Bus Inf Syst Eng 65(2):201–208 (2023)
https://doi.org/10.1007/s12599-022-00783-7

CATCHWORD

Dark Patterns

Conceptualization and Future Research Directions

Tim Kollmer · Andreas Eckhardt

Received: 1 November 2021 / Accepted: 28 November 2022 / Published online: 12 December 2022

Keywords Dark patterns · Digital dark nudging · Digital sludging · Manipulation techniques · Deception techniques

1 Introduction

Every day, millions of users encounter dark patterns in information systems (IS) (Adams and Sarah 2022). Dark patterns refer to user interface design elements that benefit organizations by deceiving and manipulating users (Brignull 2010; Narayanan et al. 2020). Specifically, dark patterns are designed to infringe on user autonomy by preventing informed choices (Loewenstein et al. 2014; Sunstein 2015). In the context of IS, user autonomy can be defined as self-governance that leads to independent choices and the expression of free will among users (Levy 2006). For example, Instagram, a social networking service, deceives users to activate app notifications by providing a modal dialogue with the options "Not Now" and "OK." Thus, user autonomy is compromised because the necessary option to decline the activation is not provided. As a result, usage frequency increases because more and more users are notified about recent updates (Gray et al. 2018). Consequently, users share their frustrations in online forums such as Reddit (r/assholedesign) and Twitter (#darkpattern) by denouncing organizations that utilize dark patterns (Mathur et al. 2021).

Dark patterns in the IS context can be found across multiple industries and services. (Narayanan et al. 2020; Mathur et al. 2021). Organizations implement dark patterns to increase their revenue, collect data, and steer users' attention (Narayanan et al. 2020). For example, a study by Mathur et al. (2019) shows that around eleven percent of e-commerce websites utilize dark patterns. Surprisingly, well-known websites are more likely to take advantage of dark patterns than little-known websites (Mathur et al. 2019). To protect users and to ensure fair market competition, regulators are taking steps to govern dark patterns (Akhtar 2021). However, regulating dark patterns is challenging because there are already over 100 identified manifestations, and that number continues to grow (Mathur et al. 2019). To protect users against dark patterns, research on digital nudging has proposed several countermeasures, including design principle recommendations and ethical guidelines that aim to guide user interface design processes and ensure user autonomy (Weinmann et al. 2016), but these recommendations and guidelines are neither uniformly mandatory nor enforceable. Consequently, there is only limited research into this potentially dangerous form of user manipulation and deception, despite the need for IS researchers and practitioners to better understand the full scope of dark patterns and to curtail their application by organizations to protect users (Narayanan et al. 2020).

2 Evolution and Significance of Dark Patterns

Initially, manipulation and deception techniques were predominantly applied in brick-and-mortar retail advertising to increase sales (Troisi et al. 2020). With the increasing digitization of sales and advertising processes, organizations also started utilizing manipulation and

Accepted after two revisions by Christine Legner.

T. Kollmer (✉) · A. Eckhardt
Department of Information Systems, University of Innsbruck,
Universitätsstraße 15, 6020 Innsbruck, Austria
e-mail: tim.kollmer@uibk.ac.at

deception techniques in the digital space. During the first decade of the twenty-first century, organizations implemented so-called growth hacking techniques to grow and retain their user base and gain exposure (Narayanan et al. 2020). An example of growth hacking is exploiting user data by inviting everyone in a contact list to use a service without prior permission or notice (Mathur et al. 2021). Over the years, manipulation and deception techniques have also been used for additional purposes, such as to increase revenue, collect data, or steer users' attention (Narayanan et al. 2020).

