Ethics and Manipulation in Digital Interfaces

A Research Paper Presented to

The Department of Engineering and Society
Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree Bachelor
of Science, School of Engineering and Applied Science

Ky Nguyen
Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisors
William Stafford, Department of Engineering and Society

Introduction

Distinguishing persuasion from manipulation in digital systems extends beyond traditional models of consent and trust. No longer can software UX/UI , user experience and user interface, designers expect a straightforward agreement statement to be a definitive contract between user and software. Designers are generally aware of explicit guidelines for data privacy, such as the EU General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). However, the moral and social responsibilities of developers in UX design are still unclear, with developers often relying on legal or corporate authorities to set persuasive versus manipulative design boundaries for them. Often developers are advised to "ignore" potentially unethical solutions by rejecting or accepting client requests because their professional reputation is at risk. Consequently, the intentions of different stakeholders can influence the reasoning for design choices whether persuasive or manipulative, with less emphasis on upholding user integrity. Even user expectations can be contradictory, as seen with the privacy paradox.

Discussion of Case

In a study conducted by Chamorro et al, developers primarily agreed that trust, transparency, and user autonomy are three major tells of a system's ability to manipulate (Sánchez et al., 2023). Using Nelissen, L. G. M., & Funk, M. classification for dark patterns common in UI design, we discuss how traditional consent-based models can be circumvented by dark patterns (Nelissen et al., 2022). By definition, dark patterns in software UI design refer to deceptive or misleading strategies employed to influence user decisions, often leading them to act against their own interests. A well-known principle is that design prioritizes familiarity over innovation. On one hand, a familiar design leads users to feel more at ease and confident using tools they recognize, but too innovative and the user may feel lost or confused. This can lead to increased susceptibility to dark patterns due to dealing with the unknown (Nelissen et al., 2022). On the other hand, designers can condition users into expecting certain user action journeys when in reality, slight nudges in the design can prime the user for unintentional consent.

This research differentiates itself by looking into the nuanced impacts of dark patterns in UI/UX design, particularly focusing on how these designs psychologically manipulate user behavior. While existing literature predominantly outlines what dark patterns are and how companies deploy them to maximize financial gains, this paper examines the deeper usage in which these patterns coerce users into unintended actions, which often to the benefit of the company. This exploration is crucial as it reveals the extent to which digital systems can exploit user vulnerabilities, thus highlighting a significant gap in current research that often overlooks the user's diminished autonomy in the rapidly evolving digital world. Below, there are several examples of manipulative UI/UX design techniques large companies often use and their respective case studies.

For example, a system can automate user choice by pre-checking an agreement checkbox, also known as interface interference (Bjørlo et al., 2024). Although the user is technically giving their consent, certain actions are privileged over others. This takes advantage of users' negligence to enforce consent with a familiar system, since they have encountered checkbox popups before but did not expect it to be pre-checked (Luguri et al., 2021). Friction and stickiness in interfaces, demonstrated respectively by interrupting a user action or repeating a call to action through pop-ups, sidebars, top bars and similar techniques can also be employed to encourage consent by reinforcing the call to action everywhere on the platform until the user consents.

Another example lies in website “cookies” , which serve as the anchor in a complex system of user tracking and information gathering (Arntz et al., 2022). At their core, cookies are small pieces of data stored on the user's device by websites to remember the user's actions and preferences over time. While designed to enhance the user experience by personalizing content and making navigation more seamless, cookies also play a pivotal role in the collection of personal data for advertising and tracking purposes. The ethical concerns around cookies stem from their ability to collect vast amounts of personal information without the explicit, informed consent of the user (Arntz et al., 2022). This is exacerbated by UI/UX designs that obscure the true extent of tracking or make it difficult for users to opt out of cookies. Furthermore, most websites today enforce a policy where users cannot access features without accepting their terms of service related to cookie usage. Cookies can contain very sensitive information about users such as users' browsing habits, websites visited, time spent on pages, clicked links, purchase history, video, and audio data. These cookies are vulnerable to cyber attacks and potentially leaked for uses in targeted advertising and potentially cyber crimes. Such UI/UX designs are ethically questionable and appear to manipulate users into giving away more information than they intend to.

