Feedback to the Guidelines 3/2022 on "Dark patterns in social media platform interfaces: How to recognise and avoid them"

Collaborative public comments by the members of the DECEPTICON (Deceptive patterns online) project, University of Luxembourg, and their collaborators[1]

Table of contents

[1] Maria W. Botes, Emre Kocyigit and Arianna Rossi, SnT, University of Luxembourg; Lorena Sanchez-Chamorro, Anastasia Sergeeva and Kerstin Bongard-Blanchy, HCI group, University of Luxembourg; Philippe Valoggia, LIST; Cristiana Santos, University of Utrecht; Rachele Carli, Università di Bologna.
Website of the project: https://irisc-lab.uni.lu/deceptive-patterns-online-decepticon-2021-24/

1. Introduction and summary of comments

The *Draft Guidelines on Dark Patterns for Social Media* are timely and a welcome development. However, as discussed in our commentary below, there is room for improvement, and we summarize the main points here. The Guidelines should:

- better explain their scope and application. The specific guidance given, the language used to explain the guidelines, and the practical implementation tips will be dictated by the intended audience (See point 2 below).
- more clearly explain the basis on which the dark patterns are categorized and expand some of the current definitions (See point 3 below).
- include additional dark patterns as identified that are currently not provided for in the guidelines (See point 4 below).
- acknowledge that all humans suffer from inherent vulnerabilities and should be protected against exploitation (See point 5 below).
- ensure that the recommended categorisation, definitions, and assessments of dark patterns, based on the GDPR, are also in line with foundational human rights, consumer rights, and ethical principles relating to autonomy and decision making (See points 6,7 and 8 below).
- acknowledge and consider the importance that the complex phenomenon of emotional steering plays as, or in, dark patterns and provide guidance accordingly (See point 9 below).
- attend to some minor editing issues to ensure a more pleasant reading experience (See point 10 below).
- provide positive guidelines as to what constitutes acceptable language and pattern use, considering the difficulty of determining what forms of manipulation are acceptable or not.

2. Scope of the Guidelines

These guidelines set out to propose practical recommendations to ***designers*** and ***users*** on how to recognize *and avoid* dark patterns on social media platforms that infringe the GDPR requirements (paragraph 1, page 2). They further specifically mention that "*data protection authorities are responsible for sanctioning the use of dark patterns if these breach GDPR requirements*" (paragraph 2, page 2). These assertions trigger the following questions:

2.1. **Data Protection Authorities (DPAs).** In this context these guidelines have been drafted primarily to enable DPAs to recognize dark patterns that breach the GDPR and sanction the breaching parties. To truly enable DPAs to recognize and identify dark patterns and their harms the EDPB is invited to:

2.1.1. Identify, through cooperation mechanisms within each DPA or other stakeholders, the use of dark patterns by carrying out '**sweeping' investigations,** not only on current social media platforms, but also on specific sectors such as marketplaces of social media, cookie banners, gaming, and retail websites where the use of dark patterns is rife.

2.1.2. **incorporate and advise DPAs by incorporating more behavioral insights into the guidelines** to assess how a given dark pattern is likely to affect data subjects. DPAs could also consider conducting user studies on user interfaces to assess and clarify in an

evidence-based manner the impact of such designs on users – with the caveat that each UI implementation and each user group are different, therefore it is exceedingly difficult to achieve generalizable guidance on the effect of a dark pattern (a type could be implemented in many different manners) on a group of users (each group being different from each other).

2.1.3. suggest platforms and DPAs to disclose complete and conclusive evidence about the use of behavioural experiments for the design or optimization of a given interface, failing which, a legal presumption will be made that a platform did indeed use information for behavioural experiments.

2.1.4. compile and publish national decisions of public authorities or civil courts **on dark patterns,** creating a database relating to design practices.

2.1.5. provide clearer, evidence-based guidance to companies on how to avoid designing their choice architecture in a way that can be unfair and misleading to consumers.

2.2. **Users.** Paragraph 1 states that "*These guidelines aim to educate users to recognize dark patterns and to protect their privacy in a conscious way*". Considering this proposed aim, the guidelines are not written in a way that will educate social media users to be more privacy conscious. Even assuming that the guidelines were accessible, understandable, and usable by others than experts in data protection law, educating end users is not the role of the EDPB.

The guidelines seem to fail to mention the fact that most of the time users **are not experts in data protection, nor it its violations,** which is why they can easily fall prey to dark patterns. Since the language used in the guidelines is very technical and long–winded, it poses a barrier for understanding its content, especially for individuals without a legal background.

2.3. **Designers of social media**. If these guidelines are aimed at designers, then they must be written in plain language, and presented in a format that makes it accessible to designers - and not only to people with a legal background. Images included in the guidelines must be in higher resolution and additional mockups of examples may prove to be immensely helpful in showing what is meant by the guidelines.

