Conceptualizations of User Autonomy within the Normative Evaluation of Dark Patterns*

Sanju Ahuja & Jyoti Kumar
Department of Design
Indian Institute of Technology Delhi
Hauz Khas, New Delhi 110016, India
Email: sanju.ahuja@design.iitd.ac.in; jyoti@design.iitd.ac.in

Abstract

Dark patterns have received significant attention in literature as interface design practices which undermine users' autonomy by coercing, misleading or manipulating their decision making and behavior. Individual autonomy has been argued to be one of the normative lenses for the evaluation of dark patterns. However, theoretical perspectives on autonomy have not been sufficiently adapted in literature to identify the ethical concerns raised by dark patterns. The aim of this paper is to conceptualize user autonomy within the context of dark patterns. In this paper, we systematically review 151 dark patterns from 16 taxonomies to understand how dark patterns threaten users' autonomy. We demonstrate through this analysis that implications for autonomy arise along four dimensions, because autonomy itself can be understood as subsuming several distinguishable concepts. These are agency, freedom of choice, control and independence. We argue that an assessment of whether a design pattern qualifies as 'dark' should account for the sense in which autonomy is threatened, as individuals' rights and expectations of autonomy vary in various contexts and depend upon the interpretation of autonomy. This paper aims to contribute to the development of the normative lens of individual autonomy for the evaluation of dark patterns, as well as for persuasive design more broadly.

1. Introduction

The use of dark patterns has become ubiquitous on the web, in digital platforms, in information systems and within mobile applications. Dark patterns are user interface designs which intend to coerce or manipulate users into acting in certain ways (Mathur et al., 2021). 'Dark patterns' is a practitioner created construct and the term was coined by Brignull (2010) to raise awareness about potentially unethical design practices. It encompasses instances of design where knowledge of human psychology and behavior is used to influence users into making unintended and unwanted choices or behave in ways that are not in their best interests (Gray et al., 2018). Dark patterns are often designed to fulfil commercial goals, such as increasing revenue, gathering user information and maximizing user engagement. Research has demonstrated the preponderance of dark patterns in various contexts such as e-commerce, mobile games and online privacy (Krisam et al., 2021; Mathur et al., 2019; Utz et al., 2019; Zagal et al., 2013).

Ethical concerns raised by dark patterns have been frequently discussed in literature. Individual autonomy has been identified as an important normative lens for the evaluation of dark patterns. Individual autonomy is understood in philosophical literature as an individual's right to self-governance (Buss & Westlund,

* This is the accepted version of the manuscript for the paper:
Ahuja, S. & Kumar, J. (2022). Conceptualizations of User Autonomy within the Normative Evaluation of Dark Patterns. Ethics & Information Technology, 24(4), Article 52. https://doi.org/10.1007/s10676-022-09672-9

2018). It is constituted by the freedom to be the person one wants to be and to pursue one's goals without unjustifiable hindrances or interferences (Roskies, 2021). Concerns about autonomy are implicit within dark pattern definitions. For example, Brignull (2010) defined dark patterns as tricks that 'make you do things you didn't mean to' and Bösch et al. (2016) argued that dark patterns trick users into performing 'unintended and unwanted' actions. Others have argued that dark patterns deceive, manipulate and mislead users (Lacey & Caudwell, 2019; Maier & Harr, 2020; & Chiasson, 2021). On the other hand, the autonomy perspective has also been critiqued for sweeping broadly, depending on a highly idealized version of human action and dubbing all interferences with decision making as dark (Mathur et al., 2021). However, this paper takes the view that whenever any design intervention intends to affect a change of behavior, considerations of autonomy are fundamental to their evaluation. Both theoretical and intuitive understandings of autonomy acknowledge that not all interventions with decision making undermine people's autonomy or are ethically problematic. Psychological sciences have demonstrated that human decision making is a combination of automatic and reflective processes, and that the 'idealized' rational version of autonomy does not account for much of human behavior (Kahneman & Tversky, 1979; Stanovich & West, 2000; Tversky & Kahneman, 1974). Despite this nature of decision making, with its inherent biases, dark patterns introduce externalities which undermine the quality of whatever choice was otherwise possible through the reasonable process of everyday information gathering and evaluation. Even though human decision making is not perfectly rational, it still supports the experience of autonomy, and burdens can be placed upon this process. Therefore, this paper argues that there is a need to develop the autonomy perspective for the evaluation of dark patterns, such that it can account for these criticisms as well as help experts and policymakers identify threats to autonomy within information technologies.

The word autonomy itself subsumes several distinguishable concepts. The 'sense' in which autonomy is infringed upon differs across dark pattern interactions. For example, within e-commerce, the sense in which nagging a user infringes upon their autonomy, through relentless pestering, differs from the sense in which sneaking a product into a user's shopping cart infringes upon their autonomy, by hiding important information and bypassing their consent (Gray et al., 2018). In the first case, the user is painfully aware of the pestering but the sneaking is often non-transparent. These approaches are again different from the sense in which 'FoMo-centric design' infringes upon users' autonomy, by exploiting their own tendencies to make decisions based on the behavior of peers (Westin & Chiasson, 2021). This distinction is captured by interpreting autonomy in its different 'conceptualizations' (Vugts et al., 2020). Users' experiences of autonomy, as well as their rights and expectations in any context, are dependent on the sense in which autonomy is interpreted. While restrictions on choices or the use of incentives may be considered legitimate in many contexts, the use of manipulation and deception is often considered unacceptable. Users also tend to voluntarily adopt technologies which place restrictions upon them, such as quit-smoking apps, and digital well-being apps, to enhance their overall sense of autonomy. This suggests that different senses of autonomy take precedence in different contexts. Therefore, identifying the conceptualization of autonomy, i.e., the sense in which a dark pattern poses an autonomy threat to users, is crucial to its normative evaluation. However, the various conceptualizations of autonomy which underlie concerns about dark patterns have not been identified in literature.

In this paper, we conduct a systematic review of literature to identify these different conceptualizations of autonomy at play within the concerns raised by dark patterns. We present an analysis of 151 dark patterns from

16 taxonomies to identify the ways in which dark patterns threaten users' autonomy. For each dark pattern, we first interpret its mechanism of influence on users to identify the underlying ethical concern. We then conduct a thematic analysis upon this corpus of dark patterns, to consolidate them into dark 'strategies'. We identify the shared ethics considerations underlying these 'dark strategies' and situate them within different theoretical conceptualizations of autonomy. Overall, from the analysis of 151 dark patterns, we discovered 25 dark strategies which raise seven ethical considerations. These considerations are grounded in four theoretical conceptualizations of autonomy: *agency, freedom of choice, control and independence*. This paper shows that the ethical concerns raised by dark patterns from a user autonomy perspective can belong to any of the four dimensions of autonomy, and dark patterns can be deemed ethically impermissible due to one or more of the seven ethical considerations identified in this paper. If the impact of a dark pattern is conflicting along multiple dimensions, its normative evaluation also needs to account for the sense of autonomy which takes precedence in any particular context.

2. Background and Related Work

In this section, we first provide background on how persuasive techniques have historically been used to influence people, preceding the era of dark patterns within information technologies. We highlight how influence through information technologies is different from more traditional forms of persuasion, such as political persuasion or marketing techniques. We then provide background on the literature on dark patterns, followed by literature from two related domains: 'persuasive technology' in human computer interaction and 'nudge' in behavioral economics. We then present theoretical perspectives on autonomy which can aid the normative evaluation of dark patterns.

2.1 Traditional Forms of Persuasion

The use of persuasion to influence people precedes the era of modern day information technologies and interactive systems. Persuasive techniques have been used by governments and private entities alike to influence people' attitudes and behaviors. Politicians and media have used propaganda techniques to alter citizens' perceptions of reality (Herman & Chomsky, 1988; Lasswell, 1927). Government policies such as interest rates and credit systems are often intentional attempts at influencing citizens' economic behavior (von Neumann & Morgenstern, 1944). Businesses seek to influence consumers through sophisticated marketing strategies (Cialdini, 1984). Supermarkets are designed to maximize purchases through product positioning, lighting, background music and lack of time cues (Lindstrom, 2012; Milliman, 1982). Retailers have since long gathered consumer information through loyalty cards to generate mail coupons and offers for consumers (Cortiñas et al., 2008; Passingham, 1998). In the workplace, it has been common for decades for employers to monitor attendance through biometric systems (Woodward, 1997).

However, advances in information technologies have added newer dimensions of sophistication and pervasiveness, vastly increasing the possibilities and opportunities of persuasion. For example, latest employee monitoring systems not only monitor attendance, but keep a minute-by-minute track of employee activity and productivity[2]. E-commerce websites do not merely persuade by positioning and aesthetic, but also by personalizing and targeting their offerings based on intricate characteristics of the consumer (Zuboff, 2019). There

[2] https://www.pcmag.com/picks/the-best-employee-monitoring-software

has also been global outrage over the use of personalized political targeting during electoral campaigns (Susser et al., 2019). Persuasion is also pervasive in the domain of online privacy. There is an abundance of websites which collect private data through the use of cookies for advertising purposes (Frischmann & Selinger, 2018; Urban et al., 2020). There is also a dimension of context, which determines who is being persuaded in what situation. For example, gambling machines have been historically designed to exploit people's obsessive tendencies and limited propensity for self-control (Schüll, 2012). Similar techniques are now being deployed in children's games, encouraging children to spend excessive time and money on gaming and normalizing addictive forms of interaction (Lewis, 2014). Another dimension of persuasion within information technologies is lack of transparency, which also relates to their novelty (Susser et al., 2019). When consumers become aware of and accustomed to persuasive techniques, it provides them with an opportunity to adjust their behavior, which partially nullifies their influence (Friestad & Wright, 1994). However, at present, a large proportion of consumers are unable to understand or reconstruct the impact of digital influence on their own behavior. Therefore, persuasion embedded in information technologies faces a crisis of transparency (Hansen & Jespersen, 2013). These characteristics of persuasion in the digital era have led to the emergence of the specialized domains of their study, such as dark patterns, persuasive technology and nudge.

