Learning from the Dark Side about How (Not) to Engineer Privacy: Analysis of Dark Patterns Taxonomies from an ISO 29100 Perspective

Philippe Valoggia[1][a], Anastasia Sergeeva[2][b], Arianna Rossi[3][c] and Marietjie Botes[4][d]

[1] *ITIS, Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg*

[2]*DBCS, University of Luxembourg, Esch-sur-Alzette, Luxembourg*

[3]*LIDER Lab, Sant'Anna School of Advanced Studies, Pisa, Italy*

[4]*University of KwaZulu Natal, South Africa*

Keywords: Privacy Principles; Dark Patterns, Privacy Engineering, ISO/IEC 29100:2011

Abstract: The privacy engineering literature proposes requirements for the design of technologies but gives little guidance on how to correctly fulfil them in practice. On the other hand, a growing number of taxonomies document examples of how to circumvent privacy requirements via "dark patterns," i.e., manipulative privacy-invasive interface designs. To improve the actionability of the knowledge about dark patterns for the privacy engineering community, we matched a selection of existing dark patterns classifications with the ISO/IEC 29100:2011 standard on Privacy Principles by performing an iterative expert analysis, which resulted in clusters of dark patterns that potentially violate the ISO privacy engineering requirements. Our results can be used to develop practical guidelines for the implementation of technology designs that comply with the ISO Privacy Principles.

1 INTRODUCTION

Privacy-by-design is increasingly recognized as the standard approach in ICT system engineering. Still, developers face challenges when they translate high-level privacy requirements into specific implementation solutions at a fine-grained level (Huth and Matthes, 2019) in software applications. These privacy requirements must be refined to a granular level that corresponds to the systems' functionalities and that can, at the same time, be easily matched with the legal requirements that must be respected in the design of technologies that process personal information (Sangaroonsilp et al., 2023). There is a recognized need for a unified privacy requirements implementation procedure that is able to translate legal provisions, such as those of the General Data Protection Regulation, and international standards, such as the ISO/IEC 29100:2011 Privacy framework (ISO/IEC 29100:2011, 2011), into practical applications (Sangaroonsilp et al., 2023; Anthonysamy et al., 2017; Martin and Kung, 2018). To address this gap, multiple privacy implementation frameworks have been developed (e.g.,(Mead and Stehney, 2005; Deng et al., 2011)); however, most of them currently offer broad guidelines without sufficient practical examples of effective practices, thereby leaving developers unsure on whether their design choices are in conformity with standards and in compliance with applicable regulations. Simultaneously, various taxonomies of design practices have emerged that can be regarded as counterexamples of privacy-enhancing practices, also known as dark patterns or deceptive design patterns. These taxonomies collect and describe privacy-invasive interface design solutions that intuitively contradict well-established privacy standards. However, a direct link between the two has never been established.

Dark patterns in user interfaces can be considered one of the main obstacles to the ethical design of technologies that respect user preferences and interests and that uphold consumer rights and data protection rights. In general, they can be described as manipulative design instances created to ignore the user's best interests in favor of the interests of the business employing them, such as revenue. Academic scholars, practitioners, and supervisory authorities have developed multiple taxonomies of dark patterns to account for such phenomenon (e.g.(Gray et al., 2018; Bösch et al., 2016; Jarovsky, 2022; Conti and Sobiesk, 2010; Zagal et al., 2013). Still, no consensus exists about their exact definition and systematization,

[a] https://orcid.org/0000-0002-4294-0848
[b] https://orcid.org/0000-0003-3701-3123
[c] https://orcid.org/0000-0002-4199-5898
[d] https://orcid.org/0000-0002-6613-6977

even though recent attempts have tried to unify the existing knowledge to create a common, reliable, interoperable vocabulary (Gray et al., 2023b). In the present article, we analyze a selection of the current taxonomies of dark patterns by matching them with the privacy principles defined in ISO 29100 (ISO/IEC 29100:2011, 2011). Namely, we leveraged the diversified expertise of a focus group to group such dark patterns based on the ISO privacy principle(s) they are likely to violate. We found that dark patterns are likely to violate, in order of frequency, the following privacy principles: ”Consent and choice,” ”Openness, transparency and notice,” ”Data minimization,” ”Use, retention and disclosure limitation,” and ”Purpose legitimacy and specification”. Our discussion focuses on how our findings can be transformed into actionable recommendations for privacy engineers and product developers, that can be useful also for auditors and certification bodies that perform conformity checks.

2 RELATED WORK

2.1 The ISO/IEC 29100 Privacy Framework

Among the various existing ISO standards related to privacy and personal data, ISO/IEC 29100:2011 is the privacy framework that provides guidance for handling personal information in Information and Communication Technology systems (ISO/IEC 29100:2011, 2011) by establishing a set of privacy principles that govern various activities related to the processing of personal data, such as their collection, storage, use, transfer, and disposal. Translating legal obligations and standards into specific privacy requirements for software systems is a well-recognized challenge for software engineers(Sangaroonsilp et al., 2023). Organizations currently adhere to two sources of regulation: legal frameworks and standards (Antignac et al., 2016). The first ones are determined by lawmakers and differ across countries of jurisdiction, while the latter are established by the industry through consensus procedures and incorporate widely accepted best practices across national boundaries. Compared to the legal frameworks, industrial standards offer two advantages in the analysis of the privacy aspects of a system design: they align closely with industry perspectives, rather than policymakers’, and are not dependent on the legislation of different countries (Antignac et al., 2016).