In 2010, Harry Brignull first coined the term dark patterns, which refers to "*tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something*" (Brignull 2010). Dark patterns (also referred to as deceptive designs) deceive (Narayanan et al. 2020) and manipulate (Westin and Chiasson 2021) users using elements of the choice architecture, which is defined as structure and presentation of choices (Thaler and Sunstein 2008), and the exploitation of psychological vulnerabilities (Mathur et al. 2021). An example for a psychological vulnerability represents the status quo bias, which states that users tend to favor and keep preselected default options (Schneider et al. 2018). Consequently, organizations utilize the status quo bias in dark patterns for instance to foster newsletter subscriptions through preselection of the option to subscribe to the newsletter (Mathur et al. 2021; Weinmann et al. 2016).

However, the initial definition of dark patterns by Brignull (2010) is deficient because it suggests that the subversion of users' intentions is an essential characteristic of dark patterns. Lukoff et al. (2021) enhance Birgnull's definition by investigating dark patterns utilized to maximize the time spent on IS. Here, dark patterns such as infinite scrolling, autoplay, and pull-to-refresh are in line with the user's intention but foster technology addiction (Monge Roffarello and De Russis 2022), which represents an impairment of user autonomy (Levy 2006). In order to provide a more comprehensive definition of dark patterns, we define dark patterns based on Mathur et al. (2021), Weinmann et al. (2016), and Sunstein (2015) as *user interface design elements that compromise user autonomy by preventing informed choices and that may lead to adverse outcomes for the user, such as invasion of privacy, financial loss, and technology addiction*.

Recent research on dark patterns and related phenomena has focused primarily on specifying dark patterns (e.g., Mathur et al. 2021; Bösch et al. 2016), creating dark pattern taxonomies (e.g., Mildner and Savino 2021; Mathur et al. 2019; Gray et al. 2018), and identifying the ethical considerations of dark patterns (e.g., Gray et al. 2018; Fansher et al. 2018). In addition, several studies investigate dark patterns in the context of privacy violations (e.g., Mager and Kranz 2021; Nouwens et al. 2020). In recent years, the volume of research into dark patterns has increased steadily, which also illustrates its relevance for the scientific community (Lukoff et al. 2021). At the same time, the growing pervasiveness of digital technologies in professional and private environments underscores the need to understand and protect users against the effects of dark patterns (Weinmann et al. 2016).

As user information is often collected, shared, and sold by organizations without users permission, there is also a clear demand that such dark patterns need to be regulated by governmental institutions (Smit et al. 2014). Consequently, institutions worldwide invest substantial effort into regulating dark patterns by law (Nouwens et al. 2020; Narayanan et al. 2020). To date, most regulations aim to protect users' data privacy rights (Akhtar 2021). In 2016, the European Parliament passed the General Data Protection Regulation (GDPR), the most comprehensive regulation of user information to date (European Parliament 2016). The GDPR forces organizations to ask users for their consent before collecting any data, provide comprehensive and clear information about how and what data will be collected and processed, and give users the free choice to allow or refuse data collection. Furthermore, data collection consent must be given for one or several specified purposes, and pre-ticket boxes or inactivity may not be interpreted as a user choice or implied consent. Consents also require unambiguousness that results in an affirmative choice of the user. Finally, consent requests must be clearly distinguishable from other user interface design elements (European Parliament 2016).

Although regulations such as GDPR help to protect users against dark patterns, they have limitations. Given that GDPR prohibits the omission of relevant information, organizations utilize user interface design elements to persuade users to provide consent to data collection, which consequently undermines user autonomy (Kollmer 2022). In addition, existing regulations only apply to the use of consents, not to dark patterns per se, which extend to many more aspects of IS (Di Geronimo et al. 2020).

3 Conceptualizing Dark Patterns

Our proposed conceptualization aims to establish a comprehensive and unified understanding of dark patterns. Overall, dark patterns compromise user autonomy by preventing informed choices through digital dark nudges and digital sludges. In the following section, we will define and discuss these two terms and their relationship in greater detail (see Fig. 1).