2.2 Dark Patterns

The term dark patterns was coined by Brignull (2010) to highlight unethical design practices on websites and mobile applications. Since then, literature has developed upon the concept with rich descriptive contributions, identifying and taxonomizing dark patterns in various contexts. Brignull's original taxonomy consisted of 12 dark patterns, with an intent to raise awareness about the problem. Gray et al. (2018) collected a corpus of dark patterns in the wild and synthesized them into a taxonomy which subsumed Brignull's taxonomy of dark patterns. Zagal et al. (2013) developed a taxonomy of dark patterns in mobile games, Bösch et al. (2016) developed a taxonomy of privacy dark strategies using the privacy by design framework, and Mathur et al. (2019) categorized dark patterns that they encountered in the wild from a crawl of e-commerce websites. Researchers have also raised concerns about the darkness of design 'strategies' such as the cuteness of robots (Lacey & Caudwell, 2019) and 'FoMo-centric design' (Westin & Chiasson, 2021). Dark patterns have also come under the notice of policymakers with various ongoing attempts to regulate or restrict them, such as the California Privacy Rights Act [CPRA] (California Secretary of State, 2020) and the Deceptive Experiences to Online Users Reduction [DETOUR] Act (Warner & Fischer, 2019) in the United States. Wherever public awareness exists of the use of dark patterns, such as in online communities and forums (Twitter #darkpatterns, @darkpatterns; Reddit r/assholedesign), it is accompanied with both a sense of frustration and condemnation (Gray et al., 2020).

2.3 Persuasive Technology

Although the term 'dark patterns' was coined in 2010, similar concepts have been previously articulated in literature. Fogg (2002) used the term 'persuasive technologies' for interactive systems designed to influence people's attitudes and behavior. In his book on the subject, Fogg primarily focused on examples of technologies that were persuasive on the level of functionality or overall intent. However, he predicted a future trend in which persuasive strategies would start being designed into everyday consumer products for influencing and motivating people, even when technologies were not explicitly designed for behavior change. He also argued that within this trend, the 'strategy' and not the 'product' would become the unit of analysis. Fogg also discussed persuasive

'tactics' in his book, which were specific implementations of persuasive strategies. He argued that persuasive strategies were finite but the possibilities of 'tactics' were limitless. We posit that dark patterns can be viewed as persuasive 'tactics', which are specific implementations of their underlying persuasive strategies.

Ethics concerns about persuasive technologies were perhaps first articulated by Berdichevsky and Neuenschwander (1999), who argued that persuasive technologies should be used to promote ethical outcomes, should respect the autonomy of the individual, and that designers should bear the responsibility for any predictably harmful outcomes of the technology. Since then, several discourses on the ethics of persuasive technologies have touched upon concerns about users' autonomy. Fogg (2002) discussed the ethics of persuasive technologies and raised concerns about using emotions to persuade, deception, coercion, operant conditioning and surveillance. Verbeek (2009) argued that ambient intelligence creates radically new experiences of persuasive design, as these technologies merge with the environment. He argued that these technologies can encroach greatly on our everyday activities and our choice processes. According to Verbeek, the desirability of such persuasions is dependent on whether there are mechanisms to determine what persuasions are acceptable, whether responsibility of outcomes can be ascribed and whether users are able to withdraw from persuasive influences. Nagenborg (2014) articulated ethical concerns about persuasion based on surveillance technologies and their implications for users' freedom, even when privacy concerns are minimal. Spahn (2011) conceptualized persuasion as a 'speech act' and derived ethical guidelines for persuasive technologies by applying discourse ethics to their assessment.

2.4 Nudge

The present work on the ethics of dark patterns also takes place in the context of research being conducted in other fields concerned with persuasion and behavior change interventions. The research on the ethics of nudges in behavioral economics has focused significantly on autonomy. Within literature on nudging, the concern for freedom of choice has taken a central consideration in ethics discussions. When Thaler and Sunstein (2008) proposed nudging as a policy solution for socially desirable behavior change, they proposed their suggestions with a libertarian paternalism framework. The framework suggested that nudges, even when they intend to benefit those being nudged, should always preserve people's freedom of choice by not making alternative choices difficult or costly. Hansen and Jespersen (2013) argued that the mere theoretical preservation of freedom was insufficient to prevent people against manipulation, and that in practice only nudges which were transparent and promoted reflective decision making truly preserved people's freedom. Saghai (2013) developed the concept of 'easy resistibility' to help ascertain the ethics of nudges. He argued that an influence is easily resistible when there is a possibility of it becoming transparent, when the persuaded individual has the capacity to inhibit their triggered propensity towards the target behavior and when the persuaded individual is not put under circumstances which would undermine the relatively effortless exercise of transparency and inhibition. However, Saghai does not claim that easy resistibility is a justification for moral permissibility since the persuader may lack the legitimacy to interact with the persuaded individual on those terms.

2.5 Autonomy

2.5.1 The Importance of Autonomy

Autonomy is widely appreciated as a valuable aspect of personhood (Roskies, 2021), and the concept of autonomy gives rise to notions of morality and responsibility (Frankfurt, 1971). Autonomy has also been argued to have

innate psychological value for humans. According to self-determination theory, autonomy is one of the three innate psychological needs of humans (Ryan & Deci, 2000). Deci and Ryan (2000) argued that the sense of autonomy creates a heightened sense of motivation and positive emotions. Conversely, the psychological reactance theory suggests that restrictions on one's freedom elicit a state of negative arousal (Brehm, 1966; Steindl, 2015). André et al. (2018) outlined the benefits of experiencing a sense of autonomy for positive affect, satisfaction, overall well-being and better life outcomes. The experience of autonomy improves the subjective utility of choice whenever choice is made that self-signals willpower against giving in to temptation (Dhar & Wertenbroch, 2012). In a marketplace, the experience of autonomy improves the experience of hedonic consumption when the choice is made autonomously, as opposed to being made by someone else such as an expert (Botti & McGill, 2011). Experiments show that the feeling of control over one's life has important consequences for physical and physiological health, in addition to psychological consequences (Langer & Rodin, 1976). Although the lens of autonomy has been criticized as being overly individualistic, accounts of autonomy have been developed to account for shared or relational aspects of autonomy (Mackenzie & Stoljar, 2000). In applied ethics, autonomy is a fundamental value for the protection of humans. Examinations of autonomy figure in medical ethics, education policy, and research on human subjects (Christman, 2020). In technological applications such as persuasive technology, ambient intelligence, big data applications and brain computer interfaces, autonomy has emerged as an important normative lens through which to view and analyze the ethical impact of technology (Brey, 2005; Fogg, 2002; Friedrich et al., 2018; Verbeek, 2009).

2.5.2 Philosophical Conceptualizations of Autonomy

Across domains, autonomy has been understood as subsuming different concepts or notions. Two conceptualizations of autonomy widely appear within normative assessments of novel technologies: competence and authenticity. In a critical analysis of brain computer interfaces, Friedrich et al. (2018) adopted the view of autonomy as competence, which can be understood as an individual's capacity for self-determination or self-rule. They conceptualized autonomy as a multi-component ability consisting of a) the ability to use information and knowledge to produce reasons, b) ability to ensure that intended actions are realized effectively (control), and c) ability to enact intentions within concrete relationships and contexts. Another frequently appearing conceptualization of autonomy in literature is that of authenticity. To be considered self-governing, common intuition requires a person to act for reasons grounded in her authentic self, reasons which can be considered her own (Betzler, 2009). In psychological terms, the authenticity perspective emphasizes the importance of a coherent self or a narrative self (Mackenzie and Walker, 2015; Erler, 2011; Pugh et al., 2017, Schechtman, 2014). Research has shown that the ability to create and sustain this narrative is a measure of psychological health (Waters & Fivush, 2014). Concerns about authenticity have been discussed significantly in relation to neurotechnology, since even modest brain changes can affect the construct of the self (Levy, 2007). Other non-invasive technologies have also been argued to pose threats to authenticity. For example, indirect and covert manipulation of thoughts through subliminal advertising and neuromarketing could potentially be used to induce desires and behavioral changes not in line with one's conceptions of value.

A recent work by Vugts et al. (2020) presented a systematic review of nudge literature with the aim to identify the conceptualizations of autonomy underlying the ethical debate on nudging. Through a thematic

analysis of autonomy references in literature, they showed that three conceptualizations of autonomy dominated the discussions: agency, freedom of choice and self-constitution.

- The conceptualization of agency concerns an individual's capacity to choose and decide (Vugts et al., 2020). Agency, which has also been referred to as 'competence' in certain contexts (Friedrich et al., 2018), involves being able to lead one's life voluntarily on the basis of reasons and intentions. It includes the ability to reason about one's preferences based on one's own goals, and the ability to reflect on one's choices. Vugts et al. argue that the ability to govern oneself, rather than exhibiting mere stimulus-response behavior or following only instincts and immediate desires are indispensable elements of autonomy. The threats to agency in this sense are manipulation and deception, such that a person's decision making processes and reasoning capabilities are hijacked by others.
- The conceptualization of freedom of choice concerns the availability of options in a choice environment (Nagenborg, 2014; Vugts et al., 2020). Freedom of an individual is most clearly violated when relevant options are taken away, however, it also includes that the person has practical, and not just a theoretical accessibility of relevant choices (Hansen & Jespersen, 2013). Freedom can be undermined through force, pressure and coercion, and also by making relevant choices impossible or costly (Brehm, 1966).
- The conceptualization of self-constitution is close to notion of authenticity and includes concerns dealing with a person's identity (Betzler, 2009; Levy, 2007). Vugts et al. (2020) argued that one of the deepest threats to self-constitution was indoctrination, making individuals endorse and values not truly their own. As examples, they discussed how marketing strategies could potentially induce perceptions of value other than the ones an individual had reasons to value. They also discussed that nudges in the public domain could potentially undermine autonomy in this sense if they were effective in shaping people's preferences and values without due reason on the part of the individual.