Therefore, we have decided to consider the eleven privacy principles outlined in the ISO/IEC 29100:2011 standard: ”Consent and choice,” ”Purpose legitimacy and specification,” ”Collection limitation,” ”Data minimization,” ”Use, retention, and disclosure limitation,” ”Accuracy and quality,” ”Openness, transparency, and notice,” ”Individual participation and access,” ”Accountability,” ”Information security,” ”Privacy compliance.” Each principle is decomposed into a fixed and mandatory set of goals (i.e., the privacy requirements).

2.2 Dark Patterns Taxonomies

Dark patterns can be used for various purposes on online services, such as to make consumers spend more money or share more personal data than necessary, benefiting businesses that employ them. Dark patterns have become a growing concern over the last ten years because they can harm users in various manners, particularly those less experienced with technology (Goodstein, 2021; Gray et al., 2018; Luguri and Strahilevitz, 2021; Chamorro et al., 2022). To address the problem, scholars have proposed various methods to mitigate and eliminate the effects of dark patterns (Rossi and Bongard-Blanchy, 2021). Some approaches address the ”human side” of dark patterns, focusing on raising awareness in users and designers about the harmful effects of dark patterns use (Rossi and Bongard-Blanchy, 2021; Fansher et al., 2018; Bongard-Blanchy et al., 2021) and offer alternative ”fair patterns” or ”bright” patterns (e.g (Graßl et al., 2021)). Other approaches are geared toward the engineering community and aim to develop applications that detect and flag dark patterns in user interfaces (Kollnig et al., 2021; Curley et al., 2021; Mathur et al., 2019; Hasan Mansur et al., 2023). However, both approaches require a well-established and feature-based classification of dark patterns. Several different researchers and organizations have proposed their own taxonomies for dark patterns (e.g.(Gray et al., 2018; Mathur et al., 2021; Bösch et al., 2016; Zagal et al., 2013; Greenberg et al., 2014; NCC, 2018; CNIL, 2019; EDPB, 2022)); Some taxonomies focus on the high-level intention behind dark pattern designs or their overarching attributes that distinguish them from legitimate design patterns (Gray et al., 2018; Mathur et al., 2021), while others focus on specific tactics or techniques that are employed(Conti and Sobiesk, 2010; Bösch et al., 2016). Some pattern catalogues are domain-specific, such as those for online shopping(Mathur et al., 2019) or video gaming (Zagal et al., 2013); it is also possible to create a taxonomy for a specific type of interface (Di Geronimo et al., 2020). Often, different terms are used to designate the same deceptive design pattern. Moreover, some practices could be discussed within the legal framework of consumer protection (BEUC, 2022), while others are rather related to data protection (EDPB, 2022). As a result of this divergent phase of classification, the interdisciplinary community experiences confusion and disagreement about what constitutes a dark pattern and how it should be classified. Recent efforts are made to establish a standard set of categories and definitions (Gray et al., 2023b; Gray et al., 2023a; Gray et al., 2023c); however, this is still an ongoing process with continuous evolution.

Dark patterns are a threat to users' privacy (Gunawan et al., 2022) since they can, for example, manipulate users into agreeing to privacy terms that are not in their best interests (Bösch et al., 2016) or nudge them to share more personal data than intended (Jarovsky, 2022). The various data privacy implications of dark patterns have been discussed both in the user experience (Gray et al., 2018; Habib et al., 2019) and legal(Matte et al., 2020; Santos et al., 2021; Gray et al., 2021; Jarovsky, 2022; Martini et al., 2022; Gunawan et al., 2022; EDPB, 2022) domains, resulting in a series of legislative and recommendation initiatives(Voigt and Von dem Bussche, 2017; CNIL, 2019; CPRA, 2020; EDPB, 2022). In the present paper, we go beyond the state of the art by deliberately focusing on the privacy risks created by implementing dark patterns in ICT systems by recurring to the ISO/IEC 29100 Privacy Principles framework.

3 RATIONALE AND RESEARCH QUESTION

Except for (Bösch et al., 2016; Jarovsky, 2022; CNIL, 2019; EDPB, 2022; Kitkowska, 2023), most existing taxonomies do not focus solely on privacy-invasive deceptive design patterns that may violate data protection obligations. They rather have a broader scope and usually include only a few examples of categories threatening users' privacy. Hence, they do not constitute off-the-shelf solutions for privacy-focused systematic evaluations of ICT systems.

Moreover, the existing taxonomies seem to focus on infringements of the General Data Protection Regulation (GDPR)'s data protection requirements, which inherently constrains their applicability primarily to the European Union's context. In contrast, international organizations often operate within a framework of multiple standards and guidelines. For those already compliant with global benchmarks like ISO/IEC 27001 for information security management, there is an inherent ease in integrating ISO/IEC 29100 principles, given the synergy between their structures and requirements. To address this gap and conduct a comprehensive analysis of current dark pattern categories and examples concerning potential privacy violations, we have sought to answer the following research question: **Which of the privacy principles provided by the ISO 29100 International Standard are most frequently violated by the dark patterns presented in existing taxonomies?**

4 METHODOLOGY

First, to collect dark patterns classifications from existing literature, we scanned through the most well-known research databases (ACM Digital Library, Google Scholar, ScienceDirect) by the keywords ”dark patterns” and ”deceptive patterns.” We largely based our list on the previous work in taxonomy's analysis (Mathur et al., 2021) and updated the list with taxonomies from our search. We excluded the experimental papers and focused on the papers that addressed the problem of classifying dark patterns. We included the non-academic publication of Harry Brignul, presented on his website (Brignull, 2022), as this classification is widely used within the academic community. We also added to the analysis the reports and guidelines issued by the regulatory bodies (BEUC, 2022; CNIL, 2019; EDPB, 2022). As some of the taxonomies were re-elaborations of existing ones and some categories were overlapping, we merged several dark pattern definitions. We also consider separately the categories and subcategories of EDPB guidelines (EDPB, 2022). The final body of analysis included a list of 98 dark patterns out of 13 taxonomies. The list of taxonomies used for the analysis is presented in the APPENDIX.