2.4 **Other stakeholders**. Designers are not the only stakeholders that take decisions about the design of social media. We are currently conducting expert workshops with UX/UI designers and, although the results are not published yet, what emerges is that in social media companies, designers usually trust other stakeholders in their design process. They rely on legal and IT departments to guide them on specific issues, for instance, compliance and technical implementations. It is, therefore, necessary that the guidelines are written in a clear and easy to understand and apply way. To the contrary, we also noticed in our results that SMEs do not always have compliance departments, so designers are usually front-end developers that need to implement these guidelines based on their own knowledge of the law. More importantly, they usually rely on what other stakeholders, and customers, such as business and marketing teams prefer, which may not be aligned with legal requirements.

3. Categorization, definitions used in the guidelines.

While it seems desirable to provide some quick and catchy names to categorize dark patterns, the proposed definitions raise some issues due to their ambiguity and the use of certain words:

3.1. **Baseline for the definition of dark patterns.** The definition of dark patterns given in the guidelines comprises: "*UIs and UXs on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data*". A more precise characterization of the components of dark patterns will enable its detection (by manual and automated means). Several issues arise from this definition:

3.1.1. **Why only on social media platforms**? The guidelines need to motivate their choice and limitation to only these platforms. Does it mean that the same dark pattern on other kinds of digital services is not a dark pattern?

3.1.2. **Unintended, unwilling *and* potentially harmful**: Does it mean that all 3 conditions need to be satisfied as cumulative requirements to qualify as a dark pattern, or is one of these elements enough?

3.1.3. **Harmful.** How is harmful defined? What are the harms that the guidelines consider as legally acknowledged harms? Literature (Gunawan, 2021; Mathur, 2021) discusses several types of harms caused by dark patterns that includes harms of a **material nature**, such as financial harms, as well as harms of a **non-material nature**, such as privacy invasion, loss of time, addiction, cognitive burdens, loss of autonomy, and emotional or psychological distress. Besides identifying the harms, the guidelines could further clarify whether the manifestation of such harms may trigger compensation for individuals who fell prey to practices of dark patterns in terms of Article 82 of the GDPR.

3.1.4 **Decisions.** Why only "decisions"? What about other actions that do not involve decision-making? In this regard the definition offered by Mathur et al. consider "deception" to have a much wider scope, which includes user's beliefs and states that deception "*Induce false beliefs in users either through affirmative misstatements, misleading statements, or omissions*" (Mathur, 2021).

3.1.5. **UX.** The definition of user experience as per these guidelines is described as the "*overall experience users have with social media platforms, including the perceived utility, ease of use, and efficiency of interacting with it."* But this definition is just describing a part of user experience, called the *pragmatic user experience* (closely related to Usability) (Hassenzahl, 2007), not mentioning the hedonic aspects of UX, which relate to dimensions of pleasure and interest in the user's interaction with platform. This dimension could also contribute to the interaction between the user and perception of malicious patterns. If the guidelines decide to concentrate just on the usability part of the user experience, they also need to provide rationales behind this decision.

3.1.6. **UI and UX of dark patterns.** The definition of dark patterns that considers "interfaces and user experiences" as dark patterns is problematic. To determine UX from a theoretical point of view (through guidelines, or what social media providers may expect with their analysis for accountability and transparency purposes) is very hard. Service providers can

explain their analysis and intentions – as is mentioned in the Accountability and Transparency section, but not the user experience *per se*. User experience is about individuals, and how they experience the interaction with technological products, which is difficult to determine *ex ante* on paper. The experience of dark patterns can vary in a wide range of directions since the users may respond in quite different ways. Dark patterns do not only create bad user experiences. For example, some, like not having to take a time-consuming cumbersome decision about online tracking every time users enter a website, may be illegal, but still provide a better user experience. Using emotions, for instance, connect with the hedonic dimension of the user experience. In this regard, *"hedonic quality refers to the product's perceived ability to support the achievement of "be goals", such as "being competent", "being related to others", "being special" for more on do-and be goals".* A playful experience can trigger positive emotions in the user, and it may not have the intention of nudge users in a particular direction. Therefore, considering "dark patterns" as user experiences can be problematic, hard to define and an issue to deal with from provider's perspective.

3.2. **Rationale behind the categorization**

3.2.1. **Absence of rationale**. These guidelines offer no rationale behind the choice of names for the categories of dark patterns or their definitions. Some names, such as "*Look over there*" mentioned in paragraph 100, are not intuitive and connected to an example based on language and about distinguishability of consent.

3.2.2. **Absence of methodology**. There is a lack of transparency about the adopted methodology, such as what is meant by evidence-based guidelines.

3.2.3. **The notion of intention**. All definitions contain two conditions: an implementing strategy (e.g., users are confronted with an avalanche of requests) and a goal/intention (e.g., to prompt them to share more data). Should the intention be proved and both conditions be respected for a design pattern to be labelled as a dark pattern? If not, then the intention/goal should not be part of the definitions. Or would the implementation of a strategy sufficient?