Privacy Zuckering is a common dark pattern that falls under the forced action classification where the user cannot opt out of a data privacy processing step in order to use a service (Nelissen et al., 2022). Unintentionally sharing more information than you consented to appears to be a direct violation of user transparency, which developers agree to consciously avoid while designing. The problem is that users state they want data privacy while expecting the convenience provided by modern platforms, which sacrifices privacy for customizability in user preferences. This privacy paradox obfuscates the balance between privacy expectations and user experience. The user may enjoy data privacy within a digital system at the risk of potential dissatisfaction due to the limited features of the system without the requisite user data.

A subcategory under interface interference is named as aesthetic manipulation. A design will leverage tangible or intangible incentives to persuade a user to act (Nelissen et al., 2022). An example of a tangible incentive is offering a 20% discount promotion if a user gives their email to subscribe to a newsletter. Examples of intangible incentives could be feelings, trust, and connection. Certain concepts in the realm of social engineering such as the "fear of missing out" can be utilized here to convince the user to agree to a service, such as a badge indicating the user is of an exclusive membership and thus, providing the user with the incentive of a community where they belong. Zooming into the topic of feelings, designers tend to gravitate towards reinforcing positive feelings rather than negative to promote a better user experience. Thus emotional design often considers user needs, expectations, and experience in order to influence users. In this way, some designers interpret autonomy as more of a "negative liberty: as freedom from external barriers, instead of a positive one, freedom to act".

Case Study

Case 1: Dark patterns design in Google and Facebook caused a fine in $240 million for making cookies hard to refuse [Rikke, Arntz]

In 2022, France's Commission Nationale de l'Informatique et des Libertés (CNIL) imposed fines amounting to €210 million on Google and Facebook for employing manipulative User Interface (UI)/User Experience (UX) designs in their cookie consent mechanisms. This case exemplifies the ethical concerns associated with "dark patterns" in digital design strategies that subtly guide users towards making decisions that may not be in their best interest, yet serve the business models of technology companies by facilitating user consent through deceptive means.

Cookies are small data files used by websites to track user behavior and preferences. While essential for personalizing user experiences, they have become central to practices that infringe on user privacy through extensive tracking without clear, informed consent (Arntz et al., 2022). With that in mind, Google and Facebook take advantage of their website's design to force users to accept cookies in order to use their site. Typically, the website should still allow the user to use their website without the need to accept cookies, but that is not the case for Facebook and Google because they need every single data point from its user as much as possible. As a result, users of Facebook and Google have filed complaints against these two companies for actively collecting data without their informed consent and using it for advertising as well as other corporate gains. Because of this, the CNIL issued a €210 million fine to these companies as a penalty for their "dark pattern" UI/UX design to take advantage of user's privacy data (Arntz et al., 2022). The fines issued by CNIL highlight not just the manipulation embedded in the consent process of the digital system - whereby accepting cookies is straightforward, often requiring a single click, while rejecting them involves navigating through long complex steps.

This case study on privacy complaints against Facebook and Google further exposes the vulnerable point of the digital consent mechanisms, highlighting how these platforms maximize data collection under the guise of consent. This is achieved through UI/UX designs that obscure the implications of consent, burying critical privacy choices under layers of complex navigation and information. Large companies often use these "dark pattern" strategies because it is a "legal" way to manipulate its user to follow the companies interests. As a result, this generates more financial gains to those companies with the cost of their customers, often unknowingly so. From an ethical standpoint, the core issue centers on the balance between user privacy rights and the business models of online platforms, which rely heavily on data exploitation. The ethical implications of such UI/UX design practices raise concerning questions about the responsibility of tech companies to ensure transparency, user autonomy, and informed consent. Ethical design principles advocate for clear choices and transparent information regarding data use, allowing users to make informed decisions about their privacy. However, the CNIL's actions against Google and Facebook, coupled with the detailed exploration of privacy complaints against these companies, reveal a gap between these ethical concerns and current practices.