Second, Authors 1 and 2 gathered a group of four experts in data protection law and computer science who have expertise on dark patterns (including authors 3 and 4), to whom they sent the list of dark pattern definitions and a short presentation containing the ISO 29100 privacy principles. The experts were asked to identify if the first 25 dark patterns' definitions from the list represented a lack of conformity with the privacy principles, with a maximum of two principles per definition. Experts could also consider the definition to be not related to any privacy problem. Then, Authors 1 and 2 leveraged their expertise in conducting focus groups and privacy engineering to organize two 2-hour focus groups with the experts to discuss the differences between the various experts' attributions and reach an agreement where there were none.

This was pivotal in establishing and clarifying the criteria for which deceptive pattern categories should be assigned to certain privacy principles, which the experts then used to code the rest of the definitions.

Third, Authors 1 and 2 merged the experts' results, proposed the final attribution, and asked for expert feedback. Then, they discussed the experts' feedback about the final classification to ensure the method's robustness and to address disagreements between the experts. Overall, the experts co-developed two main guiding strategies:

1. Law-agnosticism. Many of the ISO 29100 privacy principles are closely related to the foundational data protection principles enshrined by the GDPR, although there are relevant differences. Hence, the analysis was carried out by deliberately ignoring the GDPR's principles, which could have led the experts astray, even though knowledge of the GDPR was important to reflect on the nuances of the ISO principles and underline the differences between the two to obtain a reliable matching.

2. Interpretation of Immediate Threats and Consequences. The experts acknowledged that certain definitions of dark patterns focused on the resulting effect on users (e.g., "Automating the user away"), whilst others described the functioning mechanisms of the dark pattern (e.g., "Interruption"). The latter group of patterns was excluded because it lacked exclusive privacy-related consequences.

Fourth, Author 1 and 2 engaged in multiple rounds of discussion with experts to resolve disagreements and create a reliable classification. The pre-final version of the classification was shared with the experts. The full cycle of expert analysis and discussion took three months. The presented analysis was finalized in April 2023.

5 FINDINGS

We first provide an overview of the results of the analysis (a graphical representation of findings is presented in Figure 1) and then provide more granular information about each privacy principle.

The principle that is violated by most dark patterns in our analysis (near 39% of analyzed patterns) is "*Consent and choice*," where dark patterns are likely to violate the conditions for the validity of consent: the "user's choice" must be freely given, specific, and informed. Note that the user's choice can have a broader meaning than consent as one of the legal bases under the GDPR, since it can also refer to other kinds of data controls that users can use (e.g., app permissions). Practices that pressure users to make a choice or provide inadequate information about handling personal data based on that choice are likely to threaten the validity of consent and choice. This principle additionally concerns the need for "clear, prominent, easily understandable, accessible, and affordable mechanisms to exercise choice and give consent regarding the processing." Some deceptive design patterns hide controls or offer deceptive, cumbersome affordances, making it hard or even impossible for users to manage their privacy settings. The second privacy principle most targeted by dark patterns is "*Openness, transparency, and notice*" (near 30% of all analyzed patterns). It refers to the obligation to provide users with clear and easily accessible information about the policies, procedures, and practices regarding data processing to enable them to make informed decisions. The third privacy principle is "*Individual participation and access*" (near 16% of patterns): adhering to this principle means equipping individuals with "the ability to access and review" their personal information. It is also necessary to implement organizational and/or technical measures that enable users "to exercise these rights in a simple, fast, and efficient manner, without undue delay or cost." Dark patterns can hinder people from exercising their data rights by adding unnecessary friction that raises the costs of performing certain actions.

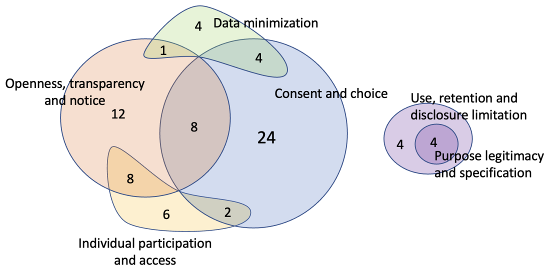

Figure 1: The distribution of the analyzed dark patterns across the various privacy principles that they are likely to violate. Overlapping areas indicate those dark patterns that may infringe two principles

In this study, requirements related to the fourth principle, "*Collection limitation*," were merged with the requirements of the "*Data minimization*" principle to ease their assessment (in sum near 9% of analyzed patterns). Dark patterns that pose a risk to these principles aim to encourage users to share more personal data than necessary to achieve the processing purpose, for example, by presenting privacy-invasive default options.