Dark patterns that utilize digital dark nudging and digital sludging apply various manipulation and deception

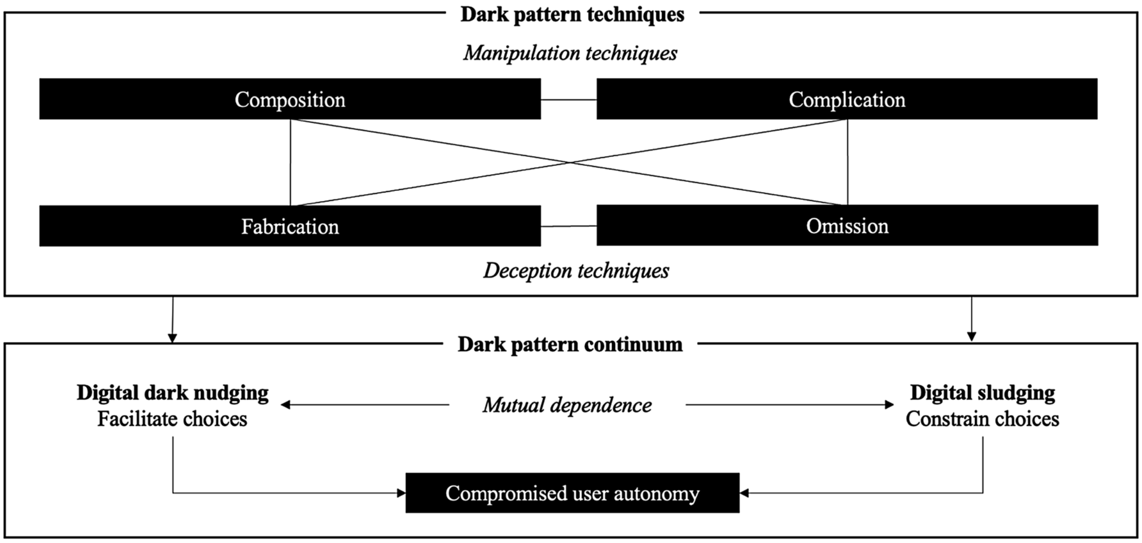

Fig. 1 Conceptualization of dark patterns

techniques. Manipulation techniques provide complete and accurate options and information to the user but exploit users' psychological vulnerabilities and prevent informed choices through composition and complication. In contrast, deception techniques include fabrication of false information concerning an option and the intentional omission of relevant information and/or options. Deception techniques may include dark patterns that are not compliant with regulations. For instance, consent walls omit the option to reject the consent and therefore are not compliant with regulations such as GDPR (Gray et al. 2021). In summary, organizations often utilize a mixture of various manipulation and deception techniques to create dark patterns within their IS.

3.1 Digital Dark Nudging and Digital Sludging as Building Blocks for Dark Patterns

Generally, digital dark nudging and digital sludging represent the essential building blocks in the conceptualization of dark patterns. The term nudging was first introduced in behavioral economics by Thaler and Sunstein (2008), who define it as "*any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives*" (Thaler and Sunstein 2008).

In the digital space, the term digital nudging emerged for user interface design elements that guide users' choices (Weinmann et al. 2016). Thereby, digital nudges activate the non-volitional user agency and facilitate user choices (Meske and Potthoff 2017). Several scholars have proposed nudging principles (e.g., Weinmann et al. 2016) and ethical guidelines (e.g., Renaud and Zimmermann 2018; Sunstein 2015) to "*maximize the good of the nudgee, as judged by the nudgee him- or herself*" (Renaud and Zimmermann 2018), which can be achieved by promoting user autonomy and informed choices (Sunstein 2015). For instance, a digital nudging principle is the mapping of difficult and complex information to familiar evaluation schemes to simplify the information provided (Weinmann et al. 2016). In addition, ethical guidelines demand that digital nudging should respect users' expectations of truthful information and should only be utilized for essential options (Acquisti et al. 2017; Jesse and Jannach 2021). Consequently, digital nudging that is aligned with design principles and ethical guidelines promoting user autonomy can be considered digital bright nudging.