Case 2: FTC Takes Action Against Amazon's Interface Interference Behavior for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel [FTC, Bjørlo]

The Federal Trade Commission (FTC) filed a complaint against Amazon for deceptive practices in enrolling consumers into its Amazon Prime subscription without clear consent (FTC et al., 2023). The complaint alleges that Amazon employed "dark patterns" in its user interface design to manipulate consumers into unknowingly signing up for Prime. This involved making the process to decline or cancel the subscription overly complex and misleading, essentially trapping consumers in a subscription model they did not actively choose (Bjørlo et al., 2024). During the cancellation process, amazon will actively try to provide promotion and fake deals that users would gain from remaining an active Prime member. This shows how Amazon, and other tech giants, can and will exploit consumers' cognitive biases to trap users in their ecosystem. Such practices not only frustrated users but also led to financial troubles for those unable to navigate the cancellation process effectively.

This case raises ethical concerns regarding the respect for consumer informed consent in digital transactions. The calculated design choices by Amazon to obscure the subscription and cancellation process shows a broader issue in the tech industry: the exploitation of user interfaces to prioritize corporate profit over user rights and transparency. These big companies always implement tactics that psychologically manipulate its users to keep giving them their data and money. They have to keep doing this to satisfy their shareholders, and other stakeholders that are at play. Even though these companies always advertise themselves as "for the people" and remain "ethically right" is the goal. But ethical principles in design call for clear communication, respect for user decisions, and transparency, and companies like Amazon's actions show otherwise. The FTC's action against Amazon indicates the need for regulatory oversight to protect consumers from manipulative digital practices that seems to be an increasing trend.

Case 3: FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook due to "Privacy Zuckering" allegations [FTC, Staff]

The case between the Federal Trade Commission (FTC) and Facebook in 2019 is relevant to the concept of privacy zuckering, a term coined to describe deceptive tactics used by companies to manipulate users into sharing more personal information than they intend. Privacy zuckering encompasses practices that exploit users' actions, often resulting in the unauthorized collection and selling of their personal data (Nelissen et al., 2022). Regarding the case, the investigation was initiated following the Cambridge Analytica scandal, which exposed how Facebook allowed third-party developers to access users' personal data without their explicit consent, ultimately breaching trust between the platform and its users. This shows how Facebook, and other large tech companies, are prioritizing profit over data privacy.

With over 185 million daily users in the United States and Canada alone, Facebook holds immense amounts of personal data, which, if mishandled, can have consequences for individuals' privacy and security (Staff et al., 2023). The impact of the case extends beyond Facebook itself to its vast user base and the broader tech industry. Millions of users experienced a loss of control over their personal information, as their data was shared with third parties without their consent. This breach of privacy not only violated users' trust in Facebook but also left them vulnerable to identity theft and fraud. The leaking of personal data to third parties enabled targeted advertising and manipulation, undermining users' free choice online. Moreover, the psychological impact of knowing that their personal information had been compromised caused feelings of anxiety, stress, and distrust among affected users. From an ethical standpoint, the case raises questions about the responsibilities of tech companies towards their users. Facebook's actions, as outlined in the FTC investigation, demonstrate a disregard for user consent and a prioritization of corporate interests over user privacy. By misleading users about their privacy controls and allowing third-party developers access to personal data without clear consent, Facebook violated fundamental ethical principles of transparency, autonomy, and respect for user rights.

Commonalities between the case studies

The case studies of Google and Facebook's cookie consent mechanisms, Amazon's enrollment tactics for Amazon Prime, and Facebook's privacy violations share several commonalities that highlights the pervasive nature of manipulative user interface design and its implications for data privacy.

Firstly, each case involves a manipulation of user consent, where complex UI designs or dark patterns obscure the true implications of user actions, leading users to inadvertently provide consent for data collection or service enrollment. In Google and Facebook's case, pre-checked checkboxes and convoluted consent processes make it difficult for users to opt-out of data tracking, while Amazon's tactics involve making cancellation processes deliberately challenging to navigate. Facebook's privacy zuckering tactics similarly exploit users' actions to gather more personal data than intended, highlighting a consistent theme of deceptive UI/UX practices across the digital landscape. Secondly, these cases show the tension between business interests and user rights. In all instances, the companies prioritize their financial gains over transparency and user autonomy. Whether it's maximizing data collection for targeted advertising or ensuring continued subscription revenues, the design choices reflect a disregard for ethical principles in favor of corporate profit. Moreover, these case studies highlight the inadequacies of existing regulatory frameworks in addressing manipulative UI/UX designs effectively. Despite regulations like GDPR and CCPA aiming to protect user privacy, companies find ways to circumvent these rules through intricate UI designs that exploit user vulnerabilities. This raises questions about the enforcement mechanisms and the need for more robust regulatory oversight to curb such practices effectively.