The last two privacy principles that are likely to be violated are "*Use, retention and disclosure limitation*" and "*Purpose legitimacy and specification*" (the same 4% of analyzed patterns): the former concerns those design practices that aim at collecting and retaining personal data for longer than necessary, while the latter is about adequately selecting and communicating the purpose of processing. The analysis also showed that nearly 32% of the dark patterns under examination do not pose any direct risk to privacy. Among those that do, at first sight, none seems to show non-conformity with the privacy principles of ”*Accuracy and quality*,” ”*Accountability*,” and ”*Compliance”*. However, privacy-impacting dark patterns may nevertheless infringe upon such principles, albeit indirectly: failing to conform with the principle of data minimization ultimately impacts conformity with the principle of accountability. In other words, the use of deceptive design patterns overtly impacts conformity with certain principles and, as a consequence, indirectly impacts conformity with others.

There is a reason for the accentuated focus on the direct violation of principles: dark patterns concern the interaction between the user and the system at the interface level, while they are less directly related to the system's back end. Moreover, the interconnected nature of privacy requirements also explains why the expert panel sometimes identified two privacy principles at risk due to a single dark pattern. As a result, one-third of the dark patterns considered in this study are likely to violate two privacy principles simultaneously.

5.1 Consent and choice

The data highlights that ”Consent and Choice” is the privacy principle most often violated by dark patterns, corresponding to obtaining explicit and voluntary permission before collecting and processing personal data. A significant privacy violation occurs when individuals are not given the option to allow or deny such processing, but their authorization is taken for granted, even though they are neither informed nor in control of their data. For example, dark patterns such as ”Automating the user away”(Gray et al., 2020) and ”Sneaking”(Chromik et al., 2019) correspond to this kind of violation. In the case that consent is granted, it is essential to provide individuals with a straightforward method to manage the permissions for their data. However, patterns like ”Bait and change”(Kitkowska, 2023) violate this second core privacy aspect because the affordances on the interface do not enable users to understand the consequences of their interactions with such affordances; therefore, the link between the choice and the method to signify such a choice is obscure.

Giving people a genuine choice regarding the processing of their personal data implies that individuals should make decisions freely and without any pressure. However, dark patterns based on coercing users (”Coercion” (Gray et al., 2018)), emotionally steering them (e.g., ”Confirmshaming”(Brignull, 2022) and ”Blaming the Individual”(CNIL, 2019)) or promising rewards to them (NCC, 2018) pressure individuals into a decision. Similarly, consent can be requested persistently, hoping that over time individuals will relent (”Continuous prompting”(EDPB, 2022) and ”Repetitive incentive”(Kitkowska, 2023)). Freedom of the user's choice can be restricted by manipulating the pace and complexity of the choice process like in ”Safety Blackmail” (Kitkowska, 2023) ”Forced Action,”(Gray et al., 2018) and ”Obstruction,”(Gray et al., 2018) or by seeking consent in the manner, interrupting the user's task flow (”Last Minute Consent”(CNIL, 2019)). As the ISO/IEC29100 states, the user's choice should be ”clear, prominent, easily understandable, accessible, and affordable.” Multiple dark patterns challenge these criteria. Some subtly diminish the clarity of the implemented mechanisms to enable users to express a choice by manipulating the user interface to prioritize certain actions over others (”Interface Interference”(Gray et al., 2018)). These manipulations might involve designs that artfully push users toward more privacy-invasive choices (”Hidden in Plain Sight”(EDPB, 2022)) or frame settings by emphasizing the benefits of a certain decision while downplaying its drawbacks (”Framing” (NCC, 2018)). Sometimes, explanations or questions are worded to lead users astray (”Misrepresent”(Jarovsky, 2022) and ”Trick Questions”(Brignull, 2022)), or contain conflicting information which reduces clarity (”Conflicting Information”(EDPB, 2022)). Violations may be caused by both insufficient information (”False Continuity”(CNIL, 2019)) or overwhelming information and choices (”Overloading” (EDPB, 2022) and ”Too Many Options”(EDPB, 2022)). The goal is often to create a long and tedious process for expressing choice or providing consent, leading users to give up expressing an informed decision or misunderstand their chosen settings. Some dark patterns become evident over time with repeated interactions. For instance, it might be harder to withdraw consent than give it in the first place, a tactic known as ”Roach Motel”(Brignull, 2022).

5.2 Openness, transparency, and notice

This principle mandates that individuals be informed about the processing of their personal data, including the data processing policies, procedures, and practices. This includes the purposes for processing personal data and the options available to individuals for exercising their rights. When significant changes in the handling of personal information arise, individuals must be notified. In addition to conveying this information to individuals, it should be ”clear and easily accessible.” Some dark patterns identified in this study violate these stipulations.

Clear information should be straightforward, devoid of ambiguity, and easy to understand. A group of dark patterns introduces confusion or ambiguity by using either ambiguous language or contradictory information (like ”Ambiguous Wording,”(EDPB, 2022) ”Hidden Legalese Stipulations,”(Bösch et al., 2016) ”Misrepresenting,”(Gray et al., 2020) and ”Two-Faced”(Gray et al., 2020)). A disorganized presentation of information can also lead to confusion (e.g., ”Lack of Hierarchy”(EDPB, 2022)). The user’s ability to comprehend the information can also be hampered when the information is unintelligible (”Confusion”(Conti and Sobiesk, 2010)) or presented in a language that the user is not familiar with (”Language Discontinuity”(EDPB, 2022)). Information is easily accessible when it is presented in a way that lets users readily access its content. Some user interfaces deliberately make such access unfeasible (e.g., ”Hindering,”(EDPB, 2022), ”Obfuscation” (Conti and Sobiesk, 2010)) or extremely challenging (”Privacy Maze”(EDPB, 2022)). Moreover, some interface designs intentionally divert users’ attention from data processing details (”Look Over There,” (Brignull, 2022)). Another tactic involves overwhelming users with excessive information, causing them to abandon their search (”Overloading” (EDPB, 2022)).