Vugts et al. argued for the importance of clarifying the sense in which autonomy was being interpreted, so as to understand how a nudge impacts the autonomy of an individual, and to avoid overlooking useful conceptualizations of autonomy. They argued that often nudges could undermine autonomy in one sense and strengthen it in another, and therefore it is important to make these distinctions explicit as well as make a careful normative judgment about which conceptualization is deemed more important in the context.

3. Research Methodology: A Thematic Analysis of Dark Patterns and Dark Strategies

In this section, we present a thematic analysis of dark patterns to identify the different conceptualizations of autonomy relevant to their normative evaluation. For this purpose, we systematically identified dark pattern taxonomies from literature and used them to develop an understanding of how dark patterns threaten users' autonomy. In the following subsections, we present how we selected the articles for this review, how we analyzed each dark pattern and how we grounded our analysis in theoretical perspectives on autonomy to identify the nature of the threat each dark pattern posed to users' autonomy.

3.1 Selection of Articles

We selected the articles for this analysis in two parts. Fig. 1 shows the process of selection of articles for this review.

1. We chose our initial selection of articles from Mathur et al. (2021). Mathur et al. had conducted a scoping review of dark patterns literature, in which they were interested in identifying shared attributes of various dark patterns reported in literature. They systematically identified publications that referenced dark pattern(s) or similar terms[3] on ACM Digital Library, arXiv and Google Scholar, and filtered papers that a) referenced dark patterns in the context of user interface design (excluding incidental references), and b) were published in an academic venue (with the exception of Brignull's unpublished work which was included in the analysis; Brignull, 2010). Their search yielded a dataset of 20 publications, out of which 9 proposed novel taxonomies of dark patterns. They also identified legislation and regulatory materials pertaining to dark patterns and their search yielded two documents containing taxonomies of dark patterns (National Commission on Informatics and Liberty [CNIL], 2020; Frobrukerrådet [Norwegian Consumer Council or NCC], 2018). We included these 11 taxonomies in our analysis, containing a total of 92 dark patterns. This dataset was compiled by Mathur et al. in Dec 2020.

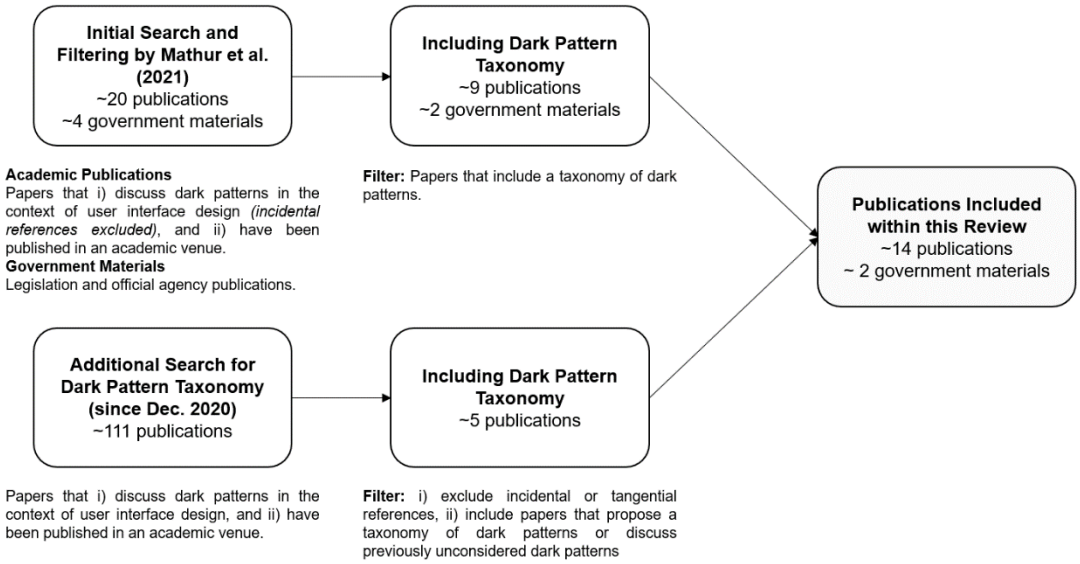

Fig. 1 Methodology for Selection of Articles

2. To expand our selection of articles beyond this time, we ran a similar search, following the search methodology of Mathur et al. We used 'dark pattern(s)' or similar search terms[1] to identify publications from the ACM Digital Library, arXiv and Google Scholar and filtered the search results to only include publications since Dec 2020. We then identified publications that a) discuss dark patterns in the context of user interface design, b) have been published in an academic venue (with the exception of a preprint by Wu et al. (2021), which was included in the analysis). This yielded 111 publications in total, many of which touched upon the subject of dark patterns tangentially. We then reviewed each of these 111 publications in full to identify those that either proposed a novel taxonomy of dark patterns or referred to dark patterns previously unconsidered in our dataset. This yielded a total of 5 additional publications which we included in our analysis. In total, we analyzed 151 dark patterns contained in 16 articles (14

[3] "dark pattern(s)," "anti-pattern(s)," "deceptive design pattern(s)," "FoMo design(s)," and "manipulative design pattern(s)

academic publications and 2 government materials), the details of which are presented in Table 1. Our dataset was compiled in Dec 2021.

Table 1. Selected Articles with Details of Dark Pattern Taxonomies

S. No.	Publication	Number of Dark Patterns	Context of the Publication
[1]	Brignull (2010)	12	Mixed Contexts
[2]	Conti and Sobiesk (2010)	11	Mixed Contexts
[3]	Zagal et al. (2013)	7	Games
[4]	Greenberg et al. (2014)	8	Proxemic Interactions
[5]	Bösch et al. (2016)	7	Privacy
[6]	Gray et al. (2018)	5	Mixed Contexts
[7]	NCC (2018)	5	Privacy
[8]	Lacey and Caudwell (2019)	1	Home Robots
[9]	Mathur et al. (2019)	12	E-Commerce
[10]	CNIL (2020)	18	Privacy
[11]	Gray et al. (2020)	6	Mixed Contexts
[12]	Bongard-Blanchy et al. (2021)	2	Mixed Contexts
[13]	Mhaidli and Schaub (2021)	5	XR Advertising
[14]	Petrovskaya and Zendle (2021)	35	Games
[15]	Westin and Chiasson (2021)	1	Social Media
[16]	Wu et al. (2021)	16	Livestream Shopping
	Total	**151**	

3.2 Corpus of Dark Patterns

The corpus of 151 dark patterns included designs from different contexts such as e-commerce, privacy, mobile games, influencer marketing and XR, and were created using different approaches. Brignull's (2010) taxonomy was created as an initial work of awareness. Since then, various authors have used systematic approaches to create dark pattern taxonomies in different contexts. Conti and Sobiesk (2010) created their taxonomy by conducting a study where 22 participants actively sought out malicious interface techniques on and off the desktop and solicited missing techniques from a group discussion at the Hackers of Planet Earth (HOPE) Conference. Zagal et al. (2013) created their taxonomy of dark patterns in games by soliciting design strategies from professional designers and through their own observations. Petrovskaya and Zendle (2021) conducted a survey of 1104 video game players to solicit examples of gaming transactions which were perceived to be misleading, aggressive or unfair. Greenberg et al. (2014) grounded the creation of their dark pattern taxonomy for proxemic interactions in thought exercises, using existing examples wherever possible. Bösch et al. (2016) identified malicious privacy behavior in the wild from a survey of popular websites and mobile applications and from public reports of privacy incidents. The NCC (2018) and CNIL (2020) reports were also concerned with dark patterns in privacy contexts. Gray et al. (2018) surveyed internet websites as well for their corpus generation of dark patterns. Mathur et al. (2019) created a taxonomy of dark patterns in e-commerce using data collected from an automated crawl of 11K shopping websites. Although they proposed 7 dark pattern categories and 15 subcategories, we found that certain subcategories within a single category were significantly different from each other, and therefore we chose to analyze them separately.

Gray et al. (2020) created a taxonomy of malicious designers through a content analysis of the posts on Reddit in "/r/assholedesign". Mhaidli and Schaub (2021) used a scenario reconstruction technique to identify potential manipulative advertising techniques in XR. Wu et al. (2021) created a taxonomy of malicious selling strategies in livestream shopping through an analysis of 40 publicly available livestream sessions on Chinese platforms Taobao and Douyin. Lacey and Caudwell (2019) and Westin and Chiasson (2021) focused their discussions on singular dark strategies (cuteness of robots and FoMo-centric design respectively). Bongard-Blanchy et al. (2021) was included in the analysis because the paper discussed two previously unconsidered dark patterns in our corpus: auto-play and bundled consent. Overall, the analyzed corpus of dark patterns covered a wide range of contexts.

