Manipulation through Design: A Law and Economics Analysis of EU Dark Patterns Regulation

Alexander Egberts, M.A.

European Master of Law and Economics

LUMSA University Rome
Department of Law, Economics, Politics and Modern Languages

Submitted on the 11th of August 2021

Supervised by Professor Dr. Fabiana Di Porto

Keywords: Dark Patterns, Sludging, Legislative Costs, EU Regulation, Study Design

JEL Classifications: K24; L51; D91

Abstract

Dark Patterns are ubiquitous: deliberate choices in website- or app-design that exploit unobservant or irrational behavior of users, tricking them into reaching agreements or consenting with settings that are not in line with the users' actual preferences. This umbrella term covers a broad variety of different online choice architecture manipulations, which differ in their effectiveness or conspicuousness, but all share one core mechanic: abusing heuristics to influence online behavior.

Even though Dark Patterns have not yet been explicitly targeted by EU regulation, they are partially covered by the existent body of EU legislation. This thesis identifies to which extent the consumer and data protection acquis already provides legal boundaries for specific Dark Patterns. It explains why (further) Dark Patterns regulation is desirable from a law and economics perspective and develops specific proposals as to how such interventions should be designed: Legislation should add on to existing regulatory mechanisms by amending them with concrete rules that take behavioral insights into account. Furthermore, the thesis explains why regulators should take a two-step approach to regulation, first establishing information disclosure duties before determining the level of optimal intervention.

Finally, as evidence-based regulation is identified to be vital to prevent overregulation, the thesis proposes a risk-based assessment to measure the effect of Dark Patterns. It suggests the design of an experimental study to identify Dark Pattern influence in the cookie banner context. It allows to both test existing hypotheses and explore new explanatory approaches to how Dark Patterns influence behavior.

Table of Contents

A. Introduction 1

B. Understanding Dark Patterns 3

I. Taxonomies, Attributes and Definitions 3

II. Occurrence in the Field 5

III. Effect on Behavior 6

1. Behavioral Economics and “Sludging” 7

2. Empirical Evidence 9

C. Regulating Dark Patterns 10

I. Why Regulate Dark Patterns 10

1. Economic Case for Regulation 10

2. Elevated Risk in the Digital Space 13

3. No Market Solution 14

II. Dark Patterns under European Legislation 16

1. Existing EU Regulation 16

a) Consumer Rights Directive 16

b) Unfair Commercial Practices Directive 17

c) GDPR 20

(i) Art. 4 (11): Consent Criteria 20

(ii) Art. 25: Data Protection by Design 22

2. Imminent EU Regulation 23

3. Regulatory Gaps 24

III. How to Regulate Dark Patterns 25

1. Focusing on Manipulation 25

2. Identifying the Necessary Scope of Intervention 26

a) Benefits: A Risk-Based-Approach 27

b) Costs and How to Reduce Them 29

3. Suggestions for Regulatory Intervention 31
a) Two-Step Approach 31
b) Rules instead of Standards 31
c) Targeted Readjustments 33
D. Testing Dark Patterns: A Study Design 34
I. Value Added through the Study 35
II. Cookie Banners as an Experimental Setting 35
III. Hypotheses 38
1. Influence on Cookie Choice 38
2. A New Hypothesis: Familiarity as Factor 39
3. Testing Previous Results: Education as a Factor 41
IV. Method 41
1. Study Design 41
2. Choosing Treatments 44
3. Participants 44
4. Analysis 45
V. Limitations 45
E. Conclusion 46

Appendix 1 – Table: Dark Patterns, their Attributes and Biases 49
Appendix 2 – Descriptive Analysis of Dark Pattern Prevalence 51
Appendix 3 – Table: Dummy Dataset and Website Screenshots 53

Page intentionally left blank.

A. Introduction

Although the term "Dark Patterns" may appear new to some readers, it describes a phenomenon that most certainly every internet user will have witnessed at some point: Design choices on websites or mobile applications regularly aim to steer users towards specific actions. If those actions go against the users' assumed preferences and instead are beneficial to the architects of such online environments, they are described as Dark (design) Patterns. They come in many shapes and sizes: highlighting the (allegedly) limited amount of hotel rooms left; deliberately burying unsubscribe-options in deep sub-menus; or merely designing one button to look more inviting than another. These and many more designs of online choice architectures are comprised by the concept of Dark Patterns.

The topic recently received growing attention from media outlets, political parties, academic scholars, and public agencies – often culminating in calls for regulatory intervention. However, unlike in the U.S.,[1] the phenomenon has not yet been explicitly addressed by the European legislator. This raises several questions: Do Dark Patterns justify regulatory intervention? To which extent are they already covered by existent European legislation? What should a potential Dark Patterns regulation look like? Using both legal and economic analytical approaches, this thesis aims to respond to those questions. It discusses whether and to which extent (further) regulation is needed from an EU perspective. As a result, concrete proposals for action, which lawmakers may possibly refer to, will be suggested.

Insights from behavioral law and economics will play an important role in doing so. Since cognitive biases and heuristics are the gateway through which Dark Patterns aim to

[1] While an attempt of the federal legislator to prohibit manipulative designs has failed with the termination of the previous legislative period (DETOUR Act, 2019), Californian state law explicitly voids agreements made "through use of dark patterns" (CCPA, 2018).

influence users' behavior, they also present the subject matter at which the law should intervene, given there is a need for regulation. Through this, an underlying normative question becomes apparent: How much manipulation is too much manipulation? This question cannot be effectively addressed without examining the impact that Dark Patterns have on human behavior. Hence, any approach to regulation will need to be based on experimental insights about the effectiveness of different patterns. To contribute to this requirement, this work proposes the design of an experimental study on the effectiveness of Dark Patterns in the context of consent management platforms (CMPs), commonly referred to as cookie banners.

Due to the limited scope of this thesis, some aspects of the topic cannot be addressed: the possibility of responding to Dark Patterns through personalized law and, the question to which extent specific Dark Patterns qualify as behavioral market failures as well as a detailed comparison to regulatory approaches in the U.S. are not discussed herein.

Going on, this thesis will be structured in four parts: First, the phenomenon of Dark Patterns will be presented, depicting the current stage of discussion regarding their prevalence and effectiveness (B.). Then, it will be examined to which extent the current EU framework captures the phenomenon, whether further regulation is justified and how such regulation could look like (C.). Finally, the design of an experimental study to further research the influence of Dark Patterns will be proposed (D.), before the thesis is concluded (E.).

B. Understanding Dark Patterns

To enable a legal and economic analysis of Dark Patterns, a more detailed comprehension of the subject is required. Subsequently, the admittedly broad terminology is defined more precisely (I.), and the frequency and contexts of their deployment is discussed (II.) based on previous scholarship. Then, the behavioral insights on which their functionality is built are explained (III.).

I. Taxonomies, Attributes and Definitions

The term "Dark Patterns" was initially introduced by the British User Experience-designer Harry Brignull in 2010 (Brignull, 2010). As the examples given in the introduction illustrate, the phrase constitutes an umbrella term for a multitude of different design patterns, all varying in their mode of operation and conspicuousness. Resulting from this variety, a myriad of taxonomies has been proposed.[2] Instead of providing additional specific examples at this point, an overview of the Dark Patterns most frequently identified in those taxonomies is compiled in Appendix 1.

The large scope of observed patterns led to several suggestions on how to congregate taxonomies into more comprehensible categories (Gray, et al., 2018, p. 4; Mathur, et al., 2019, p. 12; Luguri & Strahilevitz, 2021, p. 53). Thinking in terms of categories might be helpful for gaining a clearer overview. However, the clear-cut term of "categories" indicates a degree of distinctiveness which does not reflect reality: In individual cases, Dark Patterns can vary greatly in their specific design or intensity, which renders the assignment of categories meaningless if those differences are not accounted for.

[2] Mathur, et al. (2021, p. 9-11) provide an overview of previous taxonomies.

Instead, it is more accurate to think of Dark Patterns as proprietors of certain attributes, which do not necessarily exclude each other, as initially proposed by Mathur, et al. (2021, p. 8). Expanding on their initial suggestion, five versatile attributes can be determined:

(1) Information Hiding or Decision Space: Some patterns may disturb the flow of information (e.g., by ambiguous phrasing or withholding information); others may transfer information adequately, but instead manipulate the decision space (e.g., by making options harder to select). The differentiation may depend on intensity.
(2) Covert: Some patterns operate secretly and try to hide their influence, e.g., e-commerce websites initially suggest overpriced goods to frame other products as better deals. Other patterns are more noticeable, e.g., "Nagging"-patterns, repeatedly asking the same question.
(3) Deceptive: Some patterns actively convey false information or aim to create misconceptions, e.g., by including countdown-timers without an actual time constraint.
(4) Obstructive: Some patterns obstruct the execution of users' decisions, e.g., by making it harder to select a specific option.
(5) Pressuring: Some patterns may exert emotional or social pressure on the user to guide him towards a specific action. E.g., by framing options as being unreasonable ("*No, I don't like saving money"*).

As the term Dark Patterns covers a broad range of observations, no universal definition has yet been established: A recent literature review identified fifteen academic publications and four governmental materials published on the topic, each providing slightly differing taxonomies and definitions (Mathur, et al., 2021, pp. 2-11).

When the term was originally introduced in a blog post in 2010, it was described as "bad design patterns [which have] been crafted with […] a solid understanding of human

psychology, to trick users into doing things they wouldn't otherwise have done" (Brignull, 2010). With this hint to human psychology, the initially proposed definition already contained the common substantive core on which most[3] publications on the topic agree: Dark Patterns exploit cognitive biases and behavioral heuristics to steer users towards making choices which contradict their preference-based, rational decision making.

II. Occurrence in the Field

While presumably everyone will have encountered a Dark Pattern at some point, the question arises as to how common the phenomenon really is. Several empirical studies have been conducted to identify which Dark Patterns are employed in which contexts. Their results are briefly presented subsequently.

E-Commerce and Apps

In a 2019 study, Mathur et al. automatically crawled 11,286 shopping websites for the use of text-based Dark Patterns and manually inspected the results. They identified 1.818 instances of Dark Patterns on 1.254 of the websites (11,1%). The use of Dark Patterns was more prevalent on more frequently visited websites. Most identified patterns had Covert, Deceptive or Information Hiding attributes. While this study provides very valuable insights, it presumably only begins to describe the actual prevalence of Dark Patterns, since they are often graphics-based and therefore not included in this study. Moser, et al. (2019, p. 1-2) manually conducted a systematic analysis of 200 U.S. e-commerce websites and identified 64 different design elements that encourage impulse buying. Each website provided at least one of those elements. Finally, Di Geronimo et al.

[3] 14 out of 19 contributions identify this as a core mechanism of Dark Patterns (Mathur, et al., 2021, pp. 9-11).

(2020, p. 6-8) manually reviewed the 30 most downloaded apps in each of the Google Play-store's 8 categories. They found that 95% of the investigated apps utilize at least one type of Dark Pattern, while the on average, 7 patterns were used per app.

Cookie Banners

Utz, et al., (2019, p. 2-4) analyzed the use of Dark Patterns in CMPs by manually inspecting banners from 1000 websites, randomly selected from the 5,087 most popular European websites. They found that 57.4% of them used manipulative designs to induce privacy invasive choices. A similar study was conducted by Nouwens, et al. (2020, p. 6-9) who analyzed 680 variations of cookie banners in the UK and found that 56.2% of the banners included "Bad Default"-patterns. Soe et al. (2020, p. 6-8) manually analyzed 300 CMPs from English and Scandinavian news websites and found Dark Patterns in 297 of them.

Similarities

Particularly large number of Dark Patterns can be found in the context of cookie banners and e-commerce. While the specific patterns and their frequency of deployment differ, the contexts share a structural similarity: The decision space is unilaterally established by the website operator. It does not provide room for an individual eye-to-eye agreement but leaves the user with a take-it-or-leave-it choice. This resembles consumer transaction scenarios. Ultimately, it can be noted that Dark Patterns are most prevalent in unilaterally shaped decision-making structures, which are akin to consumer transactions.

III. Effect on Behavior

This prompts the question as to why this phenomenon occurs so frequently. The most intuitive explanation for the rationale behind Dark Pattern deployment is as simple as it is obvious: they work. (Web-)Designers implement Dark Patterns to influence the

behavior of users. This suspected effect can be explained with insights from behavioral economics (1.). To some extent, these conjectures have already been backed with experimental data (2.).

1. Behavioral Economics and "Sludging"

Economic models have long assumed market participants to be rational actors, adjusting their behavior towards maximizing their own utility. Empirical studies in the field of cognitive psychology have shattered this assumption and revealed recurring irrationalities in our thoughts and actions: Human behavior systematically deviates from the homo economicus-model. Famously, Kahneman (2011) discussed two different cognitive processes: one unconscious, automatic and nearly effortless ("system 1") – another deliberate, controlled, and effortful ("system 2"). While system 2-thinking largely resembles the homo economicus-model of mainstream economics, system 1-thinking enables quick decision-making by relying on cognitive shortcuts. These so-called heuristics are evolutionarily justified and provide an essential support in our everyday life. However, decisions based on heuristics may yield different outcomes then those resulting from deliberate thinking. These recurring divergences are referred to as biases (Tversky & Kahneman, 1974, p. 1124). Behavioral economists study these systematic deviations to obtain a more accurate understanding about how humans behave.

This paradigm shift in predicting human behavior turned out to be a powerful tool for regulators: By designing choice architectures based on behavioral insights, citizens could be "nudged" into making decisions that are more consistent with their assumed long-term preferences while using a less intrusive, more choice preserving way and without de facto restricting their individual autonomy (Thaler & Sunstein, 2008, pp. 4-8).[4] However, not

[4] It should be mentioned that this proposal has also been met with substantial criticism from early on, see Wilkinson (2013) and Alemanno & Spina (2014).

everybody used this new tool with good intentions. From early on, businesses have tried to abuse behavioral insights to increase revenue by exploiting consumers' biases, e.g., through decreasing risk-perception in tobacco markets (Hanson & Kysar, 1999, pp. 1466-1468). More recently, this practice of deliberately manipulating behavior by abusing cognitive biases has been dubbed as "sludging" (Thaler, 2018, p. 431).

Dark Patterns transport "sludging" to the digital space, by designing online choice architectures to obscure information or abuse consumers' "system 1"-thinking. This steers consumers towards specific decisions, which are – unlike "nudged" decisions – not in line with their individual preferences. Instead, they serve the interests of the website operators. Thus, they defy consumer preferences and influence behavior in favor of decision spaces' architects, by collecting personal data, enhancing user engagement, or simply increasing revenue.

Behavioral economics literature has extensively examined the cognitive biases which Dark Patterns exploit. Therefore, previous scholarship can be used to conjecture their impact on behavior. Biases that most frequently identified as influential in the Dark Pattern context are: the anchoring effect (Tversky & Kahnemann, 1974, pp. 1128-1130); the bandwagon effect (Lang & Lang, 1984, p. 129); the framing effect (Tversky & Kahneman, 1981, pp. 436-438); the scarcity effect (Worchel, et al., 1975, pp. 906-908); the sunk cost fallacy (Arkes & Ayton, 1999, p. 591); inertia effect / status-quo bias (Samuelson & Zeckhauser, 1988, pp. 7-11); hyperbolic discounting (Loewenstein & Thaler, 1989, p. 182); social image concerns (Bursztyn & Jensen, 2017, pp. 131-132); the availability bias (Tversky & Kahneman, 1973, pp. 207-210); the information overload bias (Scammon, 1977, pp. 148-150). They are allocated to the respective patterns in Appendix 1. For most of these biases, extensive experimental evidence exists.[5] This

[5] See the respective sources indicated.

evidence allows for the assumption that, if "utilized" correctly, online design architectures can have a significant influence on decision-making.