5.3 Individual Participation and Access

The ”Individual Participation and Access” privacy principle aligns with the rights of individuals concerning their personal data management. To adhere to this principle, users should be empowered to access their data, review them, challenge their accuracy, and request modifications, corrections, or removals. In practical terms, users should be provided with the necessary tools to exercise these rights. If these tools are malfunctioning, restricted, or missing, as highlighted by the deceptive design patterns (like ”Dead End”(EDPB, 2022) and ”Restricting Functionality”(Conti and Sobiesk, 2010)), users lose their ability to control their personal data.

However, merely providing tools for users to manage their data doesn’t ensure compliance with this principle. The ISO/IEC 29100 standard mandates that users should be able to exercise their rights easily, quickly, and efficiently. However, several dark patterns intentionally make this process challenging, slow, and inefficient. Some patterns hide controls, making them hard to locate (e.g.”Decontextualising,” (EDPB, 2022) ”Obfuscation,”(Conti and Sobiesk, 2010)), while others complicate the process to deter users from proceeding further (e.g., ”Immortal Account,”(Bösch et al., 2016) ”Obstruction,”(Gray et al., 2018)). Some tactics deliberately extend the process by demanding unnecessary steps from users (e.g., ”Longer Than Necessary”(EDPB, 2022)), hoping they will abandon the process. Additionally, certain patterns compromise the process’ efficiency by causing a mismatch between a user’s expectation and the outcomes of the user’s action (e.g., ”Bait and Change,”(Kitkowska, 2023) ”Misleading Information”(EDPB, 2022)).

5.4 Data minimization

Deceptive design patterns that potentially infringe the data minimization principle are used to collect a greater amount of personal data than what would be necessary to fulfil the purpose of the processing activity. The analysis identified three types of deceptive design patterns that will likely breach this principle. The first one refers to services such as social networks where users share more personal data than they intend (”Privacy Zuckering(Brignull, 2022)”). The second type implements a pre-checked privacy-invasive option for data sharing that counters the ’privacy by default’ approach and requests users to actively deselect such an option when configuring their account (”Default sharing”(CNIL, 2019)). Designers can also obscure or hide privacy controllers to prevent users from changing the pre-checked settings (”Default setting”(CNIL, 2019)). The third type uses misleading information. For example, they might suggest that the data collection is for legitimate purposes such as customizing services or improving the user experience when it is not (”Improving Experience”(CNIL, 2019)), or they might reassure users that their data will remain private and under their control when it is not the case (”Just You and Us” (CNIL, 2019)).

5.5 Use, retention, and disclosure limitation

Deceptive design patterns can also violate the use, retention, and disclosure of personal data. Just as with data collection, the use, retention, and disclosure of personal data should only extend to what is essential for well-defined, specific, and legitimate purposes. Various dark patterns violate use limitations by exploiting the user’s personal contacts to create automated communication emails to the user's contacts (e.g., "Address Book Leeching,"(Bösch et al., 2016) "Friend Spam(Brignull, 2022)).

5.6 Purpose legitimacy and specification

Finally, dark patterns violate the principles of purpose legitimacy and specification since they collect and reuse information for purposes that are not adequately communicated to the user. For instance, the Address Book Leeching(Bösch et al., 2016) pattern initially requests permission to access a user's contact list, claiming that it is necessary for the app's functionality, whereas, once granted permission, it engages in an additional activity, such as sending invitations to the people listed in the address book. Similarly, the "Shadow User Profiles"(Bösch et al., 2016) pattern is employed to create and store information about individuals from a contact list without disclosing this purpose to the user. This lack of transparency regarding the data's ultimate usage infringes upon the principle of purpose legitimacy, as users are left unaware of how their contact information is being leveraged for purposes beyond what they initially agreed to.

6 DISCUSSION AND PRACTICAL IMPLICATIONS

The study results indicate that dark patterns predominantly target privacy requirements described in terms of subjective properties such as clarity, usability, and accessibility of information and user choices related to the graphical user interface design. This may reflect the great attention of the academic and regulatory community to dark patterns used to maximize consent rates (e.g., on cookie banners), which is a visible front-end phenomenon that can be analyzed more easily than other deceptive strategies that are hidden in the back-end and therefore less blatant to the user/researcher who may need sophisticated means to detect them. For instance, it is difficult to determine whether data are collected for other purposes rather than those that have been declared, as this would entail audits of the actual data practices of the company which can not be uncovered through the mere inspection of the user interface. There is a growing awareness in the dark pattern academic, policy, and regulatory community about the need to go beyond the user interface to discover the deceptive practices that are employed in the back-end (e.g., in mobile applications, machine-learning models, etc.) (OECD, 2023; Kocyigit et al., 2023) and to cover emerging interfaces (e.g., embedded interfaces, VR, and AR) (Krauß, 2022; Owens et al., 2022). Hence, future work should analyze whether patterns that are published in novel taxonomies impact other privacy principles that appear only tangentially in the results of the present study.