3.3 Analysis

The 16 selected articles and the 151 dark patterns contained within them were analyzed following these steps:

1. Within each article, we first identified descriptions of each dark pattern to understand why a particular design pattern was proposed as 'dark'. Usually wherever taxonomies have been created, respective authors have specified in detail how a pattern works and articulated the ethical concerns which make it dark. We analyzed these definitions and created our interpretations of the 'darkness' of each dark pattern. For example, 'bait and switch', whose original description is 'you set out to do one thing, but a different, undesirable thing happens instead', was interpreted as 'information provided about action possibilities is deceptive'. The first step was to create such interpretations of the darkness of each of the 151 dark patterns. These interpretations were first created by the first author. At this stage, the first author excluded three dark patterns from Petrovskaya and Zendle (2021) from the analysis, and 148 dark patterns remained for analysis. The excluded patterns ('general existence of in-game currency', 'microtransactions as a business model', and 'dark interface design patterns') were found to be too general to be analyzed as persuasive design patterns. Then one undergraduate researcher was recruited to independently create these interpretations. The researcher had previous experience conducting user experience research on dark patterns and was generally familiar with the concept and the types of dark patterns on the web and in mobile apps. They read the original descriptions of the 148 dark patterns and independently created their own interpretations of the darkness of each pattern. The two researchers then came together to identify the similarities and differences in their interpretations. Wherever there was a difference in the understanding of why a certain pattern was 'dark', the two researchers came to an agreement through discussion. In some of these cases, one interpretation was chosen over the other, and in other cases, both researchers' interpretations were included as valid ethical concerns that contributed to the darkness of a pattern.
2. Second, a thematic analysis was conducted upon the interpretations of the corpus of dark patterns, to consolidate them into dark 'strategies'. The grouping of the patterns included a consideration of the dark aspects of the pattern and therefore, strategy labels include information about why a certain pattern is of ethical concern, such as 'deceptive information', 'misleading information', and 'information hiding'. This analysis was conducted by the first author and led to the identification of 25 dark strategies. It was observed from the interpretations of each dark pattern that some patterns raised multiple ethical concerns, i.e., there were multiple dark strategies at play. For example, 'address book leeching' uses both 'information hiding' (as it omits important information at the time of asking for contacts) and 'lack of

consent' (because it processes the information provided at a later stage without the user's consent at that stage). Therefore, several dark patterns were assigned into multiple dark strategies. Overall, the 148 dark patterns were assigned 232 times into 25 dark strategy groups.

3. The third step was to understand how the identified dark strategies posed a threat to autonomy. We first sought to observe if there was a similarity among strategies, such that some of them could be considered problematic in a similar way. We observed themes emerging from the dark strategies. For example, 'deceptive' and 'misleading' information seem problematic in a qualitatively similar sense as they prevent access to adequate information, and 'distraction' and 'time pressure' seem problematic because they both prevent users from putting an appropriate amount of thought into the decision. An inductive analysis of the 25 dark strategies led to the identification of seven underlying ethical considerations.
4. To situate the identified seven autonomy considerations within a theoretical framework, we sought to segregate them based on the 'sense' in which they threatened autonomy. A top down approach was taken to ground this part of the analysis in theoretical conceptualizations of autonomy (Section 2.5.2). We observed that five of the seven ethical considerations identified from the analysis (and all the dark strategies and patterns contained within them) reflected two notions of autonomy from Vugts et al. (2020): agency and freedom of choice. The remaining two ethical considerations pointed towards two additional notions of autonomy which have not yet explicitly emerged in nudge or persuasion literature: independence and control. These conceptualizations emerged from our data in an inductive fashion.

4. Results

The 148 dark patterns analyzed in this paper were consolidated into 25 dark strategies. The list of these 25 dark strategies and the dark patterns belonging to each strategy is provided in Table 2. Each dark pattern is numerically referenced to its source publication based on the serial numbers assigned to the publications in Table 1.

Table 2. Dark Strategies Identified from the Analysis of Dark Patterns

Dark Strategy	**Dark Patterns**
Deceptive Information	bait and switch, disguised ads, friend spam [1]; trick [2]; impersonation [3]; bait and switch [4]; immortal accounts [5]; sneaking [6]; scarcity, hidden subscription, social proof, urgency [9]; bait and change, camouflaged advertising, chameleon strategy, just you and us, wrong signal [10]; misrepresenting [11]; misleading experience marketing, emotional manipulation through hyper personalization, distorting reality [13]; useless products or duplicates, early access content, unrealistic product presentation, limited time offers [14]; fake scarcity, fake urgency, fake social proof, fake exclusive pricing, sophistry, disgracing others [16]
Information Hiding	friend spam, hidden costs, price comparison prevention, privacy zuckering, sneak into basket [1]; manipulating navigation, obfuscation, restricting functionality [2]; impersonation [3]; address book leeching, hidden legal stipulation [5]; interface interference, sneaking [6]; cuteness of robots [8]; hidden subscription [9]; comparison obfuscation, false continuity [10]; nickel and diming [11]; product does not incorporate everything the player believes, separate re-release of product, game unplayable without spending money, lack of information about product conditions, in-game currency disguises price, multiple currency types [14]; retaining customers, fuzzy targeting [16]
Misleading Information	hidden costs, trick questions [1]; confusion, interruption, manipulating navigation, trick [2]; pay to skip, pre-delivered content [3]; cuteness of robots [8]; trick questions [9]; safety blackmail, trick question, wrong signal [10]; two-faced, entrapping, nickel and diming, misrepresenting [11]; the nerf cycle, useless products or duplicates, product does not incorporate everything the player believes, early access content, payment in paid products [14]; visual misrepresentation [16]

Information Complexity	privacy zuckering [1]; confusion [2]; hidden legal stipulation, privacy zuckering [5]; two-faced [11]; multiple currency types [14]
Information Disclosure	hidden costs [1]; sneaking [6]; hidden costs [9]; nickel and diming [11]
Information Framing	framing [7]; improving experience, just you and us [10]; disgracing others [16]
Visual Bias	distraction, obfuscation [2]; interface interference [6]; ease [7]; visual interference [9]
Emotional Bias	shock [2]; cuteness of robots [8]; scarcity, social proof, urgency [9]; inducing artificial emotions in consumers, emotional manipulation through hyper personalization [13]; teasers, limited time offers [14]; playacting, retaining customers [16]
Distraction	misdirection [1]; distraction [2]; attention diversion [10]
Time Pressure	forced action [7]; scarcity, urgency [9]; last minute consent [10]
Targeting Vulnerability	targeting consumers when they are vulnerable [13]
Exploiting Trust	emotional manipulation through hyper personalization [13]
Obscuring Information	bad defaults [5]; default settings [7]; in-game currency disguises price, multiple currency types [14]
Forced Action	forced continuity [1]; coercion, forced work, interruption [2]; grinding, playing by appointment [3]; milk factor [4]; forced registration [5]; forced action [6]; forced action [7]; forced enrolment [9]; false continuity, impenetrable wall [10]; controlling [11]; bundled consent [12]; pay or grind, pay or wait, buying something not wanted, fixed purchase rates are unfair [14]; forced wholesale [16]
Lack of Options	restricting functionality [2]; captive audience [4]; immortal accounts [5]; controlling, entrapping [11]; monetization strategy changed, core aspects monetized, parts of game behind paywall, limited inventory space, game unplayable without spending money, overpricing, battle passes [14]
Asymmetric Effort	forced continuity, privacy zuckering, roach motel [1]; forced work [2]; bad defaults, privacy zuckering [5]; obstruction [6]; default settings, ease [7]; obstruction [9]; making it fastidious to adjust confidential settings, obfuscating settings [10]; entrapping [11]
Guilt / Shame	confirmshaming [1]; confirmshaming [9]; blaming the individual [10]; egoistic norms [16]
Fear	coercion [2]; safety blackmail [10]; egoistic norms [16]
Interruption	interruption [2]; nagging [6]; repetitive incentive [10]; controlling [11]; pay or wait, aggressive advertising [14]; nagging [16]
Social Obligation	social pyramid schemes [3]; FoMo-centric design [15]
Incentive Structure	monetized rivalries, pay to skip, playing by appointment, social pyramid schemes [3]; rewards and punishment [7]; advantage over other players, subscription features, boosts, pay to play competitively, game builds dependency on microtransactions, unfair matchups, free game experience underpowered, payment to avoid negative consequences [14]; forced subscription, forced endorsement [16]
Pressurizing	pressured selling [9]; pressured selling [16]
Implied Consent	sneak into basket [1]; attention grabber, personal information public [4]; interface interference, sneaking [6]; default settings [7]; pressured selling, sneak into basket [9]; default sharing [10]; automating the user [11]; auto-play [12]
Lack of Consent	forced continuity, friend spam [1]; trick, shock, exploiting errors [2]; impersonation [3]; disguised data collection, never forget, unintended relationships [4]; address book leeching, shadow user profiles [5]; automating the user [11]
Exploiting Obsession	grinding, monetized rivalries, pay to skip, playing by appointment [3]; auto-play [12]; pay or grind, game builds dependency on microtransactions [14]; FoMo-centric design [15]

From an analysis of these 25 dark strategies, we identified seven broad ethical considerations raised by this entire corpus of dark patterns. These seven considerations are grounded in four theoretical conceptualizations of autonomy. These are: *agency, freedom of choice, control and independence.* The results of this analysis are visualized in Fig. 2. We now discuss each of these conceptualizations and the ethical considerations contained within them, elaborating upon each notion using theoretical perspectives.

4.1 Agency

As discussed in Section 2.5.2, the conceptualization of agency concerns an individual's capacity to choose and decide (Vugts et al., 2020). Within our corpus, we discovered that several dark patterns threaten autonomy in this sense, by undermining or attacking the reasoning and evaluative aspect of decision making. These dark patterns either bypass the reflective aspect of decision making, or pervert it by introducing various kinds of biases.