3.2.4. **Lack of coherence**. There seems to be no clear correspondence between "categories," "types," and "examples" of the proposed dark patterns. In several cases, the definition of the type of dark pattern is so broad that it is added as a separate category. The reason for adding specific patterns under certain categories are unclear. For example, "Continuous prompting" and "Privacy Maze" were both added under the Overloading category, but they are addressed to two different big problems - the first one is connected to repeated requests for data from the user, and the second - to excessive information search. The third type belonged to this category of "too many options" is much closer to the "Privacy Maze"(this time - by providing excessive options for choosing from), so it is logical to put them together, but reasons to put "Continuous prompting" to that category and not in separate one seems less justified; if the main idea of the category is to concentrate on the things, that could overload user and put their attention out of the goal, why "Look over there" type is not posted inside that category, as it also connected to the question of excessive information presentation. In

addition, some of the definitions of specific categories are not mutually exclusive, for example it will be difficult to distinguish between “Hindering,” and “Fickle,” because in both cases the problem is created by inconsistency of interface, which blocks or slows down the user's data management ability

3.2.5. **The notion of visual nudges.** Another example is the definition of "Stirring", i.e., a dark pattern that "*affects the choice users would make by appealing to their emotions or using visual nudges*". It is necessary to clarify what types of “visual nudges” would be classified as “stirring.” Visual nudges (i.e., colors, highlights, buttons, sentences, etc.) are simply ways to help the user navigate an interface and, as such, are inevitable and often useful, for example when they are used to enhance privacy and security (Distler et al.,2020 and Acquisti et al., 2017). Only in specific cases can be considered as dark patterns. However, it is not possible to say that the use of a color is a dark pattern, so, it is necessary that these guidelines clearly specify what “visual nudges” mean, otherwise, they may create confusion, lower the level of protection, and even hinder creator’s rights.

3.2.6. **Future-proof and flexible guidelines.** Clarity in this regard is important, because as new forms or dark patterns arise in the future, these guidelines and the categorization of dark patterns should still be timely and up to date. Otherwise, these guidelines will have to be updated on a regular basis with a never-ending list of new forms of dark patterns that have developed since the last set of guidelines were published.

3.3. **Goal of the taxonomy.** The goal of the taxonomy is also unclear. If the goal is the identification of the patterns that violate certain requirements, a classification in that sense would be more useful. Having said this, creating a brand-new nomenclature is unjustified. To the contrary, we do not need new categories, we need guidance in respect of how to classify dark patterns in accordance with reliable definitions that will remain applicable in different contexts, for example, in other digital and non-digital services beyond social media. For this reason, is it advisable to use terminology developed in existing literature, like C. Gray's classification (eg. "Obstruction" instead of "Hindering"; “Preselection,” instead of “Deceptive Snugness”) (Gray et al., 2018). Their taxonomy has been used in several fields since 2018, thus the guidelines could use the same common frame of reference to avoid burdening and confusing readers with additional and new taxonomies. There is also a privacy-oriented taxonomy by Bösch et al., which made a coherent attempt to create a framework for dark patterns within Hopeman’s privacy design strategies (Bösch et al., 2016).

3.4. **“Neutral” language and design.** The EDPB points out the need to provide information in a *“neutral and objective way*” (paragraph 16) to avoid deceptive or manipulative language or design. Such a statement implies some concerns:

3.4.1. **Neutral way**. It is not clear what a “neutral way” of presenting information and options means. To quote the main global experts of usable privacy and nudges, “*In simple terms, there is no such thing as a neutral design in privacy, security, or anywhere else*.” (Acquisti et al., 2017). No other section of the Guidelines provides any definition or

further understanding of the very concepts of manipulation or deception and how a neutral form would avoid them.

3.4.2. **Individual perception.** The definition of manipulation is, *per se*, a dynamic phenomenon. The guidelines need to account for the context in which a certain expression or design element are used, and the perceptive capacities of a person, or what it *evokes* in the person who receives it, rather than on precise, *ex ante* discernible patterns (Rudinow, 1978). Even if it were possible to formulate an effectively neutral language, one should also assume that individuals are able to perceive it as such. In fact, it has been widely demonstrated that any information is filtered and reinterpreted by subjects in the light of the biases inherent in their cognitive structure and of those subjectively developed and consolidated through subjective experiences (Raz, 1986). It follows that such a provision is vague and unable to be effective in protecting users from misleading dark patterns.

3.4.3. **Providing definitions.** In page 22, the guidelines recommend as best practice the use of definitions when using platforms use unfamiliar or technical words or jargon to help users understand the information provided to them, either given directly into the text, when users hover over the word, as well as be made available in a glossary. While providing a definition might facilitate a better understanding of the word/jargon, there is a potential danger to simplification and overload of information. Complex information may become oversimplified, potentially lowering the accuracy of information. There is some evidence that consumers may be too quick to accept information that is easy to process (Rennekamp, 2012), which may be problematic if the information is misleading.

3.5. **Steering effect and the level of severity of harms of dark patterns**. The guidelines already refer to