To fulfil ISO 29100, it is paramount to prioritize protecting users' privacy over illegitimate business practices that maximize the collection and processing of personal data. This can be achieved by placing the users at the center of the development process, encouraging the adoption of respectful privacy-enhancing design patterns, and avoiding dark patterns that lower privacy safeguards. Dark patterns exemplify why a human-centered approach is necessary for privacy engineering. Human-centered design, identified as a requirement in the ISO/IEC 31700 standard (31700-1:2023, 2002), refers to an approach to system design and development that focuses on enhancing the interactions with a system for human users (ISO/IEC 31700:2023, 3.21). Adopting this human-centered engineering approach will assist privacy engineers in avoiding the implementation of deceptive design patterns, although it will not solve other systemic aspects that favor their adoption, such as those related to the AdTech business model that gathers massive amounts of data for advertising purposes and the race to the bottom in this respect that seems to be happening in online services.

Moreover, per the ISO/IEC 15288 standard (ISO/IEC, 2002) concerning System Life Cycle Processes, privacy engineers should carefully consider the privacy requirements jeopardized by dark patterns and analyze, implement, and verify the technical and organizational measures at all stages of the development process. The results of the current work can also be used for privacy threat modeling as part of LINDDUN (Deng et al., 2011) and PriS (Islam et al., 2012) methods, thereby informing system design. For example, the dark patterns identified through this work can be used to exemplify LINDDUN's threat types: "Data Disclosure," "Unawareness and Unintervenability," and, ultimately, "Non-compliance." This work can help broaden the understanding of system vulnerability to include the vulnerability that derives from human cognitive biases and human-machine interaction (such as lack of consent, transparency, and user empowerment (Wright and Raab, 2014)) and that is exploited by manipulative designs. This can support the work of privacy engineers when they define and test the system requirements. Similarly, our mapping can also be leveraged by ISO certification entities to support their analysis and integrate design considerations into their arguments for providing or confirming such certifications.

The findings of this study can also support a more objective reconceptualization of privacy-related dark patterns in terms of their violations of specific privacy requirements, thereby solving terminological fuzziness and making the definition of this phenomenon more easily actionable (e.g., when it comes to developing automated deception applications). Such reconceptualization can be integrated into the methods used for evaluating the risks related to data practices (such as privacy and data protection impact assessments), which do not traditionally consider the user manipulation aspects in determining the risks to individuals' rights and freedoms. For example, in the EU, Article 24 of the GDPR mandates companies to put in place organizational and technical measures to mitigate the identified risks and be compliant. The risks generated by the design patterns mentioned in these pages mainly encompass the privacy of users, the lack of which can engender harms such as autonomy harms (e.g., lack of control over one's own data), reputational harms (e.g., derived from the oversharing of confidential information), psychological harms (e.g., negative feelings of embarrassment, fear, anxiety, etc) and discrimination harms (e.g., price discrimination based on profiling) (Citron and Solove, 2022). Our mapping clearly identifies how avoiding specific dark patterns can lower risks for users and, therefore, simplify the obligations for companies, even in terms of mitigation measures, while lowering their compliance risks. More in general, given that the foundational principles of the ISO 29100 are shared with the GDPR, respecting these privacy principles may also help privacy engineers implement measures within their organizations to achieve compliance with legal obligations.

Furthermore, the results could also be used to determine whether the solutions proposed to tackle deceptive design patterns (for an overview, see the matrix in (Rossi and Bongard-Blanchy, 2021)) are effective. For example, the best practices that have been proposed by the European Data Protection Board (EDPB, 2022) mainly concern how to design transparent and consistent communications towards users (in sign-up interfaces, privacy policies, data breach communications, privacy settings, etc.) (alike the first three principles that resulted from our analysis), but do not provide guidance on how to implement the principles of data minimisation or purpose legitimacy and specification without dark patterns. Lastly, identifying risks related to deceptive designs and mitigation measures can be useful to address online manipulation more in general (that encompasses dark patterns, social engineering, AI-based deception and misinformation), which is increasingly recognized as one of the major digital threats of modern societies.

7 CONCLUSIONS, LIMITATIONS AND FUTURE WORK

Our analysis showed that most privacy-impacting dark patterns impact subjective properties of ICT system design related to user choice and transparency. Considering the requirements related to human-centered engineering and system life cycle design, dark pattern types and examples can provide practical guidance to privacy engineers and product developers on what to avoid to fulfill the ISO 21900 requirements and to map privacy threats and system vulnerability more comprehensively. Future work should focus on further determining ”fair design patterns” that can be adopted to implement privacy engineering in practice.

Our results are preliminary findings revealed by a small group of experts (four in the first stage of discussion and three in the re-evaluation stage, as one of the experts could not proceed further): future studies will benefit from a broader, diverse group of researchers and practitioners. Another limitation is that the collection of taxonomies was finalized in June 2022 and did not include those published later. Since then, several important attempts have been made to address the actionabilities of taxonomies (Gray et al., 2023b) and leverage transdisciplinary cooperation (Gray et al., 2023a). Future work should consider those and conduct a similar analysis on the brand-new ISO 31700 on Privacy by Design for Consumer Goods and Services (ISO, 2023) that has a pronounced user experience slant. Additionally, while one-third of the pattern definitions we discussed in the study do not create immediate privacy risks, some of them (e.g., ”Scarcity”) can still hinder users' ability to make well-considered decisions (Botes, 2023). Outside the scope of privacy engineering per se, the community should pay attention to these cases and work towards disseminating an ethical approach to the design and development of technologies.