2. Empirical Evidence

To some extent, this assumption has already been tested. Recent scholarship provides experimental evidence on how Dark Patterns influence human behavior.

The study of Nouwens, et al. (2020, p. 8) confronted users with different CMP designs and found that the employment of "Click Fatigue"-patterns leads to a 22 percentage points increase of consent-rates ($p<0.001$), while providing more detailed choices on cookies decreased consent by 8-20 percentage points ($p<0.001$). Machuletz & Böhme (2020, p. 490-492) examined the effect of "Aesthetic Manipulation"-patterns alongside the effect of increasing visible opt-in possibilities. Their lab experiment with 150 subjects found consent to increase by 20 percentage points ($p<0.01$). Utz, et al, (2019, p. 5-7) conducted a widespread field experiment that tested a variety of different cookie banner designs – inter alia the use of "Aesthetic Manipulation"-patterns – with 36,530 website visitors, by partnering with an e-commerce website. They found an increase of acceptance by 11.6 (smart-phone users) and 5.8 (computer users) percentage points, but it should be mentioned that ignoring the banner was an option in their design.

A broader and more comparative approach was taken by Luguri & Strahilevitz (2021). They conducted two large-scale online experiments, employing Dark Patterns in a sales context: A representative pool of subjects completed a survey on privacy and then were confronted with a pretend offer to subscribe to a data protection service. During this offer, subjects were treated with various Dark Patterns, revealing differing influence on their decisions. Subjects with a lower education were significantly more susceptive to Dark Patterns ($p<0.004$). While more aggressive patterns were generally more effective than milder ones, some aggressive patterns created a backlash among users, decreasing

acceptance or quitting the experiment. In general, “Hidden Information”, “Trick Question” and “Click Fatigue”-patterns were found most successful in manipulating behavior.

All the above-mentioned studies examine the effect of specific Dark Patterns in specific contexts and establish initial insights to this extent. However, beyond this, further experimental research is needed to create a broader comprehension of the influences of manipulative designs. Because of this, each of the abovementioned studies call for further experimental research on Dark Patterns.

C. Regulating Dark Patterns

Business use manipulative designs to make consumers act against their preferences. This section explains why, from an economical perspective, such practices justify regulatory intervention (I.). Furthermore, it shows that EU law already provides partial protection, albeit fragmentary, bearing many legal uncertainties and revealing systematic problems with the European consumer model (II.). Finally, it discusses how to determine and achieve a desirable scope of regulation and offer specific proposals on how to regulate Dark Patterns (III.).

I. Why Regulate Dark Patterns

Regulation that imposes limitations on the freedom of action requires justification. It must be comprehensible and sufficiently explained why the government may restrict the behavior of individuals and what purposes it pursues in doing so.

1. Economic Case for Regulation

Neo-classical economics presume that, given certain assumptions, market mechanisms lead to an optimal distribution of resources and establish an optimal price level through

supply and demand (Arrow, 1985, pp. 107-109). However, these circumstances predominantly do not apply in the real world, often leading to situations in which the distribution of resources is not optimal, and the overall utility could be improved through reallocation. Situations that leave room for such pareto-improvements which cannot be realized through market mechanisms are described as market failures (Bator, 1958, pp. 351-354). According to the public interest theory of regulation, market failures justify regulatory intervention to increase social welfare (Hertog, 2012, p. 25).[6]

Assuming rational actors, mainstream economics regularly identifies four sources of market failures: market power, externalities, public goods, and informational asymmetries (Cooter & Ulen, 2014, pp. 38-42). With the rise of behavioral economics, a fifth element has been added to this list: behavioral market failures (Hanson & Kysar, 1999, pp. 1425-1428; Bar-Gill, 2007, pp. 792): As market participants act systematically irrational, market forces may not create efficient outcomes. Certain choice architecture designs can stimulate specific irrational consumer behavior, allowing producers to "sludge" consumers into acting against their preferences, ultimately exploiting cognitive biases for increasing profits. Behavioral market failures are especially prevalent in consumer transactions, where the contractual decisions are not the result of negotiations, but unilateral designed by the seller and mass-marketed on a take-it-or-leave-it basis (Bar-Gill, 2014, p. 465). Sellers that single-handedly determine the choice architectures in which consumers act may promote and deliberately exploit irrational consumer behavior. In such situations regulation may be justified to enable more rational decision-making and thus, more efficient markets (Bar-Gill, 2014, pp. 477-486).

[6] This theory, however, is criticized to be an oversimplification, as political actors involved in legislation also consider their individual preferences.

Since Dark Patterns are manifold, have diverse specific characteristics and build on different biases, it is premature to subscribe all of them to the same market failure. To illustrate: patterns with information hiding attributes may promote informational asymmetries, whereas patterns manipulating the decision space are more likely to constitute behavioral market failures. In principle, an evaluation of each individual case is required. However, the underlying mechanism with which different Dark Patterns cause markets to fail is similar and will therefore be explained in the following.

Through Dark Patterns, companies increase consumers' acceptance beyond the scope that would be established by their rational preferences. This is true both in the data protection context (disclose more personal data than rationally reasonable) as well as the e-commerce context (buying more products for a higher price) and does not depend on the modus operandi of a pattern (both hiding information and framing choices may lead to this outcome). This mechanism can be simplified by considering the example of prices on an e-commerce website (Fig. 1):[7] With Dark Patterns, the perceived price ($P_{Perceived}$) of a good can be reduced (either directly, e.g., through "Hidden Cost"-patterns, or indirectly, by increasing the perceived value of a good, e.g., through "Scarcity"-patterns.) As the behavioral consumer will base his purchasing decision not on rational, but perceived price, the quantity demanded will be higher (q_2). The producer will adjust his supply according to the demand, creating an equilibrium that is below the price actually paid by the consumer

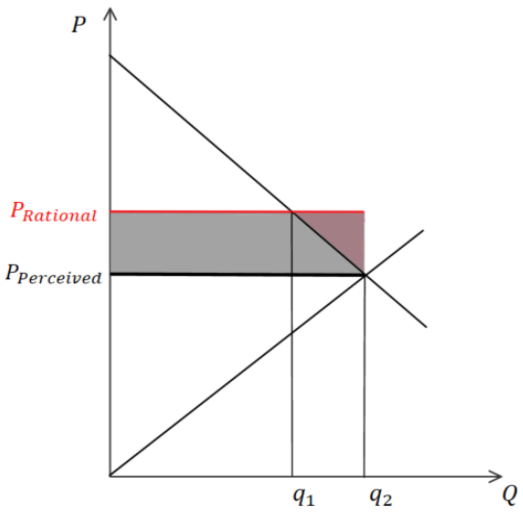


Fig. 1: Welfare Consequences of Behavioral Market Failure

[7] All figures and drawings included in this thesis were created by the author.

($P_{Rational}$). This has two consequences: First, the producer captures consumer welfare (grey area), as more consumers buy the product without any effective change in price. Second, some consumers purchase outside of their demand-curve (red area). For more sizable purchase decisions, this might bear the risk of financial overburdening for consumers.

In perfectly competitive market producers compete by decreasing prices (assuming identical quality). The Dark Patterns market allows them to compete through reducing perceived price instead. As a result, consumers face higher prices and, in some cases, higher financial risks. Price poses the most accessible example, but the mechanism applies in other contexts as well, for example when using Dark Patterns to "sludge" users to accept more cookies than their rational preferences would allow.

In economic terms, the function of law in the context of commercial activity is to avoid market inefficiencies and to promote pareto-optimal distributions. Since the underlying mechanism behind Dark Patterns leads to inefficient allocation of resources, regulatory intervention is justified from an economic perspective.

2. Elevated Risk in the Digital Space

Companies exploiting cognitive biases to increase revenue is neither a new phenomenon, nor is it exclusive to the digital world: pleasant smells or colors, tactical supermarket shelving, memorable catchphrases and many other techniques have long been used to increase consumption. However, one aspect of Dark Patterns makes them fundamentally more persuasive than analogue sales techniques, strengthening the argument for regulation: the scope of available information on users.

The private industry has an immense knowledge advantage over scholars and regulators regarding the behavioral effects of designs. By slightly adjusting their websites' design

and observing the change in users' behavior ("A/B-testing"), website operators can essentially run large-scale field experiments every day (Strahilevitz, et al., 2019, pp. 253-255). This allows them to them to pinpoint the exact influence of their design-choices. This high degree of precision in addressing consumer biases makes it more difficult for users to protect themselves against "sludging" in the digital space. While rational platform operators would seize this advantage to influence user behavior in the strongest possible way, only limited public information is available on the extent to which they indeed do so.[8]

This issue is further exacerbated when considering the trend towards personalization: Large online platforms are collecting a myriad of information about individuals, including their responses to certain design elements. They may collect information about which designs were how effective in guiding the user's behavior. Such information could be used to "weaponize" Dark Patterns by specifically personalizing interfaces in a way to which specific users are known to be most susceptible for maximizing the exerted influence (Luguri & Strahilevitz, 2021, p. 103). Such capabilities potentially pose a significant risk to consumers which could not exist in the analogue world.

3. No Market Solution

Regulatory intervention is required if a more efficient solution cannot be achieved within the market (Rose-Ackerman, 1998, pp. 347-349). This is not to be expected for Dark Patterns. Instead, market mechanisms will presumably exacerbate inefficiencies: Companies which use Dark Patterns are likely to generate more revenue, allowing them to prevail over competitors in the long run. This creates a strong incentive for all competing producers to employ Dark Patterns. Furthermore, competitive pressure may introduce a "race to the bottom" in terms of consumer friendliness, during which

[8] It is known, e.g., that Google tested 40 shades of blue in links on their interaction rate (Hern, 2014).

companies compete for consumer attention, data and purchasing decisions by trying to find the greatest possible degree of manipulation (Leiser, 2020, p. 2).

Theoretically, competitors could try to gain a competitive advantage by "taking the high road" and not use manipulative designs. This however would require producers to educate consumers about Dark Patterns. Such practice seems unlikely, as educative campaigns suffer from a collective action problem (Bar-Gill, 2014, pp. 469-471): It is costly to educate consumers, but as soon as their majority is aware of specific manipulative designs, competitors could simply choose to discontinue such designs. As the cost of education are incurred only by one competitor, but do not establish a lasting competitive advantage over the others, it is not viable for producers to engage in educational campaigns individually.

Neither can consumer reactions to Dark Patterns pose a market solution. While some patterns cause repercussions of consumers (Luguri & Strahilevitz, 2021, pp. 67-70) producers will have an incentive to establish an "optimal level" of manipulation to not forego profits through overly aggressive patterns. However, this level would not be "optimal" for consumers, as it constitutes the level of maximum manipulation available. This would potentially increase the consumers act against their preferences and thus maximize market inefficiencies. While there are indications of self-regulation through users publicly condemning companies that use manipulative designs[9], it is not noticeable that this practice is effectively reducing the use of Dark Patterns.

For these reasons, we cannot assume that the market itself will find an effective solution. On the contrary, market mechanisms create incentives to "perfect" online manipulation

[9] Noticeably on twitter under #darkpattern. Another example is https://darkpatternstipline.org.

techniques – a scenario, eventually resulting in the highest possible welfare loss for consumers. Regulatory intervention is therefore justified, if not required.[10]

II. Dark Patterns under European Legislation

To some extent, regulatory intervention already exists in the European body of laws. This section identifies which forms of Dark Patterns are (partially) covered by the acquis (1.) and whether forthcoming regulation will provide further protection (2.). This will enable the identification of existent regulatory gaps and systematical shortcomings in the European consumer model (3.).

1. Existing EU Regulation

Existing European Directives[11] and Regulations already put some constraints on the use of Dark Patterns in the EU. These limitations are context-dependent and mainly exist with regards to consumer transactions (a, b) and data protection (c). Appendix 1 provides an overview of the scope of regulation.

a) Consumer Rights Directive

The Consumer Rights Directive (CRD)[12] imposes limits on the design of e-commerce websites. It contains both precise rules and general standards.

Art. 22 prohibits concluding consumer contracts based on default options. Art. 27 stipulates, that consumers may not enter contracts without an explicit response. Thus, e-commerce contracts concluded using “Bad Default” or “Sneak into Basket”-patterns are void under EU consumer law.

[10] Art. 38 CFR explicitly calls for union policies to ensure “a high level of consumer protection”. Art. 114, 169 TFEU grant competence of the European legislator to ensure the protection of consumers' economic interests. When market failures require intervention, legislative competencies may constitute an obligation to protect consumers.
[11] Evidently, Directives produce no direct legal effect but must be transposed into national law.
[12] Directive 2011/83/EU, amended by Directive 2019/2161/EU.

Art. 8(2) sets out clear requirements for the design of buttons in online consumer transactions: They may *only* state "order with obligation to pay" or comparably unambiguous wordings. Otherwise, the contract is void. Similarly, Art. 6(1)(e), (6) obliges business to break down any key information about imminent contractual relationships. With this forced simplification and salience, "Hidden Subscription"-patterns, are effectively obstructed. Also, "Information Hiding"-patterns are prohibited to the extent that they conceal essential contractual elements or payment obligations. In addition, Art. 7, 8 state the fundamental requirement to provide information in plain and intelligible language. This general standard could provide a basis for prohibiting aggressive "Information Hiding"-patterns but requires further interpretation through adjudication.

Finally, Art. 9, 11, 12 grant the consumer the right to withdraw within 14 days of entering distance contracts. While this provision does not prevent Dark Pattern implementation, it enables consumers a way out of contracts made under their influence. However, it is questionable to what extent this constitutes an effective defense, as manipulation is often conducted subtle and unbeknownst to the consumer.

b) Unfair Commercial Practices Directive

The Unfair Commercial Practices Directive (UCPD)[13] includes additional restrictions for Dark Patterns. It applies to "business-to-consumer commercial practices", Art. 3(1) and prohibits "unfair" commercial practices, Art. 5(1), i.e., practices which contradict the requirements of professional diligence and can distort the average consumer's economical behavior, Art. 5(2). These requirements are met if the practice is "misleading", Art. 5(4)(a), 6, 7, "aggressive", Art. 5(4)(b), 8, 9, or included in Annex I.

[13] Directive 2005/29/EC, amended by Directive 2019/2161/EU.

Annex I UCPD

Some of the misleading commercial practices stated in Annex I prohibit specific Dark Patterns partially or completely:

- Nr. 7 prohibits falsely stating that a product is available only for a limited time. However, this only applies if an expiration of the time limit has no actual consequences. If the expiration does, e.g., lead to an increase in price, the timer would not be "false", even if such time limit was arbitrary (Martini, et al., 2021, p. 64). Therefore, "Urgency"-patterns may only be covered by the norm if they bear no consequences.
- Nr. 11a prohibits displaying advertisements amongst search results, without disclosing them as such, which covers one specific instance of "Disguised Ads"-patterns.
- Nr. 23b, 23c prohibit displaying consumer reviews without ensuring that they have purchased the product, as well reviews which have been commissioned. Thus, "Social Proof"-patterns are covered only when reviews are not based on genuine consumer experiences. However, it is not forbidden to present positive ratings more saliently.
- Nr. 26 prohibits unwanted solicitations towards the consumer by e-mail or any other remote media – this may cover extreme cases of "Nagging"-patterns, in which businesses insistently apply pressure, e.g., to provide a rating.

While Annex I Nr. 6 mentions a conduct named "Bait and Switch", this does not include the eponymous Dark Pattern. Nr. 6 prohibits the conduct of advertising for a product different from the one intended to sell. The Dark Pattern describes the process of giving a button another function than expected by the user (e.g., clicking on a red X-button opens another website). This pattern is therefore not covered, because it is more versatile than the conduct prohibited by Nr. 6 (Martini, et al., 2021, p. 64).