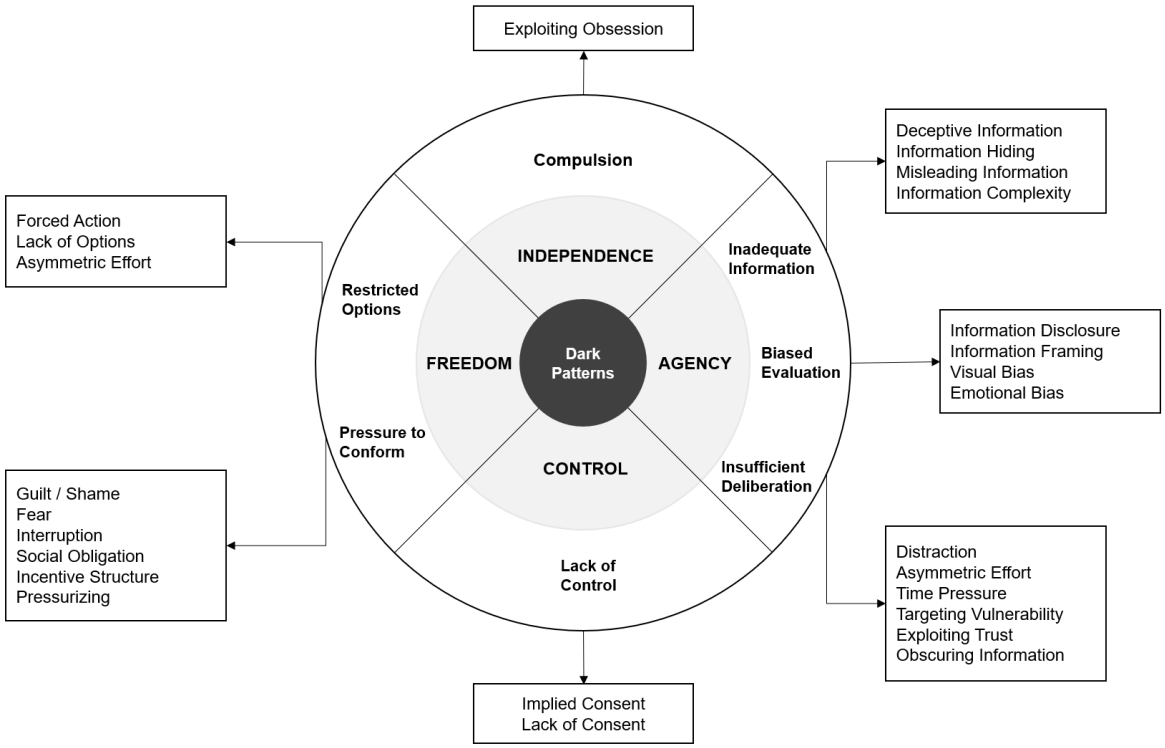

Fig. 2 Dark Patterns and User Autonomy – An Overview of Ethical Considerations

Our analysis reveals that dark patterns within this conceptualization can be synthesized into three broad ethical considerations, all of which are grounded within the notion of agency. These considerations are as follows:

1. **Inadequate information:** This consideration includes strategies such as 'deceptive information', 'information hiding', 'misleading information' and 'information complexity', which are designed to lead users into decisions that they potentially would not have made otherwise, or which they did not intend to make, had they been provided with relevant information. The essence of this approach is that users' decision making is grounded in inaccurate or incomplete beliefs, which can occur as a result of outrightly lying to them, strategically leading them to believe things which are not true, not revealing important information or revealing information in a way that it is incomprehensible. This theme includes dark patterns such as 'disguised ads', 'trick questions', 'hidden legal stipulations' and deceptive 'urgency' and 'scarcity' messages.
2. **Biased evaluation:** This consideration includes dark patterns which intervene within the process of decision making, and 'steer' or 'direct' it in an intended direction. In psychological literature, this is known as biasing the decision making of an individual. Within behavioral economics, the term bias originates from an understanding that human decision making deviates from the economic and

mathematical conception of rationality, and can be affected by seemingly irrelevant cues such as framing and anchors (Tversky & Kahneman, 1974; 1981). This is a result of the reliance of humans on automatic processes for decision making (Stanovich & West, 2000). However, this tendency can also be misused through dark patterns which bias users towards irrelevant or suboptimal choices. Within this theme, we have included dark strategies such as 'information framing', 'emotional bias' and 'visual bias', which trigger automatic tendencies in users that make them lean towards the choice intended by the dark pattern.

3. **Insufficient deliberation:** This consideration consists of dark patterns which attempt to undermine the time and attentional resources that a user devotes to a choice. This can be accomplished through strategies such as 'time pressure' and 'distraction', which make users become less involved in their decision making than they would like to be, or than the gravity of the choice demands. This situation also arises when dark patterns use 'asymmetric effort' to discourage users from sufficiently engaging with their choices, such as in privacy contexts (Bösch et al., 2016). Other ways to undermine users' autonomy in this way is to exploit a relationship of trust, through XR or deepfake technologies, or intervene into users' decision making in times of individual vulnerability (Mhaidli & Schaub, 2021).

4.2 Freedom of Choice

As highlighted in Section 2.5.2, the conceptualization of freedom of choice concerns the pragmatic availability of options in a choice environment (Brehm, 1966; Hansen & Jespersen, 2013; Nagenborg, 2014; Vugts et al., 2020). Dark patterns which threaten autonomy in this sense are those which reduce users' choices or limit the ways in which a user can interact with the system in accordance with their needs and preferences. Within our analysis, we identified several dark patterns and dark strategies which place barriers on choice, through restriction, manipulating access, or by applying pressure. These strategies can be placed into two broad considerations:

1. **Restricted options:** This approach includes designing functionality or choice architecture in a way such that users are forced to choose from a set of choices barring the most relevant, optimal or desirable ones. Dark patterns such as 'restricting functionality', 'forced continuity' and 'forced registration' fall within this approach. Sometimes these restrictions are integral to the functioning of the system, to gain meaningful access or to prevent anonymous misbehavior (Bösch et al., 2016). However, their darkness stems from the fact that they treat restricting users' choices as transactional elements within a commercial exchange, such as gaining free access to a website, without specifying or potentially negotiating the exact nature of the transaction. Often, these patterns might hide their transactional nature and (inaccurately) depict restrictions as an integral part of functionality, such as the 'false continuity' dark pattern (CNIL, 2020). Other times, restrictions pertain to the design of the product such that users have no alternate choices, such as changing product monetization strategy or overpricing (Petrovskaya & Zendle, 2021). Another strategy which intends to effectively restrict users' options is 'asymmetric effort'. This strategy is intended to reduce access to certain choices, keeping them theoretically available but manipulating their accessibility by making them unreasonably effortful to access. Patterns such as 'roach motel', 'obstruction' and 'default settings' fall within this strategy.
2. **Pressure to conform:** Dark patterns can also take the approach of applying pressure on users, to conform to certain choices against their best judgment or their preferences. This approach includes patterns such as 'confirmshaming' and 'nagging', which pressurize users into following the course of action intended

by the design. While these patterns do not utilize choice architecture or interface to manipulate choice, they reduce meaningful access to certain choices. For example, the 'social pyramid scheme' dark pattern is designed such that users are forced to 'give in' to joining the games that they have been invited to (Zagal et al., 2013). Even though they do not face any technical barriers to refusing participation in the game, the game creates a barrier in the form of social pressure, threatening users' freedom nonetheless.

4.3 Control

Control refers to an individual having the opportunity to decide on matters relevant to them, instead of having a decision made for them. The notion of control emerged from the data. In the context of dark patterns, it means that users have the choice to determine the actions of the system, including the initiation of certain actions which concern them. While in many ways this conceptualization is about having the freedom to choose, we find it useful to discuss it separately in the context of dark patterns, where it manifests in the form of non-transparent automatic behaviors of interactive systems. Loss of freedom is about the user 'having' to or being directly or indirectly forced to 'do' something. While devoid of freedom, the actions themselves are initiated by the user. When deprived of control, users are deprived of the opportunity to determine the course of action at all. For example, control is threatened when users' software updates automatically, or when information about them is collected automatically without their consent, seamlessly integrated into their browsing experience. Loss of control does not mean that users are asked to make compromises and choose amongst restricted options, but rather find themselves as passive recipients of a system's behaviors or its infrastructure.

Within this conceptualization, we found that lack of control can manifest using two design strategies: 'implied consent' and 'lack of consent'. Implied consent contains dark patterns which assume users' consent in matters which concern them and require consent. Also known as 'opt-out' mechanisms, the user is required to explicitly opt-out of the system's behavior. In the context of public display proxemics, Greenberg et al. (2014) discussed several dark patterns which assume implied consent, such as 'private information public' and 'attention grabber'. The darkness of implied consent stems from the concern that some matters should require explicit consent or opting in. Users should not face the unnecessary burden of opting out. Some patterns such as 'personal information public' are also dark because the damage to user might already be done before they opt out of situations, or users might never gather awareness of situations in which their consent has been assumed. The darkness of implied consent does not rely upon whether opting out is particularly difficult, only that the user faces the burden, or the responsibility of opting out to protect themselves. The second strategy which raises the same ethical concern about lack of control contains dark patterns which lack consent mechanisms altogether. This strategy includes patterns such as 'disguised data collection', 'unintended relationships', and 'impersonation'. The concern with 'lack of consent' strategy arises when the system engages in behaviors over which the user deserves a rightful control, such as disguised data collection, or contacting their friends on their behalf. However, the user is deprived of such control mechanisms.