In contrast, digital nudging that violates design principles and ethical guidelines and consequently compromises user autonomy is considered *digital dark nudging*. Specifically, digital dark nudging fosters uninformed choices by complicating, composing, fabricating, and omitting information to manipulate user choices. Digital dark nudging often includes non-essential options during the process. For instance, some European low-cost air carriers undertake digital dark nudging by presenting non-essential options such as travel insurance during the booking process (Weinmann et al. 2016).

In addition to digital dark nudging, dark patterns also represent excessive or unjustified hurdles that complicate users' task completion (see Table 1). In the IS context, these hurdles are defined as *digital sludges* (Kollmer 2022). While digital dark nudging predominantly activates non-volitional user agency, digital sludging impedes volitional user agency and therefore restricts intended user choices (see Table 1). Digital sludging often involves intentional or inadvertent waiting times and obstructions to processes (Sunstein 2020). As a result, sludged options impede users'

Table 1 Manipulation techniques (based on Sunstein 2020)

Technique	Description	Example
Composition	Shifting the hierarchy between different choices to darkly nudge a specific choice and sludge the superior alternatives and vice versa	A technology company marks the most expensive subscription service as recommended
Complication	Increasing complexity to sludge a specific choice which in turn darkly nudges the other choices	A newspaper website provides increased complexity for the option to refuse cookies by requiring separate refusals for each site vendor with a legitimate interest

free choice and autonomy. For instance, the cancellation process of a leading audiobook provider includes multiple steps that present membership benefits in order to influence the user to reconsider the cancellation (Witman 2020). Besides slowing and extending users' time for task completion, digital sludging also induces unwanted side effects, such as an increased cognitive load, to manipulate users' choices (Thaler 2018).

Mills (2020) identifies a symmetry between digital nudging and digital sludging, showing how a digital nudge that favors one choice option can lead to the respective digital sludging of all other choices and vice versa. In other words, digital dark nudging and digital sludging occur in a simultaneous, mutually dependent relationship. For instance, unsubscribing from a magazine or newsletter often involves digital sludging in the form of an onerous series of checks if users really want to terminate their subscription. At the same time, these obstacles and speed bumps to unsubscribing lead to digital dark nudging favoring the decision option to continue to subscribe (Soman 2020).

3.2 Manipulation Techniques

A focal element of dark patterns are manipulation techniques. Hereby, organizations compromise user autonomy by influencing the composition and complexity of choices in several ways. First, organizations influence the composition of choices to foster uninformed choices among users. To achieve this, organizations often rely on user interface design elements such as color, size, and placement to influence recognition (Faraday 2000). Plain color, small sizes, and placement involving scrolling decrease the likelihood of the user interface design element being recognized. In contrast, bright colors, large sizes, and central placement draw user attention (Faraday 2000). For instance, organizations stimulate users' fear of missing out by prominently indicating the scarcity of their products in user interface design elements (Westin and Chiasson 2021). The fear of missing out is characterized as a user's anxious expectation that one is absent from having a rewarding experience that others currently enjoy (Przybylski et al. 2013). Consequently, users develop a feeling of urgency and are darkly nudged into selecting a choice, instantly. The resulting choice is often uninformed because the user did not invest enough time to evaluate the remaining choices (Good and Hyman 2020).

Second, organizations often utilize dark patterns to complicate the processes of the IS by using complex language and challenging vocabulary. Such techniques make it harder for users to comprehend and evaluate the choices provided. As a result, the cognitive effort required to decipher complicated options increases (Münscher et al. 2016). According to the phenomenon referred to as the "law of less work" (Solomon 1948), most people (in this case, users) try to avoid excessive cognitive effort within the decision-making process and prefer simple choices. Table 1 provides an overview of the presented manipulation techniques and indicates an exemplary application.