Misleading Practices

Commercial practices are misleading if they are "likely to deceive the average consumer, even if the information is factually correct […] and […] cause him to take a transactional decision that he would not have taken otherwise", Art. 6(1). The attentive reader will feel reminded of the initially proposed definition for Dark Patterns: "[…] trick users into doing things they wouldn't otherwise have done" (Brignull, 2010). Consequently, some misleading designs can therefore be considered prohibited conduct.

According to Art. 6(1)(b), the main characteristics of a product, such as its availability, must be truthfully presented. Hence, "Scarcity"-patterns giving false statements about the sparsity of supply are prohibited.

Art. 7(1), (4)(c) requires that the total costs of a transaction must be disclosed when consumers are invited to purchase. This specifically intends to avoid the exploitation of sunk-cost effects (Wendehorst, 2019, at 75). "Hidden Cost"-patterns, which also aim to exploit this bias, are therefore effectively prohibited.

According to Art. 7(2), the incomprehensible presentation of information is deemed equivalent to the misleading omission of information. Against this backdrop, both "Trick Question" and "Information Hiding"-patterns may be considered prohibited conduct, whenever they exceed a certain threshold of magnitude.

In addition, it seems plausible to include other dark patterns under the general provision of Art. 6(1). However, no case law to this effect could be observed.

Aggressive Practices

Some Dark Patterns may also be considered aggressive conduct. In each case, it is necessary that they exceed a materiality threshold to be determined in the individual case.

Art. 9(a) stipulates that the presence of undue influence is determined, among other things, on the persistence of the conduct employed. Hence, aggressive "Nagging"-patterns might qualify as undue influence in sales scenarios.

Art. 9(b) prohibits the implementation of disproportionate non-contractual barriers which prevent consumers from exercising their contractual or legal rights. The "Roach Motel"-pattern – making it deliberately difficult to cancel a subscription – can be subsumed under this provision.

c) GDPR

Because third-party cookies can act as personal identifiers[14] and most of their use-cases do not provide alternative legal justification, their installation usually requires the user's consent (Santos, et al., 2020, pp. 91-93). Dark Patterns are commonly used in CMPs to entice user consent for personal data processing. "Bad Default"-patterns are not compliant with these requirements, as set forth in recital 32 and confirmed by the ECJ (ECJ "Planet49", 2019, at 74). For other patterns, the legal situation is less clear, as subsequently outlined.

(i) Art. 4(11): Consent Criteria

In the absence of alternative legal justifications, the GDPR requires user consent for any processing of personal data, Art. 6(1). Consent must be freely given on an informed basis and unambiguously indicated through clear affirmative action, Art. 4(11).

Clear Affirmative Action

"Trick-Question" and "Aesthetic Manipulation"-patterns raise doubts about the clarity of the consent, especially if the response mechanism differs from the usual process. However, it is uncertain to which extent this provision aims to protect the trust of users

[14] Explained in more detail under D.II.

in the stringency of operating elements between different websites –guidelines of the European Data Protection Board (EDPB) do not indicate any concretization in this respect. Thus, the requirements are currently too abstract to constitute a prohibition for such patterns.

Freely Given

Design methods that make access to content dependent on consenting to data processing which is not technically necessary are prohibited under Art. 7(4), effectively banning "Forced Subscription"-patterns that compel users to give consent for data processing which is not necessary for the contract performance. However, this is less clear for patterns with more subtle effects: “Nagging”-patterns may create the impression that consenting is necessary in some cases, although it really is not. Even though this does imply a lack of free choice for some users, the effect is subliminal, and it is unclear whether the GDPR already prohibits such subconscious influence (Martini, et al., 2021, p. 55).

Recital 42 clarifies that consent is not “freely given”, if the data subject cannot refuse “without detriment”. “Click Fatigue”-patterns may require cumbersome actions to avoid giving consent. While such design most likely has a behavioral impact, it seems unlikely that the additional effort necessary to reject consent qualify as a "detriment" as understood in this recital.

Informed Basis

While consent-decisions need to be taken on an informed basis, the GDPR does not provide explicit requirements regarding the form in which controllers must provide such information online. Hence, mental deviations and limitations in information processing, on which Dark Patterns are commonly based, are not accounted for. However, case law is seeking ways to consider behavioral phenomena in this context: The German Federal

Court recently ruled that design interfaces that offer an overwhelming number of choices to prevent interaction do not provide sufficient information (BGH "Cookie-Einwilligung II", 2020, at 36). Thus, the court generally recognizes that excessive information does not serve the purpose of the GDPR. This could put a stop to “Hidden Information” and “Trick Questions”-patterns in the data protection context. However, it remains to be seen to which extent this interpretation will establish on a European level.

(ii) Art. 25: Data Protection by Design

Art. 25(1) turns the focus from individual violations to fundamentally inadequate systems. It requires operators to respect the data protection principles (Art. 5) in the initial technical outset ("privacy by design"). This includes the design of the user interfaces, which represents the most visible level of technical composition. Thus, design choices should also promote the implementation of data protection principles (EDPB, 2020, p. 18).

Design patterns which contravene the principles of Art. 5, e.g., by aiming to collect as much personal data as possible, are therefore generally in violation of Art. 25(1). However, the flexible structure of Art. 25(1) leaves room for operators’ discretion, by pointing them towards “state of the art” processing and “appropriate technical and organizational measures”. Since violations may lead to the imposition of a fine – Art. 83(4)(a) – it must be clear to the operator what behavior is expected of him, given the constitutional requirement of certainty in Art. 49(1) CFR. The provision is therefore dependent on more specific guidelines to be effectively applied in combating the use of Dark Patterns (Martini, et al., 2021, p. 58).

While aggressive patterns that exceed creative freedom to a particularly high degree can already be considered inconsistent with sound technical design and thus be prohibited by Art. 25(1) GDPR – such as very aggressive “Nagging”-patterns (Martini, et al., 2021, p.

57) – the legal situation remains uncertain for lighter manipulations, such as misleading color choices. Thus, Art. 25(1) GDPR potentially constitutes a viable tool against misleading designs, but it may only turn into an effective instrument through a legislative concretization of the design standards.

2. Imminent EU Regulation

Two more items of EU legislation governing the configuration of online markets are imminent: The Digital Markets Act[15] (DMA) and the Digital Services Act[16] (DSA). Both legislative proposals were drafted by the Commission and submitted to the Parliament and Council in December 2020.

The DMA primarily aims at regulating the market power of very large digital platforms ("gatekeepers"), by banning "unfair practices" (Considerations 4, 6, 12) which are explicitly listed in Art. 5 and 6 DMA. However, it does not cover the use of Dark Patterns.

The DSA aims to establish "uniform rules for a safe, predictable and trusted online environment" in which fundamental rights of consumers are "effectively protected" (Art. 1(2) DSA). This is to be achieved, among other things, through several mandatory information disclosures: It obliges online platforms to provide clear, easily comprehensible, and detailed information about any manual or automated content moderation (Art. 13(1), Art. 23(1)(c), (2)), the extent and basis upon which advertisements are personalized (Art. 24(c)) as well as the parameters used to provide content recommendations (Art. 25(1), Art. 29(1) DSA).

The DSA-proposal also generally recognizes the problem of manipulative behavior steering in Art. 26(1)(c), Considerations 32, 63, 68 DSA. However, the regulatory intervention is limited to influence exerted by third parties. The Commission does not

[15] COM/2020/842-final.
[16] COM/2020/825-final.

address the issue of platforms themselves manipulating user behavior through design – even though they are aware of this issue (European Commission, 2019). The commission is thus missing a prime opportunity: The self-declared legislative goal – creating a safer and more trustworthy online environment – could be greatly strengthened by touching upon Dark Patterns. Accordingly, the DSA proposal has been criticized to this extent by consumer associations (Verbraucherzentrale, 2021, p. 4).

3. Regulatory Gaps

The previous sections illustrate that Dark Patterns are not explicitly addressed by EU legislation but are partially covered by existent consumer and data protection laws. Such context-dependent regulation is not per se less appropriate for regulating Dark Patterns, given that they are most prevalent in these contextual environments. However, the existing protection is highly fragmentary and riddled with legal uncertainty: Only some patterns can generally be considered prohibited with certainty. Most patterns are either covered only in specific cases or constitute legal grey areas. This is due to several broad standards which could potentially be utilized in combating Dark Patterns but are hardly mapped out by European or national adjudication. This increases legal uncertainty especially for those patterns which are not universally condemnable, but for which a qualitative assessment is required. Then again, there are some patterns which are not regulated at all under EU law. An overview is presented in Appendix 1.

Additionally, it is noteworthy how few behaviorally informed judgements could be identified when assessing the applicatory scope of broader standards for Dark Patterns. This reveals a systematic problem: The European consumer model still assumes a consumer that is “reasonably well-informed and reasonably observant and circumspect” (Recital 18 UCPD; ECJ "Citroën Commerce", 2016). While this consumer model is not identical to homo economicus (as it does account for information deficits and limited

processing capacities), it relies on the assumption that individuals generally act in a rational manner (Sibony, 2014, pp. 922-926). While initial approaches to considering behavioral insights exist in data protection (Testori Coggi, 2012) and unfair competition law (Straetmans, 2016, p. 209), the rational model prevails especially when it comes to interpreting existent norms. The necessary behavioral perspective is often overlooked by legal practitioners (Mathis & Steffen, 2015, p. 31). To adequately challenge Dark Patterns under the existent EU legislation, this very perspective would need to be considered.

III. How to Regulate Dark Patterns

Thus far, it has been established that a case can be made for regulating Dark Patterns and that exiting EU regulation does not adequately cover the existent problems. This section will discuss how to avoid overregulation (1.) and in which scope regulation would be desirable, providing potential valuation methods for a cost-benefit analysis (2.). Ultimately, specific proposals on how to regulate Dark Patterns will be presented (3.).

1. Focusing on Manipulation

Dark Pattern regulation concerns a domain which is sensitive to fundamental rights: Art. 16 CFR guarantees the “freedom to exercise an economic or commercial activity”, which protects undertaking of commercial activities and all aspects of implementation (ECJ "Polkomtel", 2017, at 60-61). This includes the general freedom of design and advertising (ECJ "Neptune", 2015, at 71). Therefore, special attention must be paid to distinguishing manipulative designs from advertising. Advertising, which aims to persuade consumers to *change* their preferences, is a permissible and desirable part of the free market – it is undisputable from a behavioral perspective, as no disparity between rational and actual behavior occurs if consumers are convinced by the advertisement. Overregulation which

disproportionally limits commercial freedom would therefore be incompatible with producers' fundamental rights.

In other respects, too, freedom of design must not be restricted excessively. There may well be a legitimate interest for unequally presenting certain options on a website, e.g., if it is only relevant for specific audiences, such as special color-display options for colorblind users (Strahilevitz, et al., 2019, p. 249). Implementing too strict limits would neither be in the operators' nor the consumers' interest, as disproportionately reducing design possibilities could potentially hamper usability, creativity, and diversity within the internet.

What should be regulated, however, are designs that manipulate behavior and lead consumers to act contrary to their preferences. It is difficult to distinguish exactly when individuals deviate from their preferences and when they change preferences before making decisions (Schwartz, 2015, pp. 1402-1403). Manipulative choice architectures may have an indicative effect for presuming manipulation. Yet, a positive identification of which patterns make users act *against* their preferences would require to determine the perceptions and sentiments of consumers, i.e., their perceived deception and regret, after they have completed the transaction.[17] This can only be achieved through experimental studies. Hence, to confidently distinguish persuasive designs from manipulative designs, evidence-based regulation is indispensable.

2. Identifying the Necessary Scope of Intervention

From an economic perspective, regulation is desirable to the extent that its benefits outweigh the costs incurred. The benefit of regulating Dark Patterns is the increase in realization of consumer preferences (a); costs arise predominantly from lawmaking, as

[17] Item lists to measure this have already been established (Román, 2007, pp. 142-145; Machuletz & Böhme, 2020, p. 487).

providing evidence for regulators might turn out costly. These costs may be reduced through information disclosure duties (IDDs), which may elevate the optimal level of regulation (b). Providing an exact assessment of these criteria is not feasible on an abstract basis. However, potential valuation methods will be outlined subsequently.

a) Benefits: A Risk-Based-Approach

Consumers benefit from the regulatory effect because they increase the realization of their preferences through a reduction of manipulation (B). This benefit is a product of the degree of manipulation, which a pattern would exert (i) and the potential harm inflicted on the consumer because of manipulation (H).

$$B = i * H$$

Thus, the benefit depends both on the influence of Dark Patterns and on the contexts in which they are employed. Therefore, a risk-based valuation method seems appropriate to evaluate the regulatory effect (Weinzierl, 2020, p. 7).

To illustrate: Prohibiting Dark Patterns with a relatively weak influence may cause a large benefit, when it is employed in a particularly vulnerable setting. Moreover, less sensitive contexts may also result in large benefits, if the design has a strong effect on behavior. These two aspects, the degree of influence and the potential harm, will be examined closer.

Degree of Influence (i)

Quantitative approaches should be utilized to obtain accurate insights on specific manipulative effects.[18] To understand the degree with which Dark Patterns lead to variation in decision-making, experimental studies need to be conducted. Participants

[18] While qualitative methods – such as reviewing previous behavioral economics insights – may roughly predict their influence, relying on them exclusively would neglect the overall circumstances in which Dark Patterns are employed.

could be presented with neutral choice architectures (B) and choice architectures that implement Dark Patterns (DP_{1-n}). Then, the decisions made by individuals could be compared. This approach is simplified in Fig. 2. Such approach would allow to measure i as the percentage change in behavior induced by Dark Patterns, enabling a direct comparison of manipulation magnitude. An exemplary study design is included in Part D of this thesis.

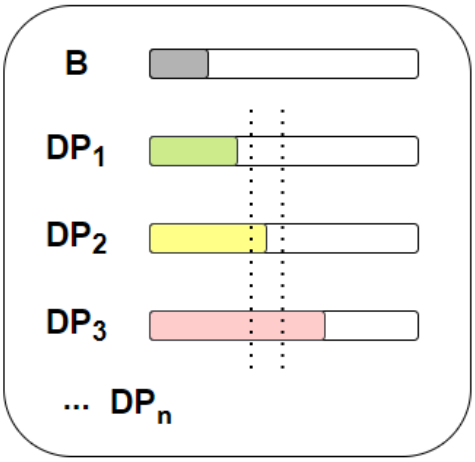


Fig. 2: Comparing Effectiveness of Dark Patterns

However, to account for context-dependent differences and changes in effectiveness over time, several studies would need to be conducted over the course of time, making this regulatory approach rather costly.

Potential Harm (H)

The potential gravity of harm caused by Dark Patterns is based on the (normative and economic) damages that result from consumers' preference deviation. Their evaluation is context dependent. H may record this value in real numbers.

In the data protection context, special categories of personal data are established by the European legislator, Art. 9(1) GDPR. These are subject to a higher level of protection because they are "particularly sensitive in relation to fundamental rights and freedoms" (Recital 51 GDPR). While it is generally difficult to assign a monetary value to privacy (Acquisti, et al., 2016, pp. 444-451), these data-categories should be subject to a lower influence-threshold, because of their heightened normative value.

In consumer protection, the potential gravity of harm depends on the economic relevance of the transaction. Certain transaction categories (e.g., consumer loans, insurances, or private investments) typically have greater financial relevance for consumers. The potential damage can be measured based on the consumer's expected financial burden in the respective scenario. Higher financial burdens should entail lower thresholds of acceptable influence.