By analyzing these commonalities, we can identify a pattern of behavior among tech companies that prioritize short-term gains over long-term user trust and societal well-being.

Addressing these issues requires a group effort from stakeholders, including regulatory bodies, companies, designers, and users, to establish clear ethical guidelines and ensure accountability in the digital system space.

Ethics behind UI/UX Design through Actor Network Theory

Following the exploration of case studies that demonstrate manipulative UI/UX designs, it becomes an important issue to discuss the ethics behind these practices. Ethical design principles, rooted in user consent, autonomy, transparency, and respect for privacy, serve as the cornerstone of user interaction on the internet (Kelly et al., 2023). The rising of dark patterns as strategic elements in UI/UX design starkly contrasts with these principles, placing business objectives above user rights. The case studies of Google, Facebook, and Amazon reveal a concerning trend where user experiences are engineered to prioritize corporate gains over ethical considerations. Using Actor Network Theory, we can further analyze the association between manipulative UI/UX design and its ethical concerns on data privacy.

The exploration of manipulative UI/UX design through an ethical lens, particularly in the context of the Actor-Network Theory (ANT), provides an understanding of the relationship between technology, users, and societal norms (Cresswell et al., 2010) . ANT claims that social phenomena emerge from the interactions between both human and non-human actors , such as technologies, objects, and ideas, offering a framework to analyze how manipulative UI/UX designs influence and are influenced by the broader network in which they operate. From an ethical standpoint, manipulative UI/UX design practices raise significant concerns about the erosion of user autonomy and informed consent. This manipulation not only undermines the ethical principle of respect for user autonomy but also challenges the integrity of the digital systems. The ethical dilemma here lies in the balance between optimizing user engagement and safeguarding user rights (Nelissen et al., 2022). Relating these ethical concerns to ANT, manipulative UI/UX designs can be seen as non-human actors that exert influence within the actor-network. They engage in a dialogue with other actors—users, regulatory bodies, competing platforms, and societal norms—shaping and being shaped by the network's dynamics. Through ANT's lens, the design of an interface is not a technical decision but a complex negotiation that reflects the power dynamics, interests, and values of various actors in the network. For instance, the introduction of a manipulative design element, such as a pre-checked consent box, becomes an actant that shifts the network's balance, potentially aligning with business interests while conflicting with regulatory norms and user expectations (Luguri et al., 2021). The ethical implications of manipulative UI/UX designs, viewed through the ANT framework, extend to the responsibility of designers and developers. As key actors within the network, they possess significant influence over the configuration of other actors and the network's overall ethical landscape. The decision to use manipulative designs implicates them in the broader consequences of these practices, including impacts on user trust, privacy violations. Using the ANT model, these various actors can be described as stakeholders and each of them play a key role in the decision making process of creating a manipulative UI/UX design.

Stakeholder Influences on UI/UX Design

The ecosystem surrounding UI/UX design is a complex network where various stakeholders, each with different incentives. This network, influenced by Actor Network Theory (ANT), offers insights into how and why manipulative design elements are influenced and implemented. Below are the five key stakeholders that present in all manipulative UI/UX design systems.

Designers and Developers

At the frontline of digital product creation, designers and developers are the main factor in shaping user experience. They are the ones who ultimately plan and develop the UI/UX design to match their customer’s needs. While many strive for ethical design, the pressure to meet business goals—such as increasing user engagement and sales—can lead to the adoption of manipulative design practices. This situation places designers and developers at a crossroads, where they must navigate the balance between fulfilling user expectations and meeting investor demands. Leaning too far towards prioritizing user needs may compromise the financial performance of the product, potentially straining investor relationships. Conversely, overly concentrating on investor interests risks the relationship with their users, which in turn decreases in the system’s user engagement metrics.

Users

As the end-users of digital products, individuals are directly impacted by the design choices made by developers and designers. It falls upon these creators to safeguard users' privacy, especially considering that access to digital services often requires users to share personal information. It is ethically questionable if the users entrusted data get manipulated for the company’s financial gain. In this dynamic, users are central in supporting the financial success of digital platforms. As a result, their personal data should be handled with care and respect.