3.3 Deception Techniques

The other focal element of dark patterns are deception techniques that provide supplemental potentialities for organizations to compromise user autonomy by fostering uninformed choices.

The first deception technique of organizations is to introduce false beliefs through fabricated information and/or options. E-commerce organizations commonly use fabrication to increase revenue (Mathur et al. 2021). For instance, deceptive product reviews in e-commerce platforms use false information about product quality and experiences with the product. As a result, users get darkly nudged into ordering products based on fabricated information. At the same time, all other potentially superior choices are sludged (see Table 2).

Dark patterns can also be utilized by omitting relevant information and choices (Münscher et al. 2016), such as when an organization hides the consequences of a choice by creating a disconnect between choice and consequence. As a result, it is difficult for users to evaluate arguments for or against the choice, which leads to uninformed choices and compromised user autonomy (Münscher et al. 2016). In addition, dark patterns include omitting relevant options

Table 2 Deception techniques (based on Gray et al. 2021; Luca and Zervas 2016)

Technique	Description	Example
Fabrication	Providing false information to darkly nudge users' choices and in turn sludge the other choices	A leading online marketplace provides deceptive and fabricated experiences in its product reviews to darkly nudge users to purchase certain products
Omission	Leaving out necessary information to sludge users' choices and in turn darkly nudge the other choices	A tax application does not allow unsubscribing from their newsletter after the initial subscription

all together with the outcome that users are sludged and unable to make the respective choice. Furthermore, organizations take actions without disclosing their actions to the user (Bösch et al. 2016). For example, organizations may intentionally omit the information that an online purchase is part of a recurring subscription to users (Di Geronimo et al. 2020). Consequently, users are darkly nudged into purchasing a recurring subscription (Mathur et al. 2021). Table 2 indicates a short description and an exemplary application for fabrication and omission.

4 Recommendations for Future Research on Dark Patterns

As business and information systems engineering (BISE) and IS scholars have become more concerned about the challenges associated with rapid digitization, a common focus is the critical issue of user autonomy (Spiekermann et al. 2022). Our conceptualization of dark patterns demonstrates how manipulation and deception techniques lead to digital dark nudging and digital sludging. In turn, dark patterns compromise user autonomy by preventing informed choices. In the following, we identify specific challenges regarding dark patterns and provide an overview of future research avenues for the BISE/IS community. We structure research opportunities according to three major stakeholders concerned with dark patterns: users, organizations, and regulators.

Users are the individuals exposed to dark patterns and compromised in their autonomy (Sunstein 2015), organizations utilize dark patterns either purposefully or inadvertently in their IS to increase their revenue, collect data, and steer users' attention (Narayanan et al. 2020). In the same vein, regulators are mainly governmental bodies with an overarching responsibility to ensure fair competition between organizations and to protect users and citizens in general against dark patterns (Mathur et al. 2021). Table 3 summarizes our identified research opportunities within this trifecta of dark pattern stakeholders.

4.1 User Vulnerabilities and Long-term Consequences

As users are targeted by dark patterns and consequently compromised in their autonomy, we suggest investigating *user vulnerabilities* towards dark patterns and the *long-term consequences* of dark patterns *on users*.

Generally, user vulnerability to internet security is highly dependent on their personality profiles (Goel et al. 2017). In the same vein, users' personality profiles determine users stress levels during the interaction with IS (Pflügner et al. 2021). Therefore, we anticipate that specific personality profiles influence how vulnerable users are to be affected by dark patterns. We thus call for nuanced empirical investigation into *dark pattern vulnerabilities based on users' personality profiles* in BISE/IS research.

From a user perspective, existing research predominately focuses on the immediate (short-term) influence of dark patterns on users' choices (e.g., Bösch et al. 2016). However, utilizing dark patterns can also have *long-term consequences for users*. For instance, existing research indicates that the dark patterns of infinite scrolling, autoplay, and pull-to-refresh may foster technology addiction among users (Monge Roffarello and De Russis 2022). However, it remains unknown whether dark patterns lead to other potentially harmful long-term consequences for users. Therefore, we recommend future BISE/IS research to examine the long-term consequences of dark patterns for users.