Following the risk-based approach, designs employed in sensitive matters should be subject to a lower threshold of permissible influence. In Fig. 2, for example, DP_2 would be prohibited in a materially sensitive matter, but tolerable in other contexts. Beyond that, a general maximum limitation on influence should apply to less sensitive contexts as well, e.g., DP_3.

b) Costs and How to Reduce Them

Regulation is costly – it takes time and resources to create rules that are fit-for-purpose but not overreaching. Since evidence-based regulation is indispensable in the domain of Dark Patterns, several experimental studies must be conducted to consider different contexts and effect changes over time. This potentially presents legislators with considerable costs. If the costs of regulation are relatively high compared to its benefits ($Costs_{normal}$), the optimal level of regulation (Reg_{normal})[19] is lower and more costly to achieve (Hertog, 2012, p. 31).

However, costs could be significantly reduced if legislators found another way to access accurate information about Dark Pattern effectiveness. And, as chance may have it, this information already exists: Large online platforms that engage in A/B-testing have a substantial knowledge advantage when it comes to effectiveness of certain design

[19] The most efficient level of regulation is reached where the net marginal benefits are maximized, i.e., the maximum distance between cost curve and benefit curve (Δ_{max}).

elements (C.I.2.). Introducing IDDs that oblige companies to disclose such insights to the regulator could offset this leverage. For example, they could constitute the obligation to disclose A/B-testing results in the case of justified interest, helping to (Martini, et al., 2021, pp. 71-72).

Admittedly, IDDs do not render all further experimental evidence obsolete (it would still be necessary to distinguish manipulation from persuasion C.III.1). However, they could tremendously reduce the costs required for Dark Pattern regulation by providing insights on the degree of influence in different contexts. As this would decrease the marginal costs of regulation ($Costs_{IDD}$), the optimal level of regulation would both be higher (Reg_{IDD}) and could be achieved at a lower cost (Fig. 3).

s

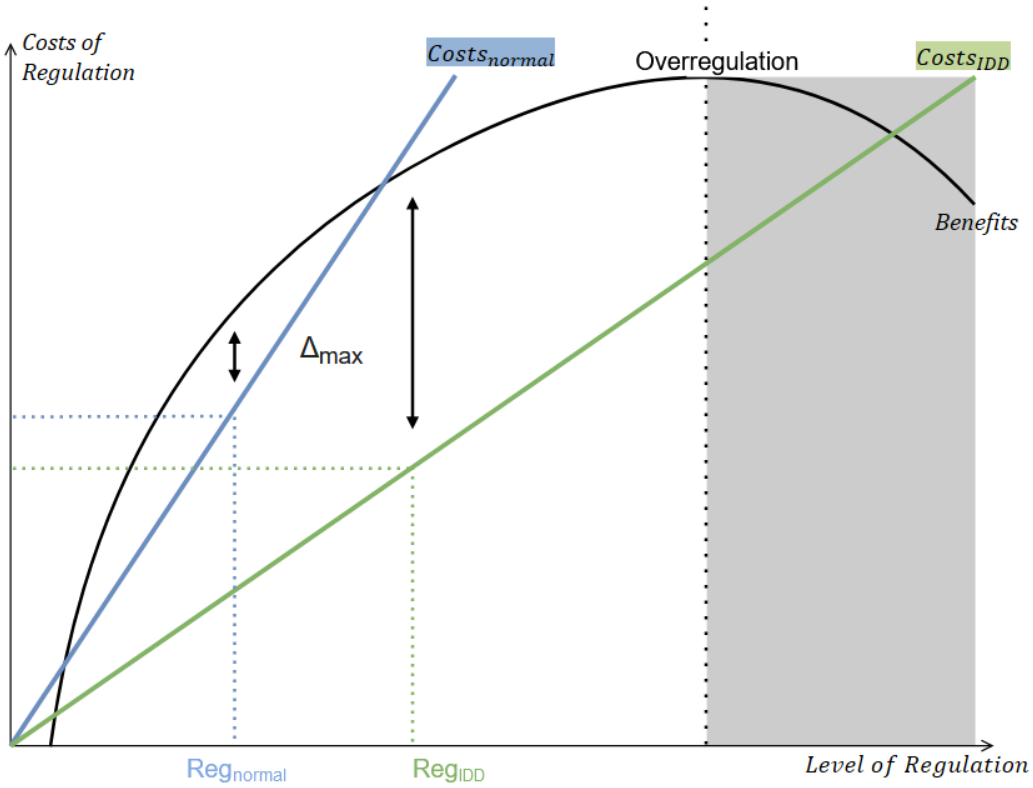


Fig. 3: CBA with and without IDDs

3. Suggestions for Regulatory Intervention

Building on previous insights of this thesis, three specific suggestions for Dark Patterns regulation can be made: taking a two-step approach (a), prohibiting specific conduct via rules (b), and building on existent regulations (c).

a) Two-Step Approach

Legislation needs to start with the methods that grant manipulative designs their special capabilities: the possibility of targeted testing. Therefore, a two-step approach is desirable: First, legislators will need to implement IDDs to access the platforms' insights on behavioral effects of design. Regardless of how Dark Pattern regulation – the second step – may ultimately look like, basing it on IDDs enables a higher level of (efficient) regulation while simultaneously reducing the incurred costs (Fig. 3).

The DSA already includes disclosure duties regarding (automated) content moderation, recommendations, and personalization of advertisements (C.II.2.) but passes up the chance to implement IDDs regarding knowledge about behavioral effects of design. It therefore passes the opportunity to take an important first step in Dark Pattern regulation.

b) Rules instead of Standards

When regulating behavior, legislators must decide between establishing concrete and ex-ante determined requirements for specific conduct ("rules") and general guidelines on how to behave, determined by adjudication in specific cases ex-post ("standards"). Typically, rules are more costly to create but provide more legal certainty, whereas standards are less expensive to draft, but create more costs in the adjudication process[20] and are more flexible in their use (Kaplow, 1992, pp. 571-572). This section explains why rules pose a better approach to Dark Pattern regulation than standards.

[20] Strongly depending on the complexity of individual cases (Teichman & Zamir, 2014, pp. 686-688).

While broader standards could theoretically enable intervention against yet-to-be-developed patterns, it is questionable whether this advantage would indeed materialize. Behavioral insights still receive little attention in the interpretation of legal norms (C.II.3.). After all, existent standards in consumer protection laws have been underutilized in opposing Dark Patterns previously, leaving gray areas when it comes to determining their legality (C.II.1.). It is thus uncertain whether legal practitioners would consider behavioral aspects when ex-post determining requirements from broad standards. An alleged flexibility of standards could therefore come at the expense of decreased protection, which would reduce the overall benefits created through regulation. This also renders the second argument for standards – reduced costs – trivial: Where regulatory benefits are low, even small costs may not be justified, as they may outweigh the benefits.

Contrarily, a rule-based approach could establish clear thresholds, facilitating the consideration of behavioral insights in Dark Patterns regulation: Clear rules allow shifting behavioral considerations into the legislator's responsibility, ensuring the consideration of non-rational consumer behavior ex-ante, even if legal practitioners have little knowledge of such topics. This will ensure behavioral biases – the driving operator behind manipulative designs – to be factored into the effect of legal norms. As rules generally have a higher deterrence effect than standards (Luppi & Parisi, 2011, p. 46), the primary aim of Dark Patterns regulation – discouraging operators from employing them – could be better achieved.

Clear rules may immediately dismantle legal gray areas, which are frequent in the context of Dark Patterns (C.II.3.), allowing consumers to determine the permissible limits of design from the law instead of relying on the interpretation of the norms through adjudication. This would render national differences in case law less influential, as a uniform level of protection throughout the EU is introduced. Such uniformity potentially

enhances the European single market, as cross-border consumer transactions – which are often concluded online – become more trustworthy. A reduction of legal uncertainties may also be beneficial for those online platforms which aim to be complaint.

c) Targeted Readjustments

In principle, there are two approaches for conceiving Dark Pattern regulation. The first option – the "all-inclusive" approach – would be to pass a separate piece of legislation, distinctively targeting manipulative designs in online environments. The second approach would be to readjust existing legislation through amendments.

The second approach appears preferable. As the legal analysis revealed (C.II.1.), the acquis already presents mechanisms which could potentially curb the use of manipulative designs. These existent tools could be sharpened to put a stop to manipulative designs: Regarding e-commerce, the UCPD already prohibits aggressive and misleading business conducts, which by their definition are reminiscent of manipulative designs. These provisions could be further fleshed out to ascertain which Dark Patterns are prohibited. Annex I UCPD would be suitable for this, as it explicitly specifies illegal conduct. Typical patterns or their underlying mechanisms could be incorporated here to render their unlawfulness undisputed. For data protection, the EDPB could issue guidelines defining more precisely to which extent Dark Patterns are incompatible with the consent requirements laid down in Art. 4(11) GDPR. Additionally, Art. 25(1) GDPR compels data processors to respect data protection principles when designing their websites (C.II.1.c). However, for this mechanism to be effective, explicit minimum requirements on the use of design patterns need to be established, for example by introducing a blacklist of certain Dark Patterns which are not considered "appropriate technical and organizational measures" under Art. 25(1) GDPR.

Another argument in favor of the second approach is its compliance with the EU Guidelines for Better Regulation. Considering the Commissions' "one-in, one-out"-approach (European Commission, 2021),[21] it seems preferable to opt for quick and cost-efficient amendments. The fact that this approach is context-dependent does not constitute drawbacks: As the use of Dark Patterns is particularly prevalent in e-commerce and data protection, it is appropriate to specifically address these areas with regulatory focus.

An exact design of these rules and the selection of Dark Patterns to be regulated cannot be proposed here, as this would require more detailed insights on specific Dark Pattern effectiveness and, eventually, a normative decision to be taken by the legislator.

D. Testing Dark Patterns: A Study Design

To regulate Dark Patterns, legislators will have to produce empirical evidence. This section presents a study design to be used for gathering further insights on the effectiveness of certain Dark Patterns.[22] Since there is a multitude of Dark Patterns in different contexts, a single experiment cannot produce behavioral insights on their entirety, as this would require several studies in different contexts and points in time. Bearing this in mind, the presented study may only highlight a fraction of the phenomenon: It examines the effects of "Aesthetic Manipulation", "Click Fatigue" and "Hidden Information"-patterns in the cookie banner-context. To this extent, the study may expand the existing knowledge on the influence of Dark Patterns on user behavior.

[21] Meaning that every newly introduced regulation must be accompanied by abolishing existing hurdles within the regulatory area.

[22] Unfortunately, the original intention to carry out this study as part of the thesis could not be realized, since the funding proposal (submitted on 15.04.2021) could not be approved before the thesis deadline. As soon as funds are available, the experiment will be conducted, and the results will be published.

I. Value Added through the Study

Previous experiments have been conducted on the effect of CMP-design on privacy choices: One study tested for "Click Fatigue"-patterns with a small sample (n=40), mostly consisting of subjects with an academic background (n=37) (Nouwens, et al., 2020, pp. 6-9). Another examines the effect of "Aesthetic Manipulation"-patterns but exclusively tested students of computer sciences (Machuletz & Böhme, 2020, pp. 486-490). A third study conducts a representative field experiment, but only tests for "Aesthetic Manipulation"-patterns (Utz, et al., 2019, pp. 4-7).

Through using representative samples, the proposed study may add to these observations by providing insights more depictive of the average internet user. Additionally, it would be the first study to directly compare the effectiveness of different Dark Patterns in a CMP-context. Finally, besides initially testing previous findings which indicate an influence of education on Dark Pattern susceptibility (Luguri & Strahilevitz, 2021, pp. 70-71; 80), this study also introduces and tests the novel hypothesis that Dark Pattern effectiveness depends on the degree of their familiarity.

II. Cookie Banners as an Experimental Setting

HTTP-Cookies are small text files which are locally stored by browsers when visiting a website. They provide a unique identification that allows websites to recognize the devices that access it. This is necessary for the internet to function in the way we know it: Without recording what happens within a "session" it would be impossible to keep track of user interaction with a website, e.g., which items have been placed in the shopping cart. All interaction would be forgotten, once the visitor moves or refreshes the page (PrivacyPolicies, 2021). Therefore, cookies are an essential tool for increasing user experience.

Initially, cookies do no raise privacy concerns – by their technical design, cookies can only be retrieved by the web servers which installed them, making it impossible to read cookies from another website. However, this changes when considering "third-party" cookies: When an operator implements third-party elements (e.g., interactive maps from Google or videos from YouTube) on their website, those elements can install cookies. When several websites use third-party elements, the provider of these element knows through which websites their cookie was installed and retrieved (Fig. 4). This allows for users' browsing behavior to be tracked throughout the internet.

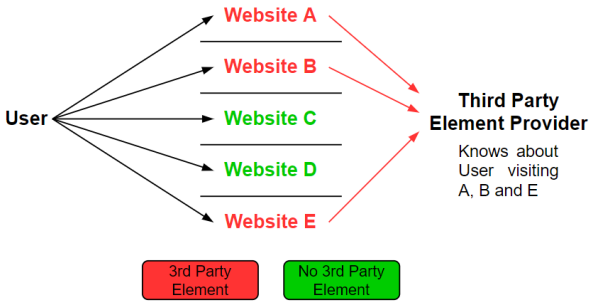


Fig. 4: Functionality of third-party cookies

As many websites use third-party cookies for analytical or advertising purposes, the amount of data thus collected is vast. The more data collected, the easier it is to identify users' identities: Current analytical tools can re-identify 99.98% of individuals from anonymized datasets with 15 demographic attributes (Rocher, et al., 2019, p. 6). Hence, when many third-party cookies are accepted, companies to directly identify and track users and their online behavior – granting deep insights – even if users never disclosed personal information directly to these companies.[23] Because of this, third-party cookies constitute personal data under Art. 4(1) GDPR. Most third-party cookie use-cases requires the data subject's consent (Santos, et al., 2020, pp. 91-93).

Testing Dark Patterns in the CMP-context brings several advantages: First, cookie banners provide high ecological validity of the study environment, because Dark Patterns

[23] One widely discussed (and litigated) example for this is Facebook's "Like"-button (ECJ "Fashion ID", 2019).

are widely used in this context, as indicated above (B.II.). Second, the common legal framework provided by the GDPR enables a transnational examination of contemporary CMP-design standards. Treatments can be designed based on a such examinations to warrant a high ecological validity of the treatments.

Finally, the main advantage of testing in a CMP-environment are the clear preference-structures of business and consumers: While website operators have an incentive to install many third-party cookies, rational users would choose to avoid them to maintain their privacy. Businesses have a rational incentive to install third-party cookies, because it increases the benefits received from operating the website: Third-party elements may increase the user experience, enable the use of analytical tools to monitor and analyze website traffic (e.g., Google Analytics), or place advertisements through ad-serving companies which implement banners on their website, thus allowing them to cover operational costs or generate revenue (Webster, 2014, pp. 10-18; 78-86). On the other hand, it is rational for consumers to value their privacy and thus avoid the excessive use of cookies: Retaining personal data can prevent price discrimination and therefore increase consumer surplus, as sellers may ask for higher prices if they have information about consumers' individual willingness to pay. Additionally, excessive disclosure of personal data bears the risk of blackmailing or identity theft incidents, which potentially create high social and financial costs (Acquisti, et al., 2016, pp. 445-447). Based on this, rational individuals would choose to reject third-party cookies whenever possible.[24]

This clear preference structure allows to directly measure the effectiveness of Dark Patterns: Cookie banners require an interaction – the more intrusive the cookie choice,

[24] However, accepting third-party cookies may also grant utility for some individuals, e.g., if they enjoy personalized advertisements because it decreases their information cost while online-shopping. For those individuals, rational choice might explain more privacy-invasive decisions. To account for this, the experiment measures individual privacy preferences (D.IV.1.).

the more likely individuals act against their preferences, i.e., the stronger the influence of the pattern.

III. Hypotheses

This experiment tests three hypothesis which are further explained in this section.

1. Influence on Cookie Choice

Dark Patterns aim to influence users' decisions by utilizing behavioral biases. The patterns chosen as treatments in this experiment are "Aesthetic Manipulation" (T1), "Click Fatigue" (T2) and "Hidden Information" (T3) (see Fig. 5). Their presumed influence is based on different cognitive biases.

"Aesthetic Manipulation": one choice is visually emphasized over another, by using brighter, more positively received colors. In (good) user experience-design, more aesthetically pleasing buttons usually indicate to users that they continue their task flow (Yablonski, 2020, pp. 65-74). This creates a framing effect on button-choice, enticing users to more privacy invasive cookie selections. Buttons that explicitly state "Accept All" might be clear from a system 2-perspective, but individuals focused on progressing on the website will likely resort to system 1-thinking when confronted with CMPs. The assumption is, that the framing effect will encourage users to select aesthetically more attractive "Accept All"-buttons, because they associate it with continuing.

"Click Fatigue": impeding the task flow by making an interaction more cumbersome than necessary. In the CMP-context, "Click Fatigue"-patterns often require users to navigate through a sub-menu. The option to reject cookies is often not initially available but can only be accessed through "settings"-buttons. This likely abuses the status-quo bias: As users are forced to access the settings to reject cookies, accepting them is presented as the default option. This increases the cognitive difficulty for rejecting cookies. Behavioral

economists link this effect to human inertia (Samuelson & Zeckhauser, 1988, pp. 33-35) an explanation which seems plausible in the CMP-context: users might simply find it too inconvenient to change the settings.

"Hidden Information": interface elements are deliberately hidden from the user. In cookie banners, it is common practice to hide non-accepting options as links within the banner text, instead of presenting them as buttons. The "Accept All"-option, in contrast, is presented as a button. The suspected mechanism behind this treatment is comparable to that of T1: At first glance, users will only see one available button, suggesting system 1-decision makers that this button is required to progress. Only at second sight, i.e., by investing the cognitive effort to switch to system 2-thinking, users will even be able to identify their possibility to alter their privacy options.

Based on these implications, the following hypothesis can be stated:

H1: The implementation of Dark Patterns in cookie banners will increase the cookie acceptance-rate.

2. A New Hypothesis: Familiarity as Factor

In previous studies, aggressive patterns have been identified to show more influence on behavior (Luguri & Strahilevitz, 2021, pp. 67-70). As all treatments chosen for this study are relatively mild, a novel factor to influence Dark Pattern effectiveness is suggested: their degree of familiarity. Familiarity builds over time as users are frequently confronted with a specific pattern. After repeatedly being exposed to it, users might begin to identify and try to "beat" the pattern and thus respond according to their preferences. While this can require substantial cognitive effort in the beginning, such effort may decrease over time, as consumers practice how to respond to the specific pattern. After some practice, users may recognize and "beat" patterns entirely in "system 1"-thinking, thus depriving the pattern of its effectiveness.

This hypothesis builds on findings suggesting that consumers, to some extent, adapt to manipulations of the digital environment over time: A representative study conducted in 2019 confronted users with "Social Proof" and "Scarcity"-patterns on hotel booking websites. Participants widely interpreted these as exerting sales pressure (65%) and stated to distrust those companies (49%). Only 16% believed claims made in the patterns to be true (Shaw, 2019). Another online experiment showed that 55% of users were able to identify "malicious designs" when they were employed (Di Geronimo, et al., 2020, p. 8). Finally, Luguri & Strahilevitz (2021, p. 67-70) witnessed a decrease in acceptance rates and even participants aborting the experiment (i.e., foregoing their compensation) when confronted with noticeably aggressive "Scarcity"-patterns.

The study could test this hypothesis. Although it is nearly impossible to gather reliable data on how familiar each participant is with each specific pattern, the prevalence of each pattern can be used as an approximate value: Since the underlying assumption behind the influence of familiarity is the amount of experience resulting from exposure to the pattern, more patterns that occur more frequently or over a longer period of time should, on average, be less effective, because have gathered more experience in dealing with them.

Previous studies mostly identified "Aesthetic Manipulation" (T1), "Click Fatigue" (T2) and "Bad Defaults" as the most prevalent patterns in CMPs (B.II.). However, a descriptive analysis conducted as part of this study (Appendix 2) as well as a recently published report of a prominent privacy-NGO (noyb, 2021) indicate a recent change in the Dark Pattern landscape: The use of "Bad Default"-patterns declined[25] and a previously unmentioned pattern, which presents further options as a link within the text instead of showing a button, is now the third most employed Dark Pattern (described as "Hidden Information", T3). Therefore, if the hypothesis on familiarity is correct, T3-treatments should constitute

[25] Likely as a response to recent ECJ-rulings (ECJ "Planet49", 2019).

the most effective treatments, as these patterns have just recently emerged and are less commonly employed than T1 and T2-patterns. Furthermore, assuming a somewhat comparable duration of employment, T2 should be slightly more effective than T1, as T1-patterns are mildly more prevalent than T2-patterns. Therefore, the following hypothesis can be raised:

H2: The more widespread the Dark Pattern in the field ($\overrightarrow{T_3, T_2, T_1}$), the lower their effect on increasing acceptance rate.

3. Testing Previous Results: Education as a Factor

Finally, this experiment tests previous findings which suggest that individuals with lower formal education are more susceptible to the influence of Dark Patterns (Luguri & Strahilevitz, 2021, pp. 70-71; 80).

H3: The susceptibility to Dark Patterns increases with a decrease in education.

IV. Method

To test these hypotheses, a blind randomized controlled trial in form of an online experiment with 500 representatively prescreened participants is to be conducted. As part of this thesis, a website was created to administer the experiment. It is accessible under www.onlinebehavior.net, a domain specifically purchased for this experiment. The exact questionnaire and treatment designs are available under this website, screenshots of which are also included in Appendix 3. Subsequently, the underlying considerations behind the study design will be explained.

1. Study Design

The study consists of three parts: cookie banner confrontation, experimental survey on privacy preferences and confrontation with cookie choice followed by a questionnaire.

Subjects will be invited to participate in a survey on “Online Behavior of Individuals”. The topic is deliberately kept ambiguous to reduce the possibility of priming bias without actively deceiving subjects about the topic of the study (Jacquemet & L'Haridon, 2018, p. 163). Prior to being able to access the information sheet, subjects are confronted with one of four randomly assigned cookie banner designs: a baseline design (B), not utilizing any Dark Patterns and three treatments: T1, employing an “Aesthetical Manipulation”-pattern; T2, employing a “Click Fatigue”-pattern; T3, employing a “Hidden Information”-pattern (Fig. 5).

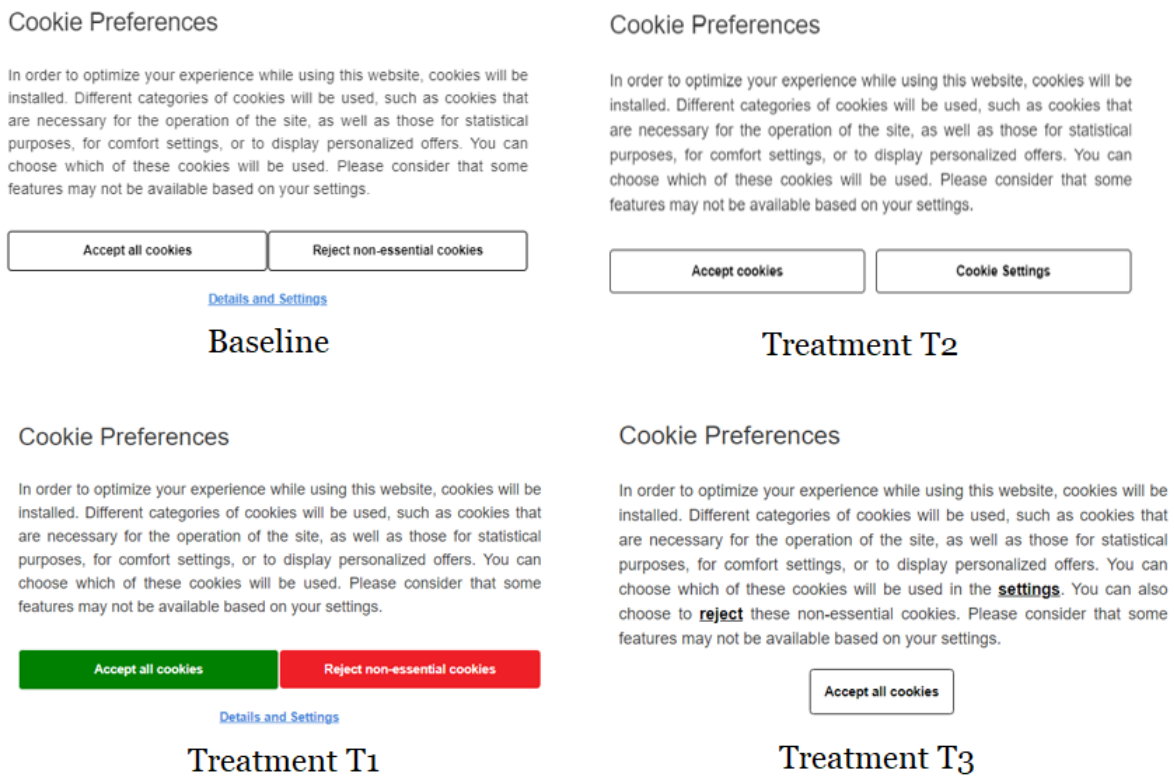


Fig. 5: Treatment Designs

After responding to the CMP, participants access the information sheet, where they may choose to participate in the study. If they do not accept, their cookie banner decision is automatically deleted. If they accept, the survey begins, asking several demographic questions, including age, gender, nationality, education, and field of employment. A field for “Prolific ID” is included to facilitate interaction with the survey research firm.

Subsequently, participants are asked to repeatedly choose between two hypothetic online retailers, one significantly more privacy invasive and the other with an increasingly higher price. This part measures participants' willingness to pay (WTP) for privacy to account for interpersonal differences in privacy appreciation. WTP was chosen over willingness to accept (WTA) to account for any bias created by endowment effects. The multiple price list (MPL) elicitation method is used to measure WTP, because its transparency and simplicity reduce the chance of a systematic WTA/WPA gap (Brebner & Sonnemans, 2018, p. 43). This experimental measurement of WTP is supplemented by a subsequent questionnaire on self-reported privacy preferences (PP), followed by five substantive multiple-choice questions about "browser cookies" to evaluate the respondents' knowledge about cookies and their privacy implications, the choice of which was influenced by online learning platforms (Welsh, 2021).

In the final section, participants are presented with two pieces of information: First, a brief text about cookies, their privacy implications, and the legal requirements to ensure participants' comprehension of CMP-related incentives without providing a normative frame. Second, participants are confronted with the respective banner they were randomly assigned in the beginning, as well as the choice they had made. After that, participants are asked to respond to questions indicating perceived deception (PDE) and perceived difficulty (PDI) of the banner, as well as their individual regret (RE). For this, the item-list implemented by Machuletz & Böhme (2020, p. 491) is used.

Questions are presented from general to specific to reduce order effects (Schwarz, et al., 1991, pp. 6-7). To enhance inclusiveness and reduce framing effects, language is kept easy and neutral. The number of simultaneously displayed questions is kept low to maintain respondents' engagement and attention. The response mode is closed-ended on a 5-point scale with semantic anchors; questions with a negative frame are placed on an

inverted scale to reduce respondents' cognitive load and account for acquiescent response attitudes (Hinz, et al., 2007, p. 1).

2. Choosing Treatments

Since the Dark Patterns-landscape changes over time (D.III.2.), treatment-patterns had to be designed based on most recent observations to ensure a high ecological validity. To identify which patterns are currently employed most frequently, a systematic review Dark Pattern employment in cookie banners was conducted. It reveled "Aesthetic Manipulation" (69,46%), "Click Fatigue" (55,69%) and "Hidden Information" (36,53%) to be the most prevalent patterns. The detailed approach and results of this descriptive analysis are presented in Appendix 2.

Shortly after this investigation was conducted, a privacy-focused NGO published a descriptive analysis on cookie banners of 560 websites, finding similar results (noyb, 2021).[26] Therefore, the selection of the treatments reflects the current state of Dark Pattern implementation in cookie banners.

3. Participants

To ensure a representative sample of participants, a survey research firm that allows pre-screening respondents can be commissioned. The service of Prolific, for example, allows pre-selecting certain groups of participants – inter alia – based on their nationality and degrees of formal education. The composition of the participants can be representative in terms of formal education so that the respective average national levels are reflected among the participants. Overall, around 500 participants should be invited to participate

[26] 81% of banners included "Click Fatigue"-patterns, 73% used "Aesthetic Manipulation"-patterns and 51% used "Hidden Information"-patterns, as defined in this thesis. While this analysis suggests even stronger numbers, they confirm the identified patterns to be currently used most frequently in CMP-design.

to ensure that the amount of available data is sufficient to facilitate the analysis of each treatment while account for each dependent variable.

4. Analysis

While the experiment has not yet been conducted, the structure of the data-output in the back end of the website is presented in a dummy-dataset included in Appendix 3. Once the data is gathered, responses can be coded as indicated therein to facilitate the empirical analysis.

After obtaining and coding the data, we can test our hypotheses. If our items are internally consistent (Cronbach's $\alpha > 0{,}7$), we can analyze the data using a PROBIT model: PROBIT regressions require a binary independent variable. While our cookie acceptance is measured on a scale from 1-3, this is mostly done to facilitate descriptive statistics. For running the regression, we can merge the middle value (agreeing to *some* cookies) with the rejection of cookies, as both pose conscious decisions of participants against cookies, meaning that they are not influenced by the pattern employed. This way, PROBIT poses a reliable analytical approach for measuring the influence of the treatment on cookie acceptance rate (**H1, H2**), while accounting for education (**H3**), as well as privacy preferences (WTP and self-assessed) and cookie knowledge. The correlation between different treatments and DPI, DPE and RE can be calculated using an OLS regression, as this is independent of participants' cookie-choice.

V. Limitations

The proposed study design comes with some limitations. One concern is that familiarity can only be determined by approximation. To obtain a more robust result on the influence of familiarity, the proposed mechanism would need to be tested separately in a more simplified environment.

Furthermore, the measurement of privacy preferences leaves room for refinement: Although the self-assessed privacy evaluation is accompanied by the experimental measurement of WTP, this measurement relies on a hypothetical scenario. Therefore, potential risk of participants overestimating their privacy preferences is still existent. This could be reduced by testing WTP in a more complex, incentive-based experiment.

Finally, education level can only be measured in categories. While this gives an approximate indication of a general tendency of the impact, it cannot indicate a linear relationship, as these formal education levels do not correspond directly to knowledge acquisition or even intelligence.

E. Conclusion

Dark Patterns pose an issue that needs to be addressed. They abuse behavioral biases through the design of online choice architectures, "sludging" users towards decisions that go against their preferences and instead are profitable for the architects of online environments. As a result, consumer surplus is captured, leading to a suboptimal distribution of resources – and since a market solution is not in sight, the law and economics-perspective dictates the need for regulatory intervention.