Regulatory Bodies

Regulatory agencies play a crucial role in establishing the legal framework within which UI/UX designs are developed. By setting standards for privacy and consent, such as the GDPR or CCPA, they provide guidelines that aim to curb the exploitative potential of dark patterns. However, the effectiveness of these regulations is contingent upon their enforcement and the adaptability of the laws to keep pace with technological innovations.

Corporate Executives and Shareholders

The strategic objectives of corporations and their shareholders often emphasize profit maximization, which can incentivize the use of dark patterns to boost financial outcomes. This focus on the bottom line may overshadow ethical considerations, prompting a design ethos where user manipulation becomes a secondary concern to economic gain.

The Impact of Stakeholders on UI/UX Design Ethics

Through the lens of ANT, the interactions between these stakeholders illustrate the dynamic and negotiable nature of UI/UX design ethics. The theory suggests that the design process—and the emergence of dark patterns within it—is the result of ongoing negotiations among all actors involved. For instance, regulatory pressures might lead to redesigns that aim to align with legal standards, while user backlash against invasive practices can force companies to reconsider their design strategies. Ultimately, the ANT framework reveals that the creation and implementation of manipulative UI/UX designs are not merely the result of isolated decisions by individual designers or developers but are influenced by a wider network of actors, each with their own set of incentives. This recognition shows the importance of a collaborative approach to ethical design, one that involves all stakeholders in a dialogue aimed at reconciling business objectives with the imperative to protect user autonomy and privacy. By understanding the interconnectedness, like shown in ANT, of these influences, the digital product design community can work towards creating experiences that respect user rights and increase trust within digital systems.

Conclusion

The exploration of manipulative UX/UX design within digital systems shows incoming trends regarding the preference of corporate interests over user rights and data privacy. Through case studies involving giants like Google, Facebook, and Amazon, this research demonstrates the strategic use of dark patterns and deceptive practices to manipulate user consent and behavior. Actor Network Theory (ANT) provides a lens to understand the complex interplay of stakeholders, from designers and users to regulatory bodies and corporate entities, each influencing the ethical landscape of digital design.

As digital interactions become increasingly integral to our daily lives, it is important to advocate for ethical design practices that prioritize transparency, informed consent, and user autonomy. The collective effort of all stakeholders in promoting these values is important in navigating the ethical dilemmas presented by technological advancements. This paper presents a future where a shift towards designing digital products that not only respect user privacy but also contribute to a more trustworthy digital ecosystem will be more beneficial to users. The commitment to ethical UI/UX design is not just a professional obligation but a necessary step towards safeguarding personal privacy and fostering a healthier digital future.

References

Kelly, D. (2023). How social networking sites influence users' privacy choices. https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1383&context=fimspub

Nelissen, L. G. M., & Funk, M. (2022). Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments. International Journal of Design, 16(1), 75-92. https://doi.org/10.57698/v16i1.05

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

Sánchez Chamorro, L., Bongard-Blanchy, K., & Koenig, V. (2023). Ethical tensions in UX Design Practice: Exploring the fine line between persuasion and manipulation in online interfaces. Proceedings of the 2023 ACM Designing Interactive Systems Conference. https://doi.org/10.1145/3563657.3596013

Bjørlo, L.V. Freedom from interference: Decisional privacy as a dimension of consumer privacy online. AMS Rev (2024). https://doi.org/10.1007/s13162-024-00273-x

Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. BMC medical informatics and decision making, 10, 67. https://doi.org/10.1186/1472-6947-10-67

Rikke Frank Jørgensen. (2023) Data and rights in the digital welfare state: the case of Denmark. Information, Communication & Society 26:1, pages 123-138.

Staff in the Office of Technology and The Division of Privacy and Identity Protection. (2023, June 21). FTC takes action against Amazon for enrolling consumers in Amazon prime without consent and sabotaging their attempts to cancel. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their

Staff in the Office of Technology. (2022, January 27). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. Federal Trade Commission.

https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Arntz, P. (2022, January 6). Google and Facebook fined $240 million for making cookies hard to refuse. Malwarebytes. https://www.malwarebytes.com/blog/news/2022/01/google-and-facebook-fined-240-million-for-making-cookies-hard-to-refuse#:~:text=It%20found%20that%20while%20the,single%20one%20to%20accept%20them.