4.2 Organizational Drivers and Long-term Consequences

We recommend future research into the *organizational characteristics* that lead to the implementation of dark patterns and the negative *long-term consequences of dark patterns on organizations.*

Previous studies mainly attribute the responsibility for creating dark patterns to the respective user experience (UX) designer (e.g., Fansher et al. 2018). This focus ignores other stakeholders involved in the dark pattern development process, such as requirement engineers, product owners and champions, strategic business executives, and marketing professionals. We recommend that BISE/IS

Table 3 Avenues and questions for future research

Stakeholder	Research avenue	Exemplary research question
Users	User vulnerabilities	Which personality profiles make users more vulnerable to dark patterns?
	Consequences of dark patterns for users	What are the long-term consequences of dark patterns for users?
Organizations	Drivers of dark patterns	What are the organizational characteristics that drive the utilization of dark patterns?
	Consequences of dark patterns for organizations	What are the negative long-term consequences of dark pattern use for organizations?
Regulators	Unified design principles	How effective are mandatory unified design principles to prevent dark pattern use of organizations?
	Dark pattern regulation enforcement	How can dark pattern prevention regulations be enforced?

scholars investigate how *organizational characteristics* such as different stakeholders and their responsibilities, roles, and traits as well as the corresponding corporate culture and processes drive the development and utilization of dark patterns.

In addition, dark patterns can distort free-market competition and create unfair market shares for specific products or services in the short-term (Mathur et al. 2021). But this may also have counter-effects if users recognize and react negatively to the dark pattern techniques utilized. Therefore, future BISE/IS research should investigate the potential *long-term negative consequences of dark pattern* use for organizations, such as declining user volumes and revenue (Narayanan et al. 2020).

4.3 Unified Design Principles and Regulation Enforcement

The increasing prevalence and ubiquity of dark patterns underscore the crucial role of regulators (Mathur et al. 2019). We encourage future BISE/IS research to investigate the relative effectiveness of mandatory *unified design principles* in preventing dark pattern use and how these *regulations can be enforced*.

In order to develop unified design principles, it is necessary to incorporate more ethical considerations into design science methodologies, both in the design process and artifact creation. In particular, engaging in deontological reasoning for design science research contributes to existing design science research within the BISE/IS community (e.g., Haße et al. 2022; Diederich et al. 2020) and may lead to *unified design principles* that prevent the creation of dark patterns in the first place. This is especially important because technological advancements will lead to novel applications of dark patterns like for example in conversational agents, virtual reality, and the metaverse (e.g., Wohlgenannt et al. 2020).

Additionally, ensuring that organizations comply with dark pattern regulations in IS remains challenging. Currently, most regulations are introduced by governmental bodies and executed as well as enforced by the respective legal authority (Tyler 2001). However, there is significant evidence that many organizations do not comply with dark pattern regulations (Gray et al. 2021; Nouwens et al. 2020). Consequently, we encourage BISE/IS research to investigate the relative effectiveness of various technical measures to *enforce organizational compliance* with dark pattern regulations. For instance, Mathur et al. (2019) investigate the use of crawlers to identify dark patterns on websites, which could also be used to monitor and enforce organizational compliance with dark pattern regulations.

As there is a keen interest in dark patterns and their implications for various groups in research and society, we encourage BISE/IS scholars to engage in research on dark patterns to guide organizations and regulators and to protect users in the digital space.

Funding Open access funding provided by University of Innsbruck and Medical University of Innsbruck.