ACKNOWLEDGEMENTS

We thank Emre Kocyigit and Lorena Sanchez Chamorro for lending their expertise and participating in the expert analysis of dark patterns. This research is supported by the Luxembourg National Research Fund (FNR) under grant number IS/14717072 (DECEPTICON - Deceptive Patterns Online) and by the Italian National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Investment 3.1 of Italian Ministry of University and Research funded by the European Union — NextGenerationEU (BRIEF - Biorobotics Research and Innovation Engineering Facilities - Project identification code IR0000036). Author 1's work is funded by the European Union under Grant Agreement No. 101092861. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible.

REFERENCES

31700-1:2023, I. (2002). ISO iso 31700-1:2023 consumer protection — privacy by design for consumer goods and services — part 1: High-level requirements.

Anthonysamy, P., Rashid, A., and Chitchyan, R. (2017). Privacy requirements: present & future. In *2017 IEEE/ACM 39th international conference on software engineering: software engineering in society track (ICSE-SEIS)*, pages 13–22. IEEE.

Antignac, T., Scandariato, R., and Schneider, G. (2016). A privacy-aware conceptual model for handling personal data. In *Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques: 7th International Symposium, ISoLA 2016, Imperial, Corfu, Greece, October 10–14, 2016, Proceedings, Part I 7*, pages 942–957. Springer.

BEUC (2022). "dark patterns" and the eu consumer law acquisition. Last accessed 9 January 2023.

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., and Lenzini, G. (2021). " i am definitely manipulated, even when i am aware of it. it's ridiculous!"-dark patterns from the end-user perspective. In *Designing Interactive Systems Conference 2021*, pages 763–776.

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

Botes, M. (2023). Autonomy and the social dilemma of online manipulative behavior. *AI and Ethics*, 3(1):315–323.

Brignull, H. (2022). Deceptive patterns. Last accessed 30 October 2022.

Chamorro, L. S., Bongard-Blanchy, K., and Koenig, V. (2022). Justice in interaction design: preventing manipulation in interfaces. *arXiv preprint arXiv:2204.06821*.

Chromik, M., Eiband, M., Völkel, S. T., and Buschek, D. (2019). Dark patterns of explainability, transparency, and user control for intelligent systems. In *IUI workshops*, volume 2327.

Citron, D. K. and Solove, D. J. (2022). Privacy harms. *BUL Rev.*, 102:793.

CNIL (2019). Shaping choices in the digital world.from dark patterns to data protection: the influence of ux/ui design on user empowerment. Last accessed 9 January 2023.

Conti, G. and Sobiesk, E. (2010). Malicious interface design: exploiting the user. In *Proceedings of the 19th international conference on World wide web*, pages 271–280.

CPRA (2020). The california privacy rights act of 2020. Last accessed 9 January 2023.

Curley, A., O'Sullivan, D., Gordon, D., Tierney, B., and Stavrakakis, I. (2021). The design of a framework for the detection of web-based dark patterns.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32.

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., and Bacchelli, A. (2020). Ui dark patterns and where to find them: a study on mobile applications and user perception. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–14.

EDPB (2022). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 1.0.*

Fansher, M., Chivukula, S. S., and Gray, C. M. (2018). # darkpatterns: Ux practitioner conversations about ethical design. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6.

Goodstein, S. A. (2021). When the cat's away: Techlash, loot boxes, and regulating" dark patterns" in the video game industry's monetization strategies. *U. Colo. L. Rev.*, 92:285.

Gray, C. M., Chivukula, S. S., and Lee, A. (2020). What kind of work do" asshole designers" create? describing properties of ethical concern on reddit. In *Proceedings of the 2020 acm designing interactive systems conference*, pages 61–73.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A. L. (2018). The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–14.

Gray, C. M., Sanchez Chamorro, L., Obi, I., and Duane, J.-N. (2023a). Mapping the landscape of dark patterns scholarship: A systematic literature review. In *Designing Interactive Systems Conference*, pages 188–193.

Gray, C. M., Santos, C., and Bielova, N. (2023b). Towards a preliminary ontology of dark patterns knowledge. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–9.

Gray, C. M., Santos, C., Bielova, N., and Mildner, T. (2023c). An ontology of dark patterns knowledge: Foundations, definitions, and a pathway for shared knowledge-building. *arXiv preprint arXiv:2309.09640*.

Gray, C. M., Santos, C., Bielova, N., Toth, M., and Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18.

Graßl, P., Schraffenberger, H., Borgesius, F. Z., and Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1):1–38.

Greenberg, S., Boring, S., Vermeulen, J., and Dostal, J. (2014). Dark patterns in proxemic interactions: a critical perspective. In *Proceedings of the 2014 conference on Designing interactive systems*, pages 523–532.

Gunawan, J., Santos, C., and Kamara, I. (2022). Redress for dark patterns privacy harms? a case study on consent interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law*, pages 181–194.

Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., Cranor, L. F., Sadeh, N., and Schaub, F. (2019). An empirical analysis of data deletion and {Opt-Out} choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 387–406.

Hasan Mansur, S. M., Salma, S., Awofisayo, D., and Moran, K. (2023). Aidui: Toward automated recognition of dark patterns in user interfaces. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, page 1958–1970.

Huth, D. and Matthes, F. (2019). "appropriate technical and organizational measures": Identifying privacy engineering approaches to meet gdpr requirements.

Islam, S., Mouratidis, H., Kalloniatis, C., Hudic, A., and Zechner, L. (2012). Model based process to support security and privacy requirements engineering. *International Journal of Secure Software Engineering (IJSSE)*, 3(3):1–22.