4.4 Independence

The notion of independence is concerned with non-reliance. Dark patterns are often designed to foster reliance upon the system, a form of irresistibility which keeps the user coming back to engage with the system (Lewis, 2014). Even when certain patterns introduce pleasure or help in desirable forms of behavior change, they foster

the change so as to perpetually engage the user within the technological loop (Nagenborg, 2014). Within this conceptualization, we discovered several dark patterns which exploit users' compulsions and foster obsessive or addictive forms of engagement. These kinds of patterns are designed to engage the user through the simulation of short-lived bursts of pleasure, exploit their competitiveness and desire for virtual rewards. They foster technological reliance in a way such that users want to consciously or unconsciously keep coming back. Dark patterns which are designed to foster compulsion are 'FoMo-centric design' in social media (Westin & Chiasson, 2021), and several dark patterns in mobile games such as 'grinding', 'monetized rivalries', 'pay to skip' and 'playing by appointment' (Zagal et al., 2013). These patterns foster a sense of desire to engage, and in a way hide their own darkness. They rely on people's tendencies for limited self-control in the face of external seductions.

5. Discussion

In this paper, we have systematically analyzed 151 dark patterns to identify their autonomy centric ethical concerns and consolidated them into 25 dark strategies. We have further synthesized these strategies into seven ethical considerations grounded in four conceptualizations of autonomy. We now discuss the implications of this analysis for the normative evaluation of dark patterns and for policymaking in the domain.

5.1 Implications for Normative Evaluation of Dark Patterns and Persuasive Technology

This paper has attempted to contribute to the development of the autonomy perspective for the normative evaluation of dark patterns within information technologies. The conceptualizations and ethical considerations identified within this paper can help specify the nature of the concern associated with any dark pattern. Our analysis shows that different kinds of dark patterns raise qualitatively different ethical concerns from an autonomy perspective. Therefore, it may be difficult to evaluate all dark patterns using the same criteria. Mathur et al. (2021) argued that some dark patterns can remain problematic even when they are blatantly transparent, such as nagging, and that neither deception nor manipulation nor covertness can cover the dark aspects of each dark pattern. If we assume that not all persuasions are problematic, then there arises a need to identify what constitutes a dark intervention for users' autonomy. Persuasions can be legitimate for several reasons, such as when a persuader has altruistic intentions or when they have a legitimate transactional relationship with the individual. For example, marketing in itself is generally considered acceptable, because of a legitimate freedom of a business to attempt to persuade a consumer into considering their product. However, certain forms of marketing are still considered unethical, such as those which deceive, exaggerate or manipulate (Mhaidli & Schaub, 2021). There is an intuitive understanding that even within legitimate persuasive relationships, the approach to persuasion is crucial for its normative evaluation. For example, 'freedom' restrictions such as blocking access to a mobile game without payment might be considered relatively ethical, as argued by Zagal et al. (2013), instead of exploiting users' compulsive tendencies to keep them engaged within a game. Therefore, for normative the evaluation of any design pattern, it is necessary to evaluate whether it uses an approach which respects the dimension(s) of users' autonomy deemed valuable in that context.

Another implication of this analysis for the evaluation of design patterns is that sometimes designs will enhance autonomy in one sense, but undermine it in another. Consider the case of digital well-being apps (Sullivan & Reiner, 2019), which use various 'freedom' restrictions to help users reduce their own device usage. They can lock users out of certain apps, or even their phones, after a pre-specified usage for a pre-specified time period.

The user is deprived of 'control', such that they cannot override this system behavior once their phone has been locked. However, they help users exercise 'independence' from compulsion. At the same time, they also pose the risk of an increased reliance on the digital well-being app itself to maintain the desired independence from their smartphone. In examples like these, a careful balancing of different kinds of autonomy concerns is required, which in itself is a normative exercise. Similar arguments can be made for several m-health apps, which help users act in accordance with their goals (enhanced 'agency'), but pose the threat of reduced 'independence', as they can promote compulsive health behaviors and undermine intrinsic motivation such that users become less capable of practicing healthy behaviors in the long term without the aid of the apps (Jacobs, 2019).

In addition to the above, a clarification of the sense in which autonomy is infringed upon is also important to determine the best mitigative approach or the corrective action required to make such interventions more legitimate. For example, in the 'personal information public' dark pattern, the darkness of the pattern stems from the issue of 'control' or the fact that the system assumes implied consent (Greenberg et al., 2014). Therefore, it cannot be mitigated by merely making it easier to opt-out of this display (which is a mitigation through improving 'freedom'). This issue, to be completely resolved, requires consideration of control, and a recognition that the ethical issue is raised by the 'implied consent' strategy, and not just by the measure of effort required to opt-out.

5.2 Implications for Policy

5.2.1 The Role of Policy in the Protection of Autonomy

The subject matter for policy in the domain is to outline users' context specific rights applicable in a marketplace aimed at the protection of user or consumer autonomy. Traditionally, threats to autonomy were posed by domains such as marketing, and therefore, many countries have established elaborate consumer protection laws against marketing techniques which threaten autonomy, such as deceptive and misleading advertising (Petty, 1997). Petrovskaya and Zendle (2021) recently discussed the applicability of UK consumer protection frameworks (The Consumer Protection from Unfair Trading Regulations, 2008) for microtransactions within mobile games. They noted that several business and design practices pertaining to microtransactions may align with the definitions of deceptive, unfair and aggressive tactics in the marketplace as per the regulations. The European Union's General Data Protection Regulation (GDPR, 2018) in the privacy domain has also fundamentally outlined rights of the 'data subject' with respect to their data, thereby granting users legally enforceable 'control' over their data. A regulatory delineation of rights itself makes it possible for design patterns to be evaluated against a legal benchmark or a requirement. If there are legal frameworks to identify in what aspects users have the right to 'govern themselves', dark patterns in those contexts can be ethically delegitimized and legally protected against.

Even for mitigating approaches using policy, we argue that it is useful to identify the conceptualization in which a dark pattern threatens autonomy. Some forms of autonomy are more readily protected by regulation than others. For example, notions of freedom and control can be formulated as legal rights. The aspects of GDPR which mandate explicit consent for the collection and processing of personal data protect autonomy in the sense of control. To protect control, regulations need to outline the rights any individual has in a particular context. On the other hand, Utz et al. (2019) argued that while GDPR may have legally granted data control to data subjects, aspects of 'agency' still remained unaddressed within the regulation. This has led to the preponderance of click-wrap consent mechanisms in which users accept privacy terms and conditions without much knowledge or

deliberation. While 'control' requires the specification of rights to the minutest detail, aspects of agency need to be protected under the relatively broader protections from deception and manipulation, as is done by advertising laws of many countries. Lastly, 'independence' is relatively difficult to protect through regulation. Approaches which are intended to protect independence may themselves be seen as paternalistic, such as restrictions and prohibitions on social media or mobile games. Independence can however be salvaged through a combination of regulations and transparency and awareness campaigns, such that users act to protect their own independence, as well as do not end up viewing technology regulations as an assault upon their autonomy as consumers.

The role of policy in the case of autonomy protections is also to distinguish between autonomy as a condition, as felt by the user, and autonomy as an ideal, which can be construed by the law itself (Christman, 2020; Vugts et al., 2020). While individuals themselves may have a limited imagination for a state of autonomy, policy can pave the way for idealized conceptions of autonomy in many contexts where dark patterns and persuasive technologies are being deployed. In contexts beyond the marketplace, such as in medicine and workplaces, persuasive technologies are gaining traction but legal conceptions of autonomy remain underdeveloped in relation to information technologies (Wang et al., 2018; Wenker, 2022; Yamazaki et al., 2018). In these contexts, the role of policy is not just to protect existing notions of autonomy, but potentially to also create idealized interpretations of autonomy which technologies are required to respect, especially when these ideals serve other desirable outcomes such as citizens' health, happiness and well-being.

5.2.2 Protecting User Autonomy through Policy: The Case of Self-Tracking m-Health Technologies

Ethical concerns with any technology may be suitably mitigated by a wide range or even a combination of approaches, such as regulation, self-regulation, professional codes of commitment or public condemnation. We argue that different regulatory approaches are required to alleviate different kinds of autonomy concerns. Take the case of self-tracking m-health technologies. These technologies are designed to persuade and promote healthy behaviors, such as exercising, healthy eating, weight tracking, disease management, etc., and hence they can be classified as persuasive technologies. These persuasive technologies use a wide range of persuasive tactics, some of which may be dark patterns.

The value of autonomy is often invoked to articulate both the benefits and the ethical concerns about self-tracking. These benefits and concerns can be situated within the conceptualization framework of autonomy. The empowerment narrative around self-trackers promises enhanced 'agency' and 'control'. Self-trackers promise greater self-knowledge through numbers, convincing customers to gain control over their sleep, weight and health, facilitated by data (Sharon, 2017; Wieczorek et al., 2022). It is argued that self-tracking allows one to know rather than guess the state of their health (agency), and then adequately respond to the knowledge by doing something about it (control). However, the empowerment narrative is difficult to separate from perceptions of individual responsibility. For example, in the workplace, more and more employers are encouraging employees to adopt self-trackers (Chung et al., 2017). Insurance companies are offering discounts to customers who self-track (McFall, 2019). While such arrangements are typically initiated with voluntary user participation, the line between voluntary and compulsory participation often blurs (Ahuja & Kumar, 2020). This leads to 'freedom' concerns, where individuals do not have a real choice to deny the use of self-tracking technologies. Self-tracking may also undermine autonomy in the sense of 'independence'. Even though a tracking device may provide large quantities of information that was earlier unavailable to the senses, it may lead to a user becoming distant from their

intuitions about their health (Sharon, 2017). This may lead to a compulsive reliance on the tracker. In this sense, self-tracking may be 'empowering' (increased control) but not 'enabling' (decreased independence). Lastly, within m-health literature, critiques have also invoked autonomy in the sense of 'authenticity'. Data centric approaches to health are critiqued as unidirectional and reductive, preventing individuals from exploring alternate means of health management (Sharon, 2017; Wieczorek et al., 2022).