References

Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Leon PG, Sadeh N, Schaub F, Sleeper M (2017)

Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput Surv 50(3):1–41

Adams KL, Sarah (2022) Frustrating user-experience tactics can have real harm, "dark pattern" expert says. https://www.marketplace.org/2022/08/10/dark-patterns-frustrating-web-app-tactics/. Accessed 26 Sep 2022

Akhtar A (2021) California is banning companies from using 'dark patterns,' a sneaky website design that makes things like canceling a subscription frustratingly difficult. https://www.businessinsider.com/what-are-dark-patterns-2021-3.

Bösch C, Erb B, Kargl F, Kopp H, Pfattheicher S (2016) Tales from the dark side: privacy dark strategies and privacy dark patterns. Proc Priv Enhancing Technol 2016(4):237–254

Brignull H (2010) Dark patterns. https://darkpatterns.org/. Accessed 9 Aug 2021

Diederich S, Brendel AB, Kolbe LM (2020) Designing anthropomorphic enterprise conversational agents. Bus Inf Syst Eng 62(3):193–209. https://doi.org/10.1007/s12599-020-00639-y

Fansher M, Chivukula SS, Gray CM (2018) #darkpatterns: UX practitioner conversations about ethical design. In: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3170427.3188553

Faraday P (2000) Visually critiquing web pages. In: Correia N, Chambel T, Davenport G (eds) Multimedia '99 Eurographics. Springer, Vienna

Di Geronimo L, Braz L, Fregnan E, Palomba F, Bacchelli A (2020) UI dark patterns and where to find them: a study on mobile applications and user perception. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376600

Goel S, Williams K, Dincelli E (2017) Got phished? Internet security and human vulnerability. J Assoc Inf Syst 18(1):2

Good MC, Hyman MR (2020) 'Fear of missing out': antecedents and influence on purchase likelihood. J Mark Theor Pract 28(3):330–341

Gray CM, Kou Y, Battles B, Hoggatt J, Toombs AL (2018) The dark (patterns) side of UX design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3173574.3174108

Gray CM, Santos C, Bielova N, Toth M, Clifford D (2021) Dark patterns and the legal requirements of consent banners: an interaction criticism perspective. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3411764.3445779

Haße H, van der Valk H, Möller F, Otto B (2022) Design principles for shared digital twins in distributed systems. Bus Inf Syst Eng. https://doi.org/10.1007/s12599-022-00751-1

Jesse M, Jannach D (2021) Digital nudging with recommender systems: survey and future directions. Comput Hum Behav Rep 3:100052

Kollmer T (2022) Digital sludging in the privacy context: evidence of a multigroup analysis. In: AMCIS 2022 Proceedings. https://aisel.aisnet.org/amcis2022/sig_hci/sig_hci/4

Levy N (2006) Autonomy and addiction. Can J Philos 36(3):427–447

Loewenstein G, Sunstein CR, Golman R (2014) Disclosure: psychology changes everything. Annu Rev Econ 6(1):391–419

Luca M, Zervas G (2016) Fake it till you make it: reputation, competition, and Yelp review fraud. Manag Sci 62(12):3412–3427

Lukoff K, Hiniker A, Gray CM, Mathur A, Chivukula SS (2021) What can CHI do about dark patterns? In: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3411763.3441360

Mager S, Kranz J (2021) Consent notices and the willingness-to-sell observational data: evidence from user reactions in the field. In: Proceedings of the 29th European Conference on Information Systems

Mathur A, Acar G, Friedman MJ, Lucherini E, Mayer J, Chetty M, Narayanan A (2019) Dark patterns at scale: findings from a crawl of 11K shopping websites. In: Proceedings of the ACM on Human-Computer Interaction 3. https://doi.org/10.1145/3359183

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

Meske C, Potthoff T (2017) The DINU-model – a process model for the design of nudges. In: 25th European Conference on Information Systems. https://aisel.aisnet.org/ecis2017_rip/11

Mildner T, Savino G-L (2021) How social are social media: the dark patterns in Facebook's interface. arXiv preprint arXiv:210310725

