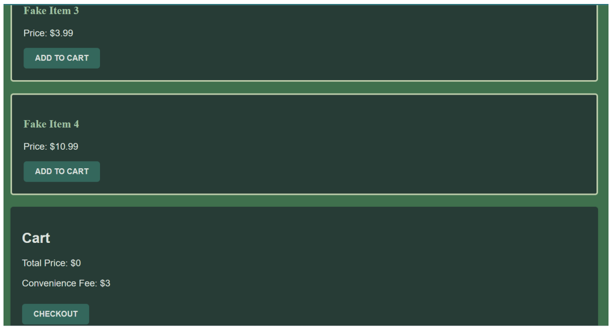
To further the exploration into the awareness of users on dark patterning, an experiment was designed to determine the differences between misleading data collection and financial dishonest dark patterning in a social media platform.

3.1 Participants

The experiment was conducted on 12 participants who volunteered for the study. Each participant was between the ages of 19 and 29 to resemble the population who uses social media the most frequent. No prior instruction was given to the participants. Before conducting the experiment, each volunteer completed a consent waiver. The 12 participants were divided randomly into three groups, control, misleading data collection, or financial dishonesty. The participants were not informed which group they will participate in. Once the groups were separated, each participant individually conducted the experiment.

3.2 Procedures

Each participant was given a laptop with the predetermined social media scenarios to complete. They were given 4 tasks to complete on the platform and each instruction was identical for each participant. Group 1 participants, the control group, has no instances of dark patterning on there media website. Group 2 participants had a social media scenarios that included instances of misleading data collection such as asking for social security numbers to verify there identity and asking for personal information for coupons and discount. Group 3 participants had social media scenarios that had instances of financial dishonesty such as over charging for items in the store and adding more fees to online subscriptions.



Fake Item 3

Price: $3.99

Fake Item 4

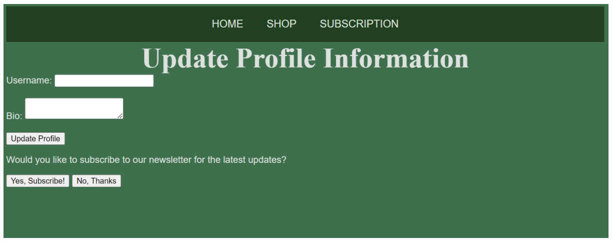
Price: $10.99

Cart

Total Price: $0

Convenience Fee: $3

Fig. 1. Fake Shop on Social Media Application



Update Profile Information

Would you like to subscribe to our newsletter for the latest updates?

Fig. 2. Updating Profile with Newsletter Subscription

Participants were not informed prior to completing the scenarios about what a dark pattern was or what they were interacting with. The task list for each participant was intentionally vague to promote a natural user experience that still has users interact with valuable information. The task list can be seen below:

(1) Go to the newsletter tab and update your user profile.
(2) Go to the shop and purchase at least two items. (No payment will be collected)
(3) View the subscriptions page.
(4) Explore the website and interact with anything you find interesting.

The members of each group performed the listed tasks only on the groups specified web application.

3.3 End Survey

After each participant completed all 4 tasks they were given a survey that consisted of 13 Likert scale questions that asked about there experience using the application. Each question was evaluated as 1 (Strongly Disagree), 2 (Disagree), 3 (Neutral), 4 (Agree), 5 (Strongly Agree). The user survey questions are listed below:

(1) I found the website easy to navigate.
(2) I felt that the website provided clear and transparent information about its use of my data.
(3) I believe the website had hidden fees or costs that were not initially apparent.
(4) I felt misled by the information presented on the website.
(5) I was comfortable with the amount of personal information I was asked to provide.
(6) I felt that the financial transactions on the website were straightforward and honest.
(7) The website used confusing language or terminology that made it hard to understand the terms and conditions.
(8) I noticed that the website used design elements that seemed intended to guide my choices.
(9) I felt that the website respected my privacy choices.
(10) I felt pressured to make purchases or sign up for services I did not initially want.
(11) The website clearly stated the costs associated with its services or products.
(12) I was able to easily find information regarding how to opt out of data collection or subscriptions.
(13) I trust this website to handle my financial information securely.

4 RESULTS

In examining the impacts of dark patterning on social media users, the study utilized a Likert scale survey to evaluate participants perceptions across three groups: a control group, a data collection group, and a financial dishonesty group.

The survey was designed to measure user experience and awareness of unethical design strategies employed on social media platforms. Once all participants had taken the survey, the average for each response was graphed below:

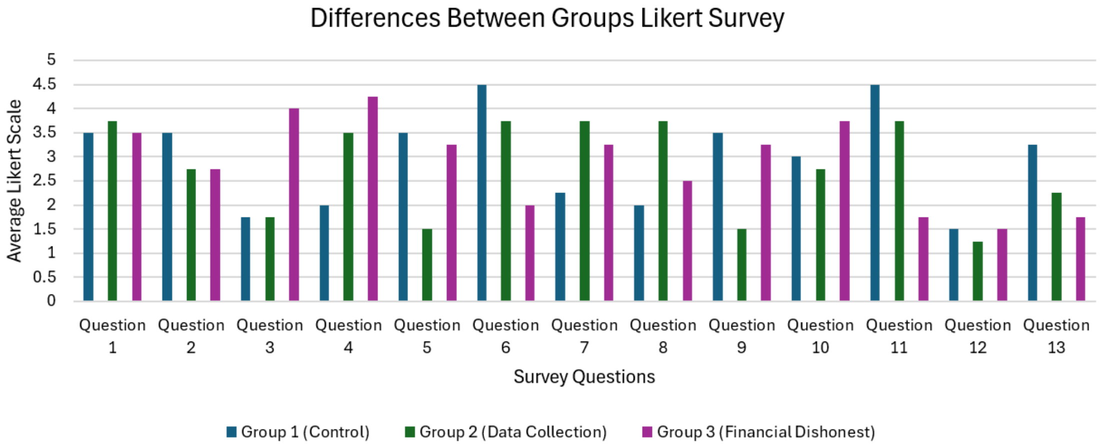


Fig. 3. Differences in Likert Scale Survey Questions Between Groups

Each group's response to the survey was recorded and analyzed. The average scores across various questions highlighted how each group perceived their interaction with the platform. A one way ANOVA test was performed within the three groups to determine the significance of the data. The ANOVA summary is displayed below:

Table 1. ANOVA Summary

Groups	*Count*	*Sum*	*Average*	*Variance*
Control	52	155	2.980769	1.470211
Data Collection	52	144	2.769231	1.435897
Financial Dishonesty	52	150	2.884615	1.39819

The variance and average of all three groups were very similar and indicate that groups were consistent in answering the survey. This may suggest that most participants in each group had similar perceptions and reactions to the scenarios they were exposed to. The one way ANOVA data analysis was completed for the three groups and the results can be seen below:

Table 2. One Way ANOVA Test

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.166667	2	0.583333	0.40657	0.666648	3.055162
Within Groups	219.5192	153	1.434766			
Total	220.6859	155				

The analysis yielded a p-value of 0.666648, significantly above the conventional 0.05. This indicates that there are no statistically significant differences between the responses of the three groups, suggesting that the presence of dark patterns did not distinctly influence the participants perceptions in this study. The high p-value indicates that the dark patterns introduced in the data collection and financial dishonesty groups did not significantly affect the perceptions compared to the control group. The F-value of 0.40657 is relatively low, suggesting that the variance attributed to group differences due to dark patterns is small. The sum of squares between groups (1.166667) being much smaller than the sum of squares within groups (219.5192) indicates that there is greater variability in responses within each group than between the different groups. This might indicate that individual differences or other uncontrolled variables had a more substantial impact on the survey responses rather than exposure to dark patterns.

5 DISCUSSIONS

The lack of variation and difference between the different groups may indicates the dark patterns were not received by the participants. Dark patterning is often hidden within the web interface and intended to be overlooked by the user [5]. Another explanation for the close variance could be the very small sample size of only four participants per group. With a larger sample size, the data would be more reliable.

6 CONCLUSION

This study looked into the impact of dark patterns on social media platforms, focusing on misleading data collection and financial dishonesty. Despite the use of such dark patterns by companies to manipulate there user behavior for profit, my findings revealed that these dark patterns did not significantly influence the perceptions of the participants consisting of individuals aged 19 to 29. The results, expressed by a high p-value and low F-value in the one way ANOVA test, suggest there was no statistically significant difference in the perception of dark patterns among the control, data collection, and financial dishonesty groups. These findings need a reassessment through continued testing and education. The participants were not sufficiently aware of the manipulative intent behind the scenarios presented which elicits the need for further education and awareness to ensure social media users are fully informed about the decisions they are making[1]. This outcome highlights a potential disregard for such manipulative tactics, suggesting that many users may not consciously recognize these patterns, even when they are directly affected by them. While this research did not find significant effects of dark patterns on user perception within the experimental setup, it further supports the need for further studies. Future research should aim to use more pronounced dark patterns and include a broader demographic and larger sample size. Such efforts are essential to develop strategies and regulations to counteract these unethical practices, ensuring a fairer and more transparent digital environment for all users.

7 ACKNOWLEDGMENTS

Thank you to everyone that participated in the user study.

REFERENCES

[1] Narayanan Arvind, Mathur Arunesh, Chetty Marshini, and Kshirsagar Mihir. Dark patterns-past, present, and future: The evolution of tricky user interfaces. *ACMQueue*, 18(2):1–25, 2020.

[2] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 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*, pages 1–14, 2020.

[3] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–14, 2018.

[4] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. A comparative study of dark patterns across web and mobile modalities. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–29, 2021.

[5] Maximilian Maier. Dark patterns–an end user perspective, 2019.

[6] Thomas Mildner, Merle Freye, Gian-Luca Savino, Philip R Doyle, Benjamin R Cowan, and Rainer Malaka. Defending against the dark arts: recognising dark patterns in social media. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, pages 2362–2374, 2023.

[7] Thomas Mildner, Gian-Luca Savino, Philip R Doyle, Benjamin R Cowan, and Rainer Malaka. About engaging and governing strategies: A thematic analysis of dark patterns in social networking services. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2023.

[8] R Sreya and PT Raveendran. Dimensions of perceived risk in online shopping-a factor analysis approach. *BVIMSR's Journal of Management Research*, 8(1):13, 2016.

[9] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un) informed consent: Studying gdpr consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security*, pages 973–990, 2019.

[10] Svitlana Volkova and Jin Yea Jang. Misleading or falsification: Inferring deceptive strategies and types in online news and social media. In *Companion Proceedings of the The Web Conference 2018*, pages 575–583, 2018.

Received 30 March 2024; revised 5 May 2024