To address these concerns, we argue that policy solutions need to account for the sense in which autonomy is threatened. To mitigate 'freedom' concerns, 'restrictive approaches' may be suitable, which can dictate what kinds of incentivization for self-tracking may or may not be permissible in different contexts. For example, in medicine, regulation might outlaw it for insurance policy premiums to be linked to self-tracking data, or for insurance payouts to be dependent on this data. This is to ensure that users are not forced into the adoption of self-trackers and are not penalized for trivial mistakes. 'Independence' concerns might also require restrictive approaches such as restricting dark patterns that promote obsessive or compulsive behaviors (ex. streak features, timely logging, etc.). On the contrary, restrictions are less likely to alleviate concerns about 'authenticity'. These concerns may be better addressed by soft 'facilitative approaches', such as improving the societal health infrastructure, access to nutrition and healthcare. These approaches may support a wide range of health behaviors and help in developing intrinsic inclinations towards health. Lastly, even though empowerment through data is central to the promised benefits of self-tracking, robust 'standardization approaches' are required for data capture and data representation. The positive autonomy impact of self-tracking materializes only when it is based on accurate, standardized and actionable data, and therefore standardization approaches ensure that 'control' and 'agency' of users are truly enhanced by self-tracking technologies. An extension of this argument involves setting standards for technology representation in advertisements and promotions.

Through this case, we argue that the conceptualization framework of autonomy helps situate the impact of self-tracking m-health technologies in a normative background. It makes explicit the nuanced differences between each ethical concern and highlights ethical tradeoffs. It helps outline potential regulatory directions. It also helps identify the potential normative impact of each regulation, that is, whether a regulatory approach is truly capable of alleviating a particular ethical concern.

5.3 Limitations of this Paper

While our work has yielded important ethical considerations which underlie the literature on dark patterns, it also has certain limitations. Although it is expected that the taxonomy of strategies which we have created is non-exhaustive, we also believe that there are ethical considerations which have not surfaced in our analysis. For example, apart from compulsion, another consideration within the independence conceptualization is self-regulation, i.e., the ability to act in accordance with one's goals in an intrinsically motivated manner (Ryan & Deci, 2000). Persuasive technologies which seek to bring about desirable behavior change through extrinsic motivators, such as m-health and digital well-being apps, pose the threat of undermining long term intrinsic motivation (Jacobs, 2019). This threat has not been captured within dark patterns literature. None of the dark patterns which we analyzed touch upon this aspect, presumably because these approaches are not intuitively 'dark' and have therefore not received enough attention. Another conceptualization of autonomy which has not surfaced in our analysis is that of authenticity or self-constitution. There are potential examples of designs which pose a threat to users in this sense as well. For example, personalized content recommendation systems expose users to

a limited set of ideas based on their engagement potential, thereby limiting their view and perspective of the world around them (Pariser, 2011). However, this threat also did not surface in our analysis of dark patterns, since threats to authenticity are potentially more systemic, i.e., a result of dark infrastructure rather than dark patterns (Westin & Chiasson, 2019).

6. Conclusions

In this paper, we analyzed 151 dark patterns from 16 taxonomies to identify the normative considerations for the evaluation of dark patterns from a user autonomy perspective. We identified seven ethical considerations grounded in four conceptualizations of autonomy. We discussed the relevance of this analysis for the normative evaluation of dark patterns and argued that any mitigations and protections against such designs need to account for the sense in which autonomy is threatened. We also argued that policy approaches seeking to tackle the issue of dark patterns should be considerate of the exact nature of the threat to autonomy, as different regulations are more suited to protect certain kinds of autonomy than others, and certain forms of autonomy are more readily protected by regulations while others might require raising awareness and increasing transparency.

Overall, our paper makes a contribution towards the development of a normative lens of autonomy for the evaluation of dark patterns and persuasive technologies. It outlines several ethical considerations which till now remained implicit within autonomy-centric ethics discussions. It acknowledges the potential conflict between these conceptualizations and highlights the need for a balancing exercise in such contexts. We argued in the paper that autonomy is an inherently valuable normative consideration for the assessment of any forms of persuasive or behavior change interventions, and we hope that unpacking the multidimensional nature of considerations pertaining to autonomy can aid in the richer normative assessment of such interventions.

References

Ahuja, S., & Kumar, J. (2020). Surveillance based Persuasion: The Good, The Bad and The Ugly. 4th International Conference on Computer-Human Interaction Research and Applications (CHIRA '20), Budapest, Hungary. https://doi.org/10.5220/0010121401200127

André, Q., Carmon, Z., Wertenbroch, K., Crum, A., Frank, D., Goldstein, W., Huber, J., van Boven, L., Weber, B., & Yang, H. (2018). Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data. *Customer Needs and Solutions, 5*, 28–37. https://doi.org/10.1007/s40547-017-0085-8

Berdichevsky, D., & Neuenschwander, E. (1999). Toward an ethics of persuasive technology. *Communications of the ACM, 42*(5), 51–58. https://doi.org/10.1145/301353.301410

Betzler, M. (2009). Authenticity and self-governance. In *Emotions, ethics, and authenticity*, ed. Mikko Salmela and Verena Mayer, 51–68. John Benjamins Publishing Company.

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. ACM Designing Interactive Systems Conference (DIS '21), Virtual Event, USA. 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, 4*, 237-254. https://doi.org/10.1515/popets-2016-0038

Botti, S., & McGill, A. L. (2011). The locus of choice: personal causality and satisfaction with hedonic and utilitarian decisions. *Journal of Consumer Research, 37*(6),1065–1078. https://doi.org/10.1086/656570

Brehm, J. W. (1966). *A theory of psychological reactance.* Academic Press.

Brey, P. (2005). Freedom and Privacy in Ambient Intelligence. *Ethics & Information Technology, 7*, 157–166. https://doi.org/10.1007/s10676-006-0005-3

Brignull, H. (2010). What are dark patterns?. Retrieved March 22, 2022, from https://www.darkpatterns.org/

Buss, S., & Westlund, A. (2018). *Personal Autonomy*. The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/spr2018/entries/personal-autonomy/

California Secretary of State. (2020). *Qualified Statewide Ballot Measures.* Retrieved March 22, 2022, from https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

Christman, J. (2020). *Autonomy in Moral and Political Philosophy*. The Stanford Encyclopedia of Philosophy (Fall 2020 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/

Chung, C., Gorm, N., Shklovski, I. A., & Munson, S. 2017. Finding the Right Fit: Understanding Health Tracking in Workplace Wellness Programs. ACM CHI Conference on Human Factors in Computing Systems (CHI '17), Denver, Colorado, USA. https://doi.org/10.1145/3025453.3025510

Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion.* Collins.

Conti, G., & Sobiesk, E. (2010). Malicious Interface Design: Exploiting the User. 19th International Conference on World Wide Web (WWW '10), Raleigh, North Carolina, USA. https: //doi.org/10.1145/1772690.1772719

Cortiñas, M., Elorz, M., & Mugica, J. (2008). The use of loyalty-cards databases: Differences in regular price and discount sensitivity in the brand choice decision between card and non-card holders. *Journal of Retailing and Consumer Services. 15*(1). 52-62. https://doi.org/10.1016/j.jretconser.2007.03.006

Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of Goal Pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry, 11*(4), 227–268. http://doi.org/10.1207/s15327965pli1104_01

Dhar, R., & Wertenbroch, K. (2012). Self-signaling and the costs and benefits of temptation in consumer choice. *Journal of Marketing Research, 49*(1), 15–25. https://doi.org/10.1509/jmr.10.0490

Erler, A. (2011). Does Memory Modification Threaten Our Authenticity?. *Neuroethics, 4*(3), 235-249. https://doi.org/10.1007/s12152-010-9090-4

Fogg, B.J. (2002). *Persuasive technology: using computers to change what we think and do.* Morgan Kaufmann Publishers.

Frankfurt, H. G. (1971). Freedom of the will and the concept of a person. *Journal of Philosophy, 68*(1), 5–20. https://doi.org/10.2307/2024717

Friedrich, O., Racine, E., Steinert, S., Pömsl, J., & Jox, R. J. (2018). An analysis of the impact of brain-computer interfaces on autonomy. *Neuroethics, 14*, 17-29. https://doi.org/10.1007/s12152-018-9364-9

Friestad, M., & Wright, P. (1994). The Persuasion Knowledge Model: How People Cope with Persuasion Attempts. *Journal of Consumer Research, 21*(1), 1–31. http://www.jstor.org/stable/2489738

Frischmann, B., & Selinger, E. (2018). *Re-Engineering Humanity.* Cambridge University Press.

Frobrukerrådet [Norwegian Consumer Council or NCC]. (2018, June 27). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy.* Retrieved March 22, 2022, from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

General Data Protection Regulation (GDPR). (2018). https://gdpr.eu/tag/gdpr/

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A.L. (2018). The Dark (Patterns) Side of UX Design. CHI Conference on Human Factors in Computing Systems (CHI '18), Montreal, QC, Canada. https://doi.org/10.1145/3173574.3174108

Gray, C. M., Chivukula, S. S., & Lee, A. (2020). What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. ACM Designing Interactive Systems Conference (DIS '20), Eindhoven, Netherlands. https://doi.org/10.1145/3357236.3395486

Greenberg, G., Boring, S., Vermeulen, J., & Dostal, J. (2014). Dark Patterns in Proxemic Interactions: A Critical Perspective. ACM Designing Interactive Systems Conference (DIS '14), Vancouver, BC, Canada. https://doi.org/10.1145/2598510.2598541

Herman, E. S., & Chomsky, N. (1988). *Manufacturing Consent: The Political Economy of the Mass Media.* Pantheon Books.

Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy. *European Journal of Risk Regulation, 1*, 3-28. https://ssrn.com/abstract=2555337

Jacobs, N. (2019). Two ethical concerns about the use of persuasive technology for vulnerable people. *Bioethics, 34*(5), 519-526. https://doi.org/10.1111/bioe.12683

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47*(2), 263-292. https://doi.org/10.2307/1914185

Krisam, C., Dietmann, H., Volkamer, M., & Kulyk, O. (2021). Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. European Symposium on Usable Security (EuroUSEC '21), Karlsruhe, Germany. https://doi.org/10.1145/3481357.3481516

Lacey, C., & Caudwell, C. (2019). Cuteness as a 'Dark Pattern' in Home Robots. 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI '19), Daegu, South Korea. https://doi.org/10.1109/HRI.2019.8673274

Langer, E. J., & Rodin, J. (1976). The effects of choice and enhanced personal responsibility for the aged: a field experiment in an institutional setting. *Journal of Personality and Social Psychology, 34*(2), 191–198. https://doi.org/10.1037/0022-3514.34.2.191

Lasswell, H. (1927). The Theory of Political Propaganda. *American Political Science Review, 21*(3), 627-631. https://doi.org/10.2307/1945515

Levy, N. (2007). *Neuroethics.* Cambridge University Press.

Lewis, C. (2014*). Irresistible Apps: Motivational Design Patterns for Apps, Games, and Web-based Communities*. Apress.

Lindstrom, M. (2012). *Buyology: How Everything We Believe About Why We Buy is Wrong.* Random House.

Maier, M. A., & Harr, R. (2020). Dark Design Patterns: An End-User Perspective. *Human Technology, 16*(2), 170-199. https://doi.org/10.17011/ht/urn.202008245641

Mackenzie, C., & Stoljar, N. (Eds.), (2000). *Relational autonomy: Feminist perspectives on autonomy, agency, and the social self.* Oxford University Press.

Mackenzie, C., & Walker, M. (2015). Neurotechnologies, Personal Identity, and the Ethics of Authenticity. In *Handbook of Neuroethics*, ed. Jens Clausen and Neil Levy, 373-392. Springer Netherlands.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human Computer Interaction, 3* (CSCW), 1-32. https://doi.org/10.1145/3359183

Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What Makes a Dark Pattern...Dark?: Design Attributes, Normative Considerations, and Measurement Methods. ACM CHI Conference on Human Factors in Computing Systems (CHI '21), Yokohama, Japan. https://doi.org/10.1145/3411764.3445610

McFall, L. (2019). Personalizing solidarity? The role of self-tracking in health insurance pricing. *Economy and Society, 48*(1), 52-76. https://doi.org/10.1080/03085147.2019.1570707

Mhaidli, A., & Schaub, F. (2021). Identifying Manipulative Advertising Techniques in XR Through Scenario Construction. CHI Conference on Human Factors in Computing Systems (CHI '21), Yokohama, Japan. https://doi.org/10.1145/3411764.3445253

Milliman, R. E. (1982). Using Background Music to Affect the Behavior of Supermarket Shoppers. *Journal of Marketing, 46*(3), 86–91. https://doi.org/10.1177/002224298204600313

Nagenborg, M. (2014). Surveillance and persuasion. *Ethics and Information Technology, 16*, 43–49. https://doi.org/10.1007/s10676-014-9339-4

National Commission on Informatics and Liberty (CNIL). (2020). *Shaping Choices in the Digital World.* Retrieved March 23, 2022, from https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Books.

Passingham, J. (1998). Grocery Retailing and the Loyalty Card. *Market Research Society Journal*, *40*(1), 1–8. https://doi.org/10.1177/147078539804000105

Petrovskaya, E., & Zendle, D. (2021). Predatory Monetisation? A Categorisation of Unfair, Misleading and Aggressive Monetisation Techniques in Digital Games from the Player Perspective. *Journal of Business Ethics.* https://doi.org/10.1007/s10551-021-04970-6

Petty, R. D. (1997). Advertising Law in the United States and European Union. *Journal of Public Policy & Marketing*, *16*(1), 2–13. https://doi.org/10.1177%2F074391569701600102

Pugh, J., Maslen, H., & Savalescu, J. (2017). Deep Brain Stimulation, Authenticity and Value. *Cambridge Quarterly of Healthcare Ethics*, *26*(4), 640-657. https://doi.org/10.1017/S0963180117000147

Roskies, A. (2021). *Neuroethics.* The Stanford Encyclopedia of Philosophy (Spring 2021 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/spr2021/entries/neuroethics/

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68

Saghai, Y. (2013). Salvaging the concept of nudge. *Journal of Medical Ethics*, *39*, 487-493. http://dx.doi.org/10.1136/medethics-2012-100727

Schechtman, M. (2014). *Staying Alive: Personal Identity, Practical Concerns, and the Unity of a Life.* Oxford University Press.

Schüll, N. D. (2012). *Addiction by Design: Machine Gambling in Las Vegas.* Princeton University Press.

Sharon, T. (2017). Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. *Philosophy & Technology*, *30*, 93–121. https://doi.org/10.1007/s13347-016-0215-5

Spahn, A. (2012). And Lead Us (Not) into Persuasion…? Persuasive Technology and the Ethics of Communication. Science and Engineering Ethics, 18, 633–650. https://doi.org/10.1007/s11948-011-9278-y

Stanovich, K. E., West, R. F. (2000). Individual difference in reasoning: implications for the rationality debate?. *Behavioral and Brain Sciences*, *23*(5), 645–726. https://doi.org/10.1017/s0140525x00003435

Steindl, C., Jonas, E., Sittenthaler, S., Traut-Mattausch, E., & Greenberg, J. (2015). Understanding psychological reactance. *Zeitschrift für Psychologie 223*(4), 205–214. http://doi.org/10.1027/2151-2604/a000222

Sullivan, L. S., & Reiner, P. (2019). Digital Wellness and Persuasive Technologies. *Philosophy & Technology*, *34*, 413-424. https://doi.org/10.1007/s13347-019-00376-5

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, 8(2). https://doi.org/10.14763/2019.2.1410

Thaler, R. H., & Sunstein, C.R. (2008). *Nudge.* Yale University Press.

The Consumer Protection from Unfair Trading Regulations 2008. (2008). Queen's Printer of Acts of Parliament. Retrieved March 23, 2022, from https://www.legislation.gov.uk/uksi/2008/1277/contents/made

Urban, T., Degeling, M., Holz, T., & Pohlmann, N. (2020). Beyond the front page: measuring third party dynamics in the field. *Proceedings of The Web Conference 2020.* http://doi.org/10.1145/3366423.3380203

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. ACM SIGSAC Conference on Computer and Communications Security (CCS '19), London, United Kingdom. https://doi.org/10.1145/3319535.3354212

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science, 185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4481), 453-458. https://doi.org/10.1126/science.7455683

Verbeek, P. P. (2009). Ambient Intelligence and Persuasive Technology: The Blurring Boundaries Between Human and Technology. *Nanoethics, 3*(3), 231–242. https://doi.org/10.1007/s11569-009-0077-8

von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. Princeton University Press.

Vugts, A., van den Hoven, M., de Vet, E., & Verweij, M.F. (2020). How autonomy is understood in discussions on the ethics of nudging. *Behavioural Public Policy, 4*(1), 108 - 123. https://doi.org/10.1017/bpp.2018.5

Wang, Y., Wu, L., Lange, J., Fadhil, A., & Reiterer, H. (2018). Persuasive Technology in Reducing Prolonged Sedentary Behavior at Work: A Systematic Review. *Smart Health, 7-8*, 19-30. https://doi.org/10.1016/j.smhl.2018.05.002

Warner, M., & Fischer, D. (2019, April 09). Senators Introduce Bipartisan Legislation to Ban Manipulative "Dark Patterns". Retrieved March 22, 2022, from https://www.fischer.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns

Waters, T. E. A., & Fivush, R. (2014). Relations Between Narrative Coherence, Identity, and Psychological Well-Being in Emerging Adulthood. *Journal of Personality, 83*(4): 441–451. https://doi.org/10.1111/jopy.12120

Wenker, K. (2022). A Systematic Literature Review on Persuasive Technology at the Workplace. *ArXiv*. https://doi.org/10.48550/arXiv.2201.00329

Westin, F., & Chiasson, S. (2021). "It's So Difficult to Sever that Connection": The Role of FoMO in Users' Reluctant Privacy Behaviours. CHI Conference on Human Factors in Computing Systems (CHI '21), Yokohama, Japan. https://doi.org/10.1145/3411764.3445104

Wieczorek, M., O'Brolchain, F., Saghai, Y., & Gordijn, B. (2022). The ethics of self-tracking. A comprehensive review of the literature. *Ethics & Behavior*. https://doi.org/10.1080/10508422.2022.2082969

Woodward, J. D. (1997). Biometrics: privacy's foe or privacy's friend?. *Proceedings of the IEEE, 85*(9), 1480-1492. https://doi.org/10.1109/5.628723

Wu, Q., Sang, Y., Wang, D., & Lu, Z. (2021). Malicious Selling Strategies in Livestream Shopping: A Case Study of Alibaba's Taobao and ByteDance's Douyin. *ArXiv*. https://doi.org/10.48550/arXiv.2111.10491

Yamazaki, R., Nishio, S., Ishiguro, H., & Kase, H. (2018). Use of Robotic Media as Persuasive Technology and Its Ethical Implications in Care Settings. *Journal of Philosophy and Ethics in Health Care and Medicine, 12*.

Zagal, J.P., Björk, S., & Lewis, C. (2013). Dark patterns in the design of games. Foundations of Digital Games (FDG '13). Society for the Advancement of the Science of Digital Games, Santa Cruz, CA.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.