Mills S (2020) Nudge/sludge symmetry: on the relationship between nudge and sludge and the resulting ontological, normative and transparency implications. Behav Public Policy. https://doi.org/10.1017/bpp.2020.61

Monge Roffarello A, De Russis L (2022) Towards understanding the dark patterns that steal our attention. In: CHI Conference on Human Factors in Computing Systems Extended Abstracts. https://doi.org/10.1145/3491101.3519829

Münscher R, Vetter M, Scheuerle T (2016) A review and taxonomy of choice architecture techniques. J Behav Decis Mak 29(5):511–524

Narayanan A, Mathur A, Chetty M, Kshirsagar M (2020) Dark patterns: past, present, and future: the evolution of tricky user interfaces. Queue 18(2):67–92

Nouwens M, Liccardi I, Veale M, Karger D, Kagal L (2020) Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In: Proceedings of the 2020 CHI conference on human factors in computing systems. https://doi.org/10.1145/3313831.3376321

European Parliament (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Pflügner K, Maier C, Mattke J, Weitzel T (2021) Personality profiles that put users at risk of perceiving technostress. Bus Inf Syst Eng 63(4):389–402. https://doi.org/10.1007/s12599-020-00668-7

Przybylski AK, Murayama K, DeHaan CR, Gladwell V (2013) Motivational, emotional, and behavioral correlates of fear of missing out. Comput Hum Behav 29(4):1841–1848

Renaud K, Zimmermann V (2018) Ethical guidelines for nudging in information security & privacy. Int J Hum-Comput Stud 120:22–35

Schneider C, Weinmann M, vom Brocke J (2018) Digital nudging: guiding online user choices through interface design. Commun ACM 61(7):67–73

Smit EG, Van Noort G, Voorveld HA (2014) Understanding online behavioural advertising: user knowledge, privacy concerns and online coping behaviour in Europe. Comput Hum Behav 32:15–22

Solomon RL (1948) The influence of work on behavior. Psychol Bull 45(1):1

Soman D (2020) Sludge: a very short introduction. Research Report Series, Behaviourally Informed Organizations Partnership. Univ of Toronto

Spiekermann S, Krasnova H, Hinz O, Baumann A, Benlian A, Gimpel H, Heimbach I, Köster A, Maedche A, Niehaves B (2022)

Values and ethics in information systems. Bus Inf Syst Eng 64(2):247–264. https://doi.org/10.1007/s12599-021-00734-8

Sunstein CR (2015) The ethics of nudging. Yale J Reg 32:413

Sunstein CR (2020) Sludge audits. Behav Publ Policy 6(4):654–673

Thaler RH (2018) Nudge, not sludge. Sci 361(6401):431

Thaler RH, Sunstein CR (2008) Nudge: improving decisions about health, wealth, and happiness. Penguin

Troisi O, Maione G, Grimaldi M, Loia F (2020) Growth hacking: insights on data-driven decision-making from three firms. Ind Mark Manag 90:538–557

Tyler TR (2001) Public trust and confidence in legal authorities: what do majority and minority group members want from the law and legal institutions? Behav Sci Law 19(2):215–235

Weinmann M, Schneider C, vom Brocke J (2016) Digital nudging. Bus Inf Syst Eng 58(6):433–436. https://doi.org/10.1007/s12599-016-0453-1

Westin F, Chiasson S (2021) “It’s so difficult to sever that connection”: the role of FoMO in users’ reluctant privacy behaviours. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3411764.3445104

Witman E (2020) How to cancel your Audible membership, or put your subscription on hold. Bus Insider. https://www.businessinsider.com/how-to-cancel-audible. Accessed 25 Feb 2022

Wohlgenannt I, Simons A, Stieglitz S (2020) Virtual reality. Bus Inf Syst Eng 62(5):455–461. https://doi.org/10.1007/s12599-020-00658-9