To a certain extent, such interventions already exist. This thesis analyzed the consumer and data protection acquis, explaining which specific Dark Patterns are prohibited, constitute legal gray areas, or are not captured by EU-regulation at all. This revealed not only that the current level of regulation is fragmentary, but also suffers from a systematic problem: European law is clinging to the concept of a rational decision-maker. At present, it does not protect rationality - it presupposes it.

To protect users against Dark Pattern manipulation, this perception of consumer behavior needs to change. Law cannot provide adequate responses to the systematic exploitation of irrational behavior if it assumes individuals to act in a solely rational manner. And since behavioral insights are widely neglected in the interpretation of legal norms, legislators will need to account for this dimension ex-ante. They can do so by issuing more specific rules instead of general standards when regulating Dark Patterns. More precisely, they should build on existent regulatory mechanisms such as the UCPD and the GDPR – which are essentially well suited to the task – and expand them through amendments.

For avoiding overregulation, legislators should adopt an evidence-based approach to determining the exact limits of permissible influence of online environments. A risk-based approach that considers both the degree of influence and the severity of its consequences seems appropriate to achieve this. For contributing to the gathering of these information, the design of an experimental study was presented as part of this thesis. It aims to measure the influence of the currently most prevalent patterns in the CMP-context, could test previous results on Dark Pattern research and introduces the novel idea of familiarity influencing Dark Pattern effectiveness.

Beyond this, the legislative process can be promoted by reducing the considerable knowledge advantage that online platforms have gathered through A/B-testing. With the introduction of IDDs, platform operators can be forced to share their insights on behavioral effects of design, which decreases the costs of legislation, thus enabling a higher level of protection. With the DSA – which does impose informational duties, but not regarding effects of design – the EU Commission missed a prime opportunity for promoting the protection against Dark Patterns.

The results of this work can therefore be summarized in five hypotheses:

1. There is a need for regulatory intervention concerning Dark Patterns.
2. Such intervention should amend the existing regulatory framework by introducing clear rules that consider behavioral insights.
3. A risk-based approach is appropriate for determining the right level of intervention; this requires the legislator to gather empirical evidence on Dark Pattern effectiveness.
4. While gathering this evidence, the familiarity of each pattern should be considered, as this possibly affects the amount of influence Dark Patterns exert on behavior.
5. Gathering this information is costly. To decrease regulation costs and thus increase the level of optimal regulation, legislators should create obligations for online platforms to share their insights on behavioral effects of design.

12.961 words, including footnotes and appendices, but excluding tables, cover page, bibliography, abstract, and authorship declaration, as specified in the EMLE Thesis Guidelines.

Appendix 1 – Dark Patterns, their Attributes and Biases (Table)

Name	Description	Attributes	Cognitive Bias	Source
Sneak into Basket	Automatically adds products to the shopping cart (often labeled "bonus" or "necessary").	Decision Space; Covert	Default Effect; Framing Effect	(Gray, et al., 2018); (Brignull, n.d.)
Hidden Costs	Discloses additional (often unreasonably high) costs only shortly before the order process is completed. For example, as "service fees" or "handling costs".	Information Hiding; Deceptive	Sunk Cost Fallacy	(Mathur, et al., 2019); (Gray, et al., 2018); (Brignull, n.d.)
Hidden Subscription	While the appearance of a one-time payment or free trial is created, a recurring payment obligation is established.	Information Hiding; Deceptive; Obstructive	Framing Effect; Inertia Bias	(Mathur, et al., 2019); (Gray, et al., 2018); (Brignull, n.d.); (Bösch, et al., 2016)
Bait and Switch	The action performed by the individual results in a different outcome than expected, e.g., a button with a cross is given an approval value.	Decision Space; Deceptive	Framing Effect; Inertia Bias	(Gray, et al., 2018); (Brignull, n.d.)
Roach Motel	Choice design that makes it difficult to delete existing accounts or cancel subscriptions, for example by having to send an e-mail or by hiding the options in submenus.	Decision Space; Obstructive; Covert	Inertia Bias; Hyperbolic Discounting	(Mathur, et al., 2019); (Gray, et al., 2018); (Brignull, n.d.)
Bad Defaults	Options in settings (for example cookie banners or privacy settings in social media websites) are preselected so that the most invasive setting is set as the default. This can also be done on e-commerce websites, for example by preselecting optional services, such as insurances, etc.	Decision Space / Information Hiding; Covert; Obstructive	Default Effect; Inertia Bias	(Bösch, et al., 2016)
Forced Subscription	Visiting a website or using a service is only possible with setting up an account, although this is not technically necessary.	Decision Space; Obstructive	Hyperbolic Discounting; Sunk Cost Fallacy	(Mathur, et al., 2019); (Martini, et al., 2021)
Urgency	Design elements suggest that there is a special offer that is time-limited and will expire soon, e.g., using a countdown timer (usually with no actual consequences upon expiration).	Decision Space; Deceptive; Pressuring	Scarcity Effect	(Mathur, et al., 2019); (Luguri & Strahilevitz, 2021)
Scarcity	Design elements suggest that there is a particularly high demand for the product, or that only a small amount of remaining stock is available.	Decision Space; Deceptive; Pressuring	Scarcity Effect	(Mathur, et al., 2019); (Luguri & Strahilevitz, 2021)
Social Proof	Messages suggesting approval of the product by other buyers, for example through (fictional) testimonials from previous customers or activity messages suggesting a high number of purchases, visits, or downloads.	Decision Space; Deceptive; Pressuring	Bandwagon Effect	(Mathur, et al., 2019); (Luguri & Strahilevitz, 2021)
Disguised Ad	Advertisements are integrated into the interface in such a way that they give the appearance of being usable elements or content. When clicked, users are directed to an external website.	Decision Space; Deceptive	Framing Effect	(Gray, et al., 2018); (Brignull, n.d.)
Aesthetic Manipulation /	The workflow is influenced by the visual design of the user interface, for example, by making some design elements more visually appealing than others.	Decision Space; Obstructive; Covert	Anchoring Effect; Framing Effect;	(Mathur, et al., 2019); (Luguri & Strahilevitz, 2021)

Hidden Information	Certain elements options or information is deliberately hidden, e.g., in a sub-menu, in small print or through visual design.	Information Hiding; Deceptive; Obstructive; sometimes Covert	Framing Effect; Information Overload Bias	(Mathur, et al., 2019); (Luguri & Strahilevitz, 2021)
Trick Questions	Deliberately misleading texts that are intended to overwhelm/confuse the user and lead her to make certain decisions (e.g., double negations).	Decision Space; Obstructive; (sometimes: Covert)	Informational Overload Bias; Framing Effect	(Mathur, et al., 2019); (Gray, et al., 2018); (Brignull, n.d.)
Nagging	The task flow is interrupted by repeated requests, e.g., by "Are you really sure" dialog boxes or by requests that can only be answered with "Yes" or "Not now" and are asked again at certain intervals.	Decision Space; Obstructive; Pressuring	Inertia Bias; Framing Effect	(Gray, et al., 2018); (Luguri & Strahilevitz, 2021)
Click Fatigue	The task flow is deliberately complicated by making certain actions more strenuous to execute than necessary, discouraging users from making those choices. For example, inserting unnecessary sub-menus or intermediate steps.	Decision Space; Obstructive; (sometimes: deceptive)	Availability Bias; Framing Effect; Inertia Bias; Default Effect	(Gray, et al., 2018); (Martini, et al., 2021)
Confirmshaming	Declining options are formulated to elicit a negative emotional response (e.g., shame) because the decision is framed as bad or irrational. E.g.: “no, I do not want to accept the deal and save money”	Decision Space; Obstruction; Pressuring	Framing Effect; Social Image Concerns	(Mathur, et al., 2019); (Brignull, n.d.)
Price Comparison Prevention	A user experience design that deliberately makes it difficult to compare prices with those of different vendors. For example, some e-commerce sites make the product information on their sites un-copyable to prevent users from comparing them with other sites.	Decision Space; Obstructive	Availability Bias; Inertia Bias	(Brignull, n.d.)

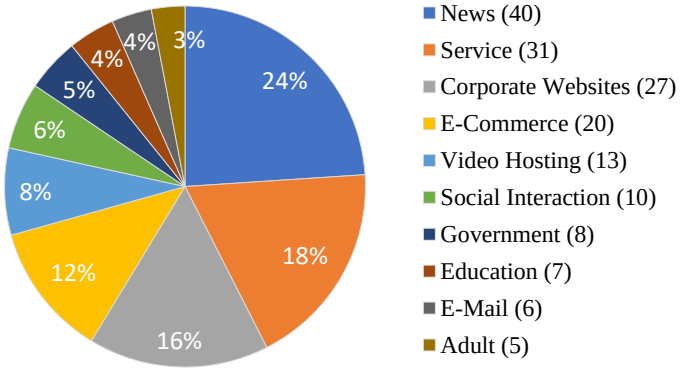
Legend	
Generally illegal in e-commerce contexts	Generally illegal in data protection contexts
Legal gray area or only specific forms prohibited in e-commerce contexts	Legal gray area or only specific forms prohibited in data protection contexts
Not illegal under EU-law	

Appendix 2 – Descriptive Analysis of Dark Pattern Prevalence

To identify the most prevalent Dark Patterns, a systematic review of the 100 most visited websites within the three largest EU economies[27] – Germany, France, Italy – was conducted. The analysis was limited to these countries because strong economies generally bear more affluent consumers, giving companies higher incentives to "sludge" customers into consumption. The research was limited to most visited websites because evidence suggests that more frequently visited websites employ more Dark Patterns (Mathur, et al., 2019).

The ranking was extracted from Alexa Internet on the 09.04.2021 and is based on the previous months' average traffic, calculated with daily visitors and pageviews. Out of 300 entries, 133 had to be removed for being duplicates (81), inaccessible (10) or not presenting CMPs (42), leaving the database with 167 observations.[28]

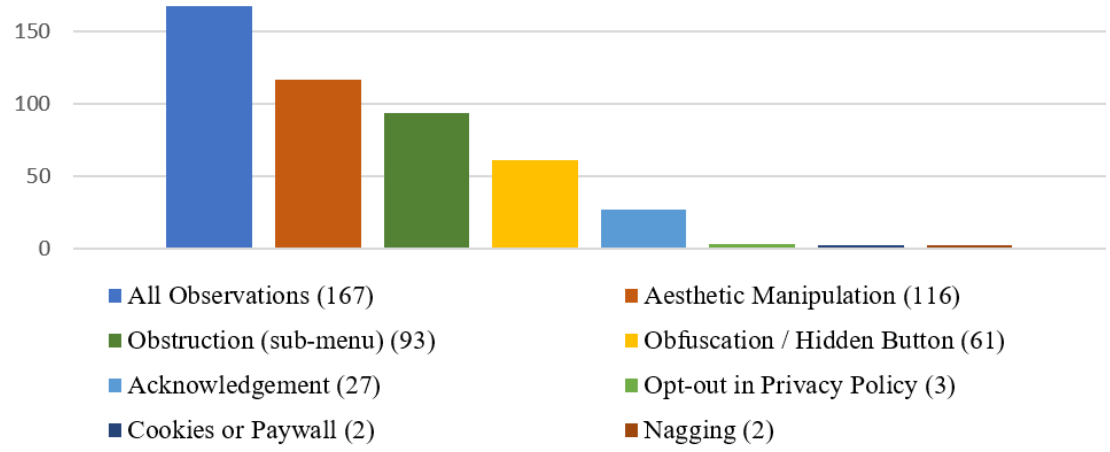
On the 14.05.2021 and 15.05.2021, these websites were categorized and individually evaluated:



Categories (167 Observations)

[27] As determined by their nominal GDP (IMF, 2020).
[28] Available under https://tinyurl.com/egbertsdata.

Out of these 167 websites, three did not contain Dark Patterns. The rest contained at least one, but most of the time several kinds of patterns. The results are indicated in the graph below.



Dark Patterns used in Cookie Banners, May 2021

Appendix 3 – Website Screenshots and Dummy Dataset (Table)

(www.onlinebehavior.net)

A: Overview of the website created to conduct the experiment

Landing Page

Information Sheet

Topic: Study on Behavior of Individuals Online

Researcher: Alexander Egberts

Contact Details: a.egberts@lumsastud.it

LUMSA University – Sede Pompeo Magno
EMLE Program
Via Pompeo Magno 28
00192 Roma

This is an invitation to take part in a study about human behavior in different online environments. Before you decide if you wish to take part, it is important for you to understand why the research is being done and what it will involve. Please take the time to read the following information carefully. If anything is unclear or if you have any questions, then please contact us using the details above before deciding whether to take part.

If you decide to participate, you will be asked to provide some basic demographic information. You will then be presented with several hypothetical scenarios and will be asked to indicate how you would decide within these scenarios. After that, you will be asked to respond to a few questionnaires about how much you value or know about different aspects of online environments. The whole procedure will last approximately 12 minutes. Please read and respond to the questions carefully, as you will not be able to alter your response once submitted.

Participation in this study is voluntary and you are under no obligation to take part. You are free to withdraw at any point before or during the study. All data collected will be anonymous, will be kept confidential and used for research purposes only. It will be stored in compliance with the General Data Protection Regulation.

If you have any questions or concerns, please do not hesitate to ask. We can be contacted at any time at the address stated above.

If you have any questions, please contact the researcher. Otherwise, if you

- Have read and understood this information sheet
- Understood that you are free to withdraw from this study at any time
- Give permission for your data from this study to be shared with other researchers provided that your anonymity is completely protected, and
- Agree to participate in this study

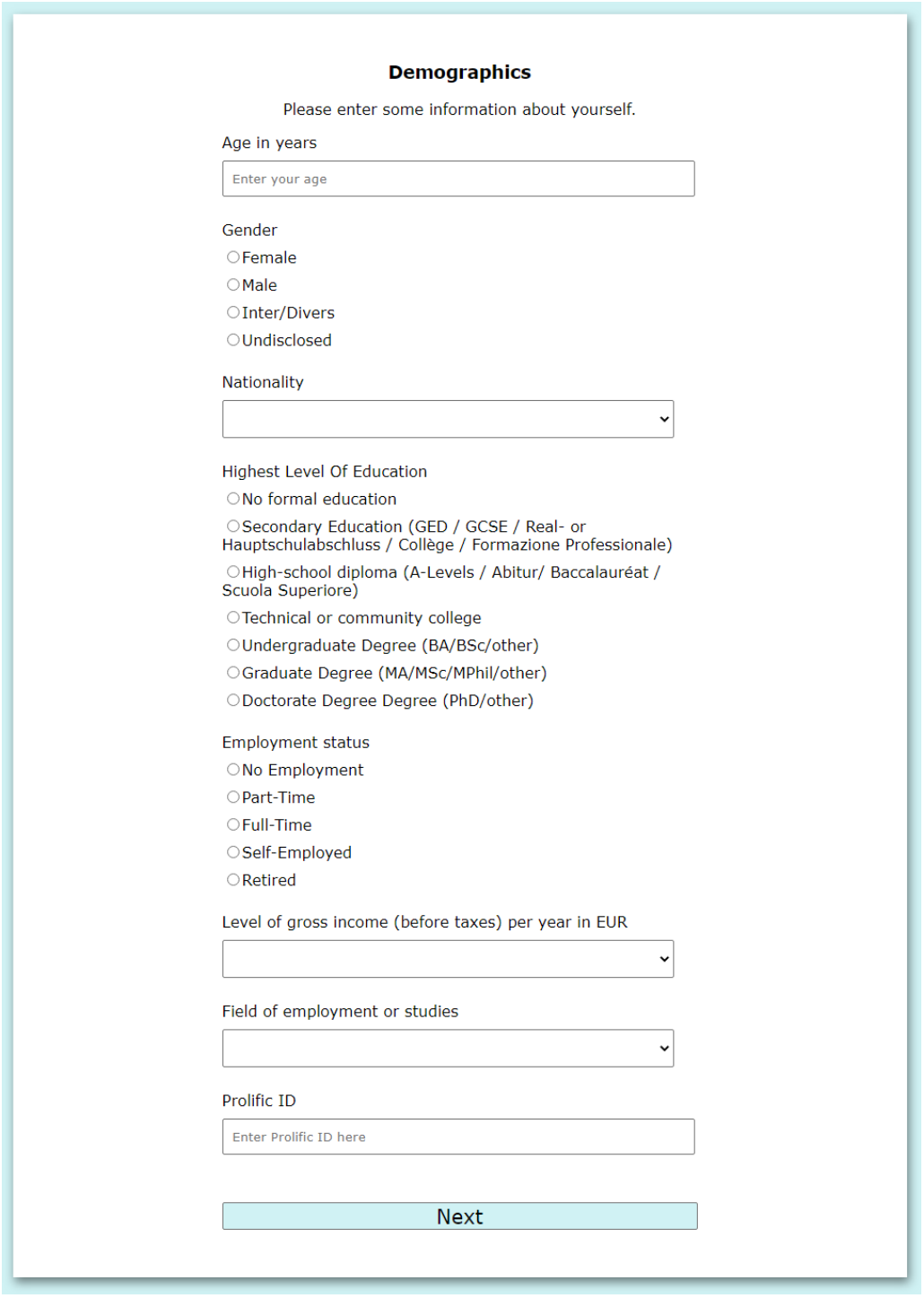
please indicate accordingly. If not, feel free to leave this website

○ I have read and understood the information above and agree to participate in the study

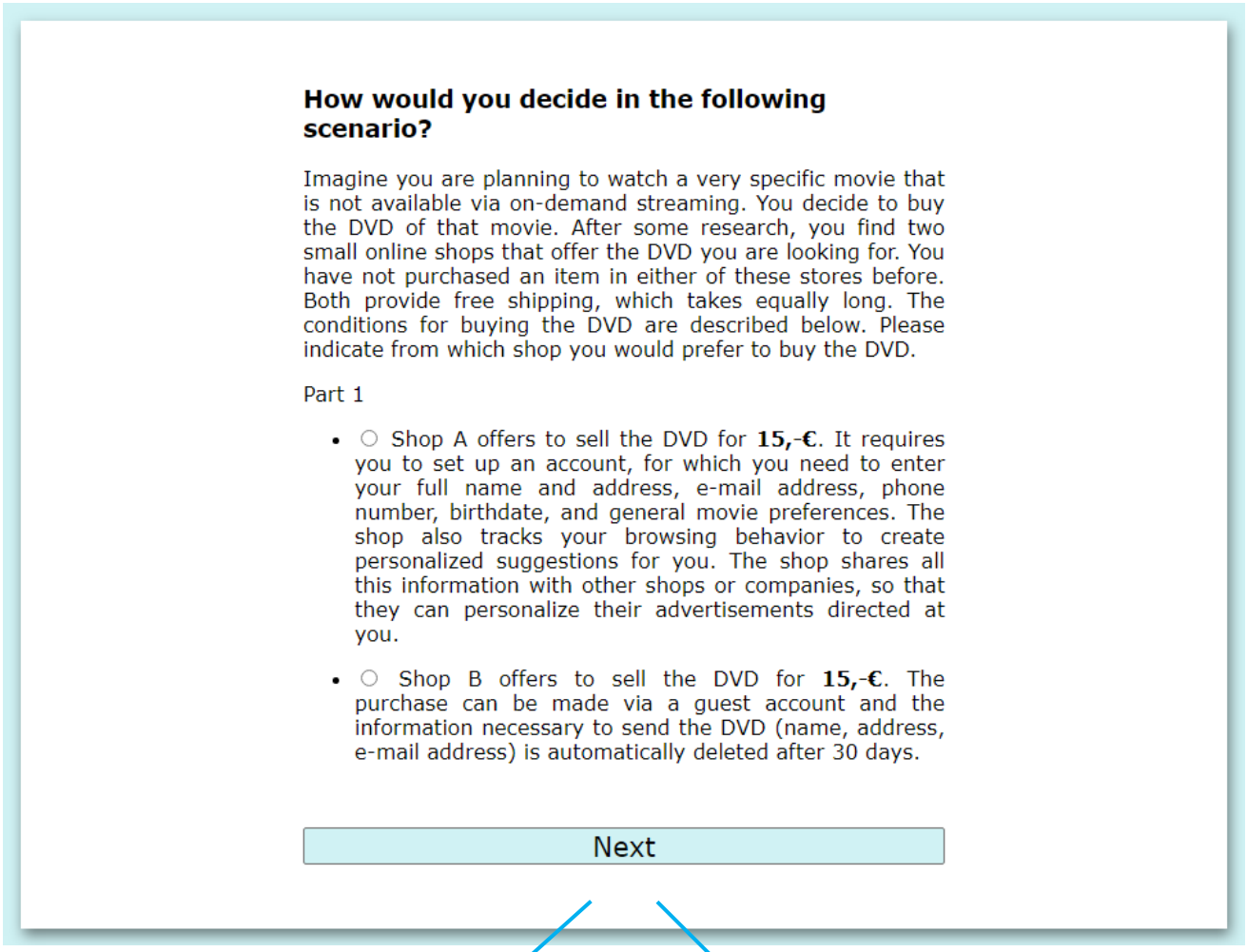
○ No, I don't want to participate and whish to leave this website

Next

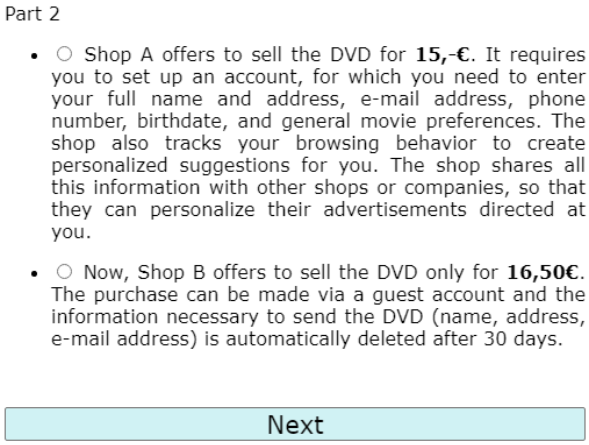
Demographics



WTP measured by MPL



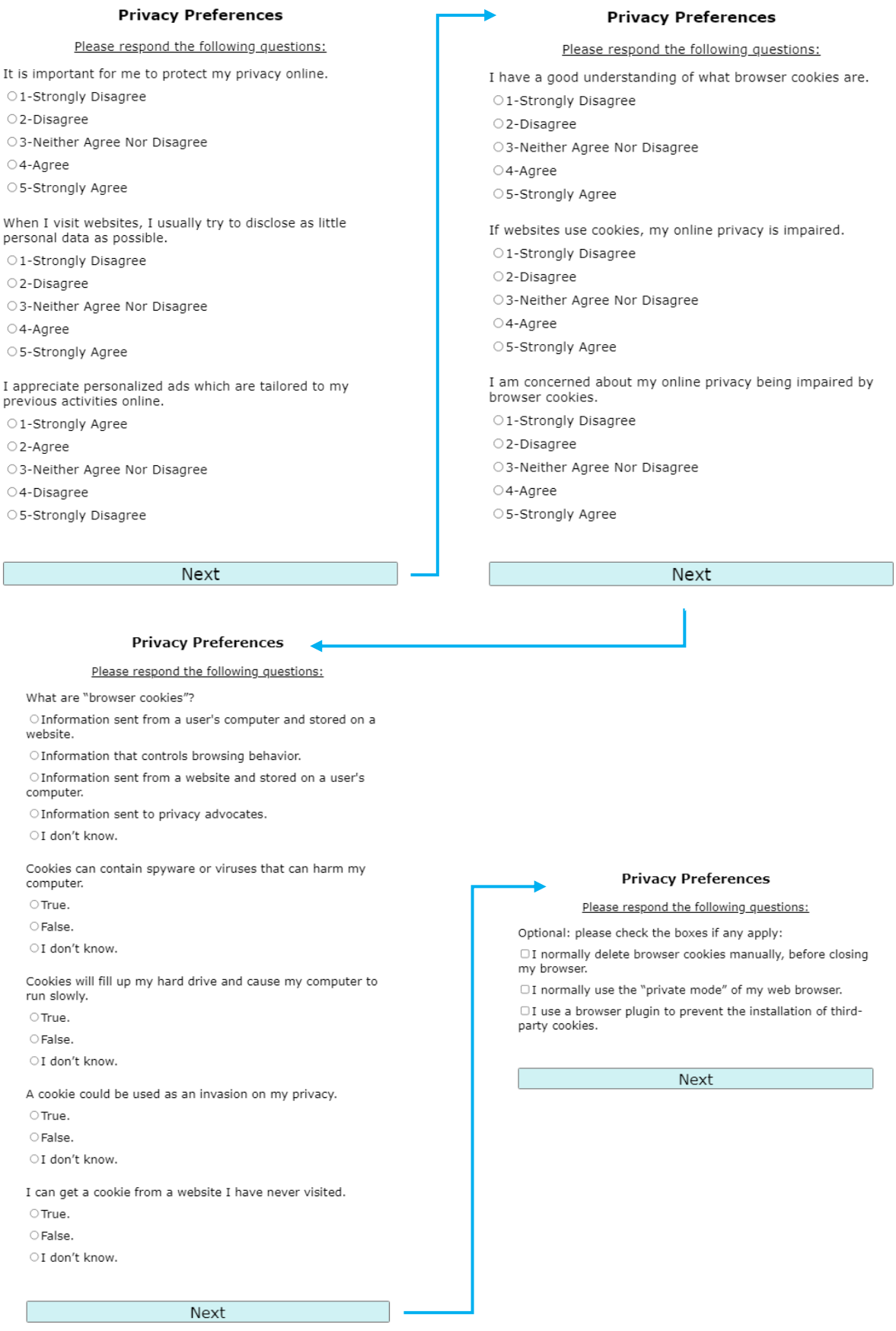
Choosing Shop B:



Whenever Shop B is chosen, the next part increases the price. This is repeated 10 times, in steps of 1,50 EUR.

As soon as Shop A is chosen, the user is forwarded to the next part.

Privacy Preferences



Information

Design Patterns in Cookie Banners

Dear participant,

Thank you for your time and attention so far – we are almost done! Please consider the following brief information about browser cookies and answer the questions on the next page.

Information about "browser cookies"

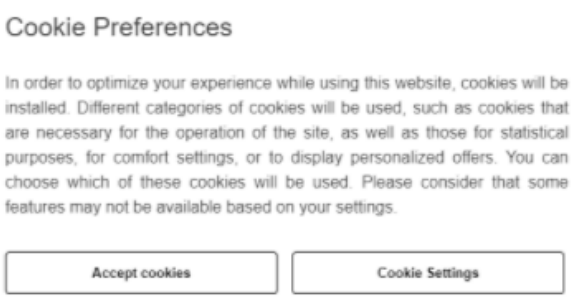
Cookies are small text-files that can be saved in your browser when visiting a website. They help the website to identify the user who is visiting. Some of these cookies are technically necessary for websites to work. For example, this survey must use a "functional cookie" to remember the answers given by each participant

Other cookies, so called "third-party cookies" are not technically necessary. But they can be used to increase the user experience on a website, for example by implementing elements from other websites, such as an embedded YouTube video. Other use cases include the gathering of analytical data or the personalization of advertisements

"Third-party cookies" can be used to track user behavior across different websites. Because of this, European Law (the General Data Protection Regulation) requires users to actively consent to the use of those cookies. This consent must be given "freely, unambiguous and on an informed basis". Therefore, many websites show cookies banners to users when they enter a website

Next

In the beginning of this survey, you have been presented with a cookie banner, that looked like this:



You have decided to "accept all cookies" . We want to inform you that no third-party cookies have been installed in your web browser, regardless of the choice you indicated.

Next

Perceived Difficulty (PDI)

You have decided to "accept all cookies" . We want to inform you that no third-party cookies have been installed in your web browser, regardless of the choice you indicated.

It was incomprehensible to select cookie settings.

- ○ 1-Strongly Disagree
- ○ 2-Disagree
- ○ 3-Neither Agree Nor Disagree
- ○ 4-Agree
- ○ 5-Strongly Agree

It was frustrating to select cookies settings.

- ○ 1-Strongly Disagree
- ○ 2-Disagree
- ○ 3-Neither Agree Nor Disagree
- ○ 4-Agree
- ○ 5-Strongly Agree

It was easy to select cookie settings.

- ○ 1-Strongly Agree
- ○ 2-Agree
- ○ 3-Neither Agree Nor Disagree
- ○ 4-Disagree
- ○ 5-Strongly Disagree

Next

Perceived Deception (PDE)

You have decided to "accept all cookies" . We want to inform you that no third-party cookies have been installed in your web browser, regardless of the choice you indicated.

This cookie banner is dishonest towards users.

- ○ 1-Strongly Disagree
- ○ 2-Disagree
- ○ 3-Neither Agree Nor Disagree
- ○ 4-Agree
- ○ 5-Strongly Agree

This cookie banner tries to make users select cookies which they do not want to install.

- ○ 1-Strongly Disagree
- ○ 2-Disagree
- ○ 3-Neither Agree Nor Disagree
- ○ 4-Agree
- ○ 5-Strongly Agree

This cookie banner uses a misleading design to make users select cookies which they do not want to install.

- ○ 1-Strongly Disagree
- ○ 2-Disagree
- ○ 3-Neither Agree Nor Disagree
- ○ 4-Agree
- ○ 5-Strongly Agree

Next

Regret (RE)

You have decided to "accept all cookies" . We want to inform you that no third-party cookies have been installed in your web browser, regardless of the choice you indicated.

I regret my choice of cookie settings.

- 1-Strongly Disagree
- 2-Disagree
- 3-Neither Agree Nor Disagree
- 4-Agree
- 5-Strongly Agree

In hindsight, I would change my cookies settings if it were possible.

- 1-Strongly Disagree
- 2-Disagree
- 3-Neither Agree Nor Disagree
- 4-Agree
- 5-Strongly Agree

I am satisfied with my choice of cookies settings.

- 1-Strongly Agree
- 2-Agree
- 3-Neither Agree Nor Disagree
- 4-Disagree
- 5-Strongly Disagree

Complete

Debriefing

Debriefing and Compensation

This is the end of the study, thank you very much for participating. In case of any further questions, please do not hesitate to contact the researcher at any given time.

Please follow the link provided below to obtain your compensation.

LINK WILL BE ADDED HERE.

Thank you once again and have a nice day!

Debriefing

Name of Researcher: Alexander Egberts

Email of Researcher: a.egberts@lumsastud.it

Title of the Study: Manipulation by Design – How Dark Patterns influence privacy choices

Background:

Dark Patterns are ubiquitous: deliberate website- or app-design design choices that aim to trick users into doing something which they did not intent to do initially. As recent studies show, their use us especially prevalent in cookie banners within the EU. While occasionally, specific Dark Patterns within cookie banners have been examined in terms of their effect in privacy choices, no study has directly compared to each other the influence of the most frequently occurring types of Dark Patterns. This study aims to expand the body of evidence by directly comparing the different consequences of different patterns and controlling for attributes that have been theorized to influence the effectiveness of their influence

Finish

B: Structure of Dataset (Dummy) to be produced by the experiment (output of website)

UserID	TimeStamp	Country	Banner Presented	Cookie Choice	Age	Gender	Education	Employee Stat	Gross Income	
1	06.07.2021 13:52	Germany	T1	1	43	male	5	Full-Time	60.000 - 64.999	
2	06.07.2021 13:55	France	T2	3	26	female	4	Part-Time	40.000 - 44.999	
3	06.07.2021 13:57	Italy	B	2	31	male	2	Self-Employed	30.000 - 34.999	
4	06.07.2021 13:59	Germany	T3	1	18	inter/divers	3	Employment	less than 5.000	
5	06.07.2021 14:00	Italy	T3	3	37	female	6	Full-Time	55.000 - 59.999	
...	...	...	...	...	...	...	...	...	...	...

1 - all cookies Rejected

2 - Some cookies accepted in settings

3 - All cookies accepted

--> Code 1 & 2 as "1": active decision made. Code 3 as "0": no active decision made.

Coded on a scale:
1: No formal education; 7: PhD

Field of Employment	ProlificID	MPL0	MPL1	MPL2	MPL3	MPL4	MPL5	MPL6	MPL7	MPL8	MPL9	MPL10	Privacy1	Privacy2	Privacy3
Law Politics & Government	xxxxxxxxx	B	B	A	-	-	-	-	-	-	-	-	4	4	5
IT & Digital	xxxxxxxxx	B	B	B	A	-	-	-	-	-	-	-	5	5	4
Engineering	xxxxxxxxx	A	-	-	-	-	-	-	-	-	-	-	4	3	4
Student	xxxxxxxxx	B	A	-	-	-	-	-	-	-	-	-	5	5	5
Sport Leisure & tourism	xxxxxxxxx	B	B	B	B	B	B	A	-	-	-	-	5	5	3
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

...

Code according to the willingness to pay, dependent on where "A" was chosen:

MPL0 = 0; MPL1 = 1,5; MLP2 = 3; MPL3 = 4,5; MPL4 = 6; MPL5 = 7,5; MPL6 = 9; MPL7 = 10,5; MPL8 = 12; MPL9 = 13,5; MPL10 = 15

Code as average: Self-assessed Privacy Preference 1,0 - 5,0

Opinion1	Opinion2	Opinion3	Quiz1	Quiz2	Quiz3	Quiz4	Quiz5	Optional: measures	PDI1	PDI2	PDI3	PDE1	PDE2	PDE3	RE1	RE2	RE3
3	3	3	0	0	0	1	0	0,0,0	2	2	2	3	4	4	2	2	5
5	3	2	1	1	1	1	1	1,1,1	4	4	4	5	5	5	4	5	4
2	3	4	0	0	0	0	0	0,1,0	2	4	3	2	2	2	2	2	3
4	3	4	1	0	1	1	0	0,0,1	4	4	4	3	3	4	3	4	3
2	4	3	0	0	0	1	1	0,0,0	4	4	5	4	4	3	5	4	5
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Code as average: perceived "danger" from cookies 1,0 - 5,0

Summarize "points" achieved by subjects: 0 - 5. The higher, the more factual knowledge about cookie banners.

Indicates technical measures used against cookies; might alter approach to banners

Code as average: perceived difficulty 1,0 - 5,0

Code as average: perceived deception 1,0 - 5,0

Code as average: user regret 1,0 - 5,0

Page intentionally left blank

References

Acquisti, A., Rylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54*(2), 442-492.

Alemanno, A., & Spina, A. (2014). Nudging legally: On the checks and balances of behavioral regulation. *International Journal of Constitutional Law, 12*(2), 27.

Arkes, H. R., & Ayton, P. (1999). The Sunk Cost and Concorde Effects: Are humans less rational than lower animals? *Psychological Association, 125*(5), 591-600.

Arrow, K. J. (1985). The Potentials and Limits of the Market in Resource Allocation. In G. Feiwel (Ed.), *Issues in Contemporary Microeconomics and Welfare* (pp. 107-124). London: Macmillan Press.

Bar-Gill, O. (2007). The Behavioral Economics of Consumer Contracts. *Minnesota Law Review, 92*(3), 749-803.

Bar-Gill, O. (2014). Consumer Transactions. In E. Zamir, & D. Teichman (Eds.), *The Oxford Handbook of Behavioral Economics and the Law* (pp. 465-490). Oxford (UK), New York City, USA: Oxford University Press.

Bator, F. M. (1958). The Anatonmy of Market Failure. *The Quarterly Journal of Economics, 72*(3), 351-379.

German Federal Court (BGH). (2020, May 28). "Cookie-Einwilligung II", I ZR 7/16. https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html.

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher. (2016). Tales from the Dark Side: Privacy Dark Strategies. *Proceedings of the Privacy Enhancig Technologies, 2016*(4), 237–254. https://doi.org/10.1515/popets-2016-0038.

Brebner, S., & Sonnemans, J. (2018). Does the elicitation method impact the WTA/WTP disparity? *Journal of Behavioral and Experimental Economics, 73*, 40-45.

Brignull, H. (2010, July 8). *Dark Patterns: dirty tricks designers use to make people do stuff*. 90 Percet of Everything. Retrieved June 8, 2021, https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/

Brignull, H. (n.d.). *Types of Dark Pattern*. Darkpatterns.org. Retrieved June 8, 2021, from https://www.darkpatterns.org/types-of-dark-pattern.

Bursztyn, L., & Jensen, R. (2017). Social Image and Economic Behavior in the Field: Identifying, Understanding and Shaping Social Pressure. *Annual Review of Economics, 9*, 131-153.

Californian State Law. (2018). *California Consumer Privacy Act (CCPA)*. Californian State Legislature. Retrieved July 27, 2021 from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Cooter, R. J., & Ulen, T. (2014). *Law and Economics* (6th ed.). Essex (UK): Pearson Education.

U.S. Senate Bill 1084, 116th Congress. (2019). *Deceptive Experiences To Online Users Reduction (DETOUR) Act*. U.S. Congress. Retrieved May 15, 2021 from https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, USA)*. https://doi.org/10.1145/3313831.3376600.

European Court of Justice (ECJ). (2015, December 17). "Neptune", C-157/14. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-157/14.

European Court of Justice (ECJ). (2017, December 20). "Polkomtel", C-277/16. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-397/14.

European Court of Justice (ECJ). (2019, July 29). "Fashion ID", C-40/17. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-40/17.

European Court of Justice (ECJ). (2019, October 1). "Planet49", C-673/17. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-673/17.

European Court of Justice (ECJ). (2020, July 7). "Citroën Commerce", C-476/14. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-476/14.

European Data Protection Board (EPDB). (2020). *Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default*. Independent European Body. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

European Commission (Jourová, M.). (2019, April 11). *Parliamentary Questions to the European Commission*. Retrieved June 17, 2021 from https://www.europarl.europa.eu/doceo/document/E-8-2019-000774-ASW_EN.html.

European Commission. (2021, April 29). *Questions and Answers on the Better Regulation Communication*. Retrieved June 5, 2021 from https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1902.

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

Hanson, J. D., & Kysar, D. A. (1999). Taking Behavioralism Seriously: The Problem of Market Manipulation. *N.Y.U. Law Review, 74*(3), 630-749.

Hern, A. (2014, February 5). *Why Google has 200m reasons to put engineers over designers*. The Guardian. Retrieved June 24, 2021 from https://www.theguardian.com/technology/2014/feb/05/why-google-engineers-designers.

(den) Hertog, J. (2012). Economic theories of regulation. In R. Van den Bergh, & A. Pacces (Eds.), *Regulation and Economics* (pp. 25-95). Cheltenham (UK): Edward Elgar Publishing.

Hinz, A., Michalski, D., Schwarz, R., & Yorck Herzberg, P. (2007). The acquiescence effect in responding to a questionnaire. *GMS Psycho-Social-Medicine, 4*, 1-9.

International Monetary Fund (IMF). (2020). *World Economic Outlook Database.* IMF Website. Retrieved June 10, 2021 from https://www.imf.org/en/Publications/WEO/weo-database/2020/October/weo-report.

Jacquemet, N., & L'Haridon, O. (2018). *Experimental Economics - Methods and Applications* (1st ed.). Cambridge (UK), New York City (USA): Cambridge University Press.

Kahneman, D. (2011). *Thinking, Fast and Slow* (1st ed.). New York City (USA): Farrar, Straus and Giroux Publishing.

Kaplow, L. (1992). Rules versus Standards: An Economic Analysis. *Duke Law Journal , 42*(3), 557-629.

Lang, K., & Lang, G. E. (1984). The Impact of Polls on Public Opinion. *The Annals of the American Academy of Political and Social Science , 472*, 129-142.

Leiser, M. R. (2020). *'Dark Patterns': The Case for Regulatory Pluralism* [Preprint Publication]. Retrieved June 24, 2021 from https://osf.io/preprints/lawarxiv/ea5n2/.

Loewenstein, G., & Thaler, R. H. (1989). Anomalies: Intertemporal Choice. *The Journal of Economic Perspectives, 3*(4), 181-193.

Luguri, J., & Strahilevitz, L. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis, 13*(1), 67.

Luppi, B., & Parisi, F. (2011). Rules versus Standards. In G. De Geest (Ed.), *Encyclopedia of Law and Economics, Volume 7: Production of Legal Rules* (pp. 43-53). Gloucestershire (UK): Edward Elgar Publishing.

Machuletz, D., & Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings of the Privacy Enhancing Technologies, 2020*(2), 481-498. https://doi.org/10.2478/popets-2020-0037.

Martini, M., Drews, C., Seeliger, P., & Weinzierl, Q. (2021). Dark Patterns - Phänomenologie und Antworten der Rechtsordnung. *Zeitschrift für Digitalisierung und Recht , 1*(1), 47-74.

Mathis, K., & Steffen, A. D. (2015). From Rational Choice to Behavioral Economics. In K. Mathis (Ed.), *European Perspectives on Bheavioral Law and Economics* (pp. 31-50). Heidelberg (Germany): Springer International Publishing.

Mathur, A., Acar, G., Friedman, M. J., Mayer, J., Chetty, M., & Naraxanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*. 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. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan).* https://doi.org/10.1145/3411764.3445610.

Moser, C., Schoenebeck, S. Y., & Resnick, P. (2019). Impulse Buying: Design Practices and Consumer Needs. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Glasgow, UK).*

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. Proceed*ings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, USA).* https://doi.org/10.1145/3313831.3376321.

noyb. (2021, May 31). *NOYB aims to end "cookie banner terror" and issues more than 500 GDPR complaints.* Noyb website. Retrieved June 1, 2021 from https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints.

PrivacyPolicies. (2021). *What Are Cookies?*. Privacypolicies.com. Retrieved May 29, 2021 fromhttps://www.privacypolicies.com/blog/cookies/

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications, 10*(3069), 1-9.

Román, S. (2007). The Ethics of Online Retailing: A Scale Development and Validation from the Consumers' Perspective. *Journal of Business Ethics, 72*(2), 131-148.

Rose-Ackerman, S. (1998). Progressive Law and Economics - And the New Administrative Law. *Yale Law Journal*, *98*(2), 341-368.

Samuelson, W., & Zeckhauser, R. (1988). Status Quo Bias in Decision Making. *Journal of Risk and Uncertainty* , *1*(1), 7-59.

Santos, C., Bielova, N., & Matte, C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners [Under Review]. *Technology and Regulation, Tilburg University*, 91-135. Retrieved June 9, 2021 from https://hal.inria.fr/hal-02875447v2.

Scammon, D. (1977). "Information Load" and Consumers. *Journal of Consumer Research, 4*(3), 148-155.

Schwartz, A. (2015). Regulating for Rationality. *Stanford Law Review*, *67*(6), 1373-1410.

Schwarz, N., Strack, F., & Mai, H.-P. (1991). Assimilation and contrast effects in part-whole question sequences: a conversational logic analysis. *Public Opinion Quarterly*, *55*(1), 3-23.

Shaw, S. (2019, June 12). *Consumers Are Becoming Wise to Your Nudge.* The Behavioral Scientist. Retrieved June 9, 2021 from https://behavioralscientist.org/consumers-are-becoming-wise-to-your-nudge/.

Sibony, A.-L. (2014). Can EU Consumer Law Benefit from Behavioural Insights? An Analysis of the Unfair Practices Directive. *European Review of Private Law, 22*(6), 901-942.

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by Design - Dark Patterns in Cookie Consents for Online News Outlets. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (Tallinn, Estonia)*. https://doi.org/10.1145/3419249.3420132.

Straetmans, G. (2016). Misleading practices, the consumer information model and consumer protection. *Journal of European Consumer and Market Law, 5*(5), 199-210.

Strahilevitz, L., Cranor, L. F., Marotta-Wurgler, F., Mayer, J., Ohm, P., Strandburg, K., . . . Verstraete, M. (2019). *Subcommittee Report: Privacy and Data Protection.* Stigler Center Committee for the Study of Digital Platforms. Retrieved June 12, 2021 from https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf.

Teichman, D., & Zamir, E. (2014). Judicial Decision Making. In E. Zamir, & D. Teichman (Eds.), *The Oxford Handbook of Behavioral Economics and the Law* (pp. 664-702). Oxford (UK): Oxford University Press.

Testori Coggi, P. (2012, June 13). *Behavioural insights in the Commission.* Politico. Retrieved June 28, 2021 from www.politico.eu: https://www.politico.eu/article/behavioural-insights-in-the-commission/.

Thaler, R. (2018). Nudge, not sludge. *Science, 361*(6401), 1.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness* (1st ed.). New Haven (USA): Yale University Press.

Tversky, A., & Kahneman, D. (1973). Availability: A Heuristic for Judging Frequency and Probability. *Cognitive Psychology, 5*(2), 207-232.

Tversky, A., & Kahnemann, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4481), 453-458.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (London, UK).* https://doi.org/10.1145/3319535.3354212.

Bundesverband Verbraucherzentrale. (2021, February 2). *Wahlfreiheit für Nutzer in digitalen Märkten sicherstellen.* Retrieved June 17, 2021 from https://www.vzbv.de/sites/default/files/2021-05/21-05-04_vzbv_Position_Paper_DMA_ENG.pdf.

Webster, J. G. (2014). *The Marketplace of Attention - How Audiences Take Shape in a Digital Age* (1st ed.). Cambridge (USA); London (UK): The MIT Press.

Weinzierl, Q. (2020). Dark Patterns als Herausforderung für das Recht - Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien. *Neue Zeitschrift für Verwaltungsrecht – Extra, 39*(15), 1-11.

Welsh, M. (2021). *Cookie Quiz*. Priority Learning. Retrieved June 7, 2021 from https://www.prioritylearningresearch.com/articles/cookie_quiz.php.

Wendehorst, C. (2019). Commentary on § 312a German Civil Code. In F. J. Säcker, R. Rixecher, H. Oetker, & B. Limper (Eds.), *Münchner Kommentar zum BGB* (3). Munich (Germany): C.H.Beck Publishing.

Wilkinson, T. M. (2013). Nudging and Manipulation. *Political Studies, 61*(2), 16.

Worchel, S., Lee, J., & Adewole, A. (1975). Effects of Supply and Demand on Ratings of Object Value. *Journal of Personality and Social Psychology, 32*(5), 906-914.

Yablonski, J. (2020). *Laws of UX - Using Psychology to Design Better Products & Services* (1st ed.). Sebastopol (USA): O'Reilly Media.

Authorship Declaration

I hereby declare and confirm that this thesis is entirely the result of my own work except where otherwise indicated. I acknowledge the supervision and guidance I have received from Professor Fabiana Di Porto. This thesis is not used as part of any other examination and has not yet been published.

Rome, the 11.08.2021

Alexander Egberts, M.A.