ISO (2023). Iso 31700-1:2023 consumer protection — privacy by design for consumer goods and services — part 1: High-level requirements.

ISO/IEC (2002). ISO/IEC 15288:2002 systems engineering – systems life cycle processes.

ISO/IEC 29100:2011 (2011). Information technology - Security techniques - Privacy framework. Standard, International Organization for Standardization, Geneva, CH.

Jarovsky, L. (2022). Dark patterns in personal data collection: Definition, taxonomy and lawfulness. *Taxonomy and Lawfulness (March 1, 2022)*.

Kitkowska, A. (2023). The hows and whys of dark patterns: Categorizations and privacy. *Human Factors in Privacy Research*, pages 173–198.

Kocyigit, E., Rossi, A., and Lenzini, G. (2023). Towards assessing features of dark patterns in cookie consent processes. In Bieker, F., Meyer, J., Pape, S., Schiering, I., and Weich, A., editors, *Privacy and Identity Management*, IFIP Advances in Information and Communication Technology, page 165–183, Cham. Springer Nature Switzerland.

Kollnig, K., Datta, S., and Van Kleek, M. (2021). I want my app that way: Reclaiming sovereignty over personal devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–8.

Krauß, V. (2022). Exploring dark patterns in xr.

Luguri, J. and Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1):43–109.

Martin, Y.-S. and Kung, A. (2018). Methods and tools for gdpr compliance through privacy and data protection engineering. In *2018 IEEE European symposium on security and privacy workshops (EuroS&PW)*, pages 108–111. IEEE.

Martini, P., Drews, C., et al. (2022). Making choice meaningful–tackling dark patterns in cookie and consent banners through european data privacy law. *Available at SSRN 4257979*.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32.

Mathur, A., Kshirsagar, M., and Mayer, J. (2021). What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, pages 1–18.

Matte, C., Bielova, N., and Santos, C. (2020). Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809. IEEE.

Mead, N. R. and Stehney, T. (2005). Security quality requirements engineering (square) methodology. *ACM SIGSOFT Software Engineering Notes*, 30(4):1–7.

NCC (2018). Deceived by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy. *Norwegian Consumer Council Report*.

OECD (2023). *Consumer vulnerability in the digital age*. Number 355 in OECD Digital Economy Papers. Paris.

Owens, K., Gunawan, J., Choffnes, D., Emami-Naeini, P., Kohno, T., and Roesner, F. (2022). Exploring deceptive design patterns in voice interfaces. In *Proceedings of the 2022 European Symposium on Usable Security*, pages 64–78.

Rossi, A. and Bongard-Blanchy, K. (2021). All in one stroke? intervention spaces for dark patterns. *arXiv preprint arXiv:2103.08483*.

Sangaroonsilp, P., Dam, H. K., Choetkiertikul, M., Ragkhitwetsagul, C., and Ghose, A. (2023). A taxonomy for mining and classifying privacy requirements in issue reports. *Information and Software Technology*, 157:107162.

Santos, C., Rossi, A., Sanchez Chamorro, L., Bongard-Blanchy, K., and Abu-Salma, R. (2021). Cookie banners, what's the purpose? analyzing cookie banner text through a legal lens. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, WPES '21, page 187–194, New York, NY, USA. Association for Computing Machinery.

Voigt, P. and Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676):10–5555.

Wright, D. and Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, 28(3):277–298.

Zagal, J. P., Björk, S., and Lewis, C. (2013). Dark patterns in the design of games. In *Foundations of Digital Games 2013*.

APPENDIX

In the presented study we used the following taxonomies:

1. European Data Protection Bord (EDPB) 2022. Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them.
2. Frobrukerrådet. 2018. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy.
3. National Commission on Informatics and Liberty (CNIL). 2020. Shaping Choices in the Digital World.
4. Bösch, C., Erb, B., Kargl, F., Kopp, H., and Pfattheicher, S. (2016). Tales from the dark side: privacy dark strategies and privacy dark patterns. Proc. Priv. Enhancing Technol., 2016(4), 237-254.
5. Brignull H. 2018. Deceptive Patterns. https://https://www.deceptive.design/. Accessed June, 2022.
6. Conti, G., and Sobiesk, E. (2010, April). Malicious interface design: exploiting the user. In Proceedings of the 19th international conference on World wide web (pp. 271-280)
7. Gray, C. M., Chivukula, S. S., and Lee, A. (2020, July). What Kind of Work Do" Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. In Proceedings of the 2020 acm designing interactive systems conference (pp. 61-73).
8. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems (pp. 1-14).
9. Greenberg, S., Boring, S., Vermeulen, J., and Dostal, J. (2014, June). Dark patterns in proxemic interactions: a critical perspective. In Proceedings of the 2014 conference on Designing interactive systems (pp. 523-532).
10. Jarovsky, L. (2022). Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness. Taxonomy and Lawfulness (March 1, 2022).
11. Kitkowska, A. (2023). The Hows and Whys of Dark Patterns: Categorizations and Privacy. Human Factors in Privacy Research, 173-198; as the main aim of this taxonomy was to reorganize previously identified patterns based on psychological principles, without changing their definitions, Authors 1 and 2 decided to merge them with those from the original taxonomies.
12. Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.
13. Zagal, J. P., Björk, S., and Lewis, C. (2013). Dark patterns in the design of games. In Foundations of Digital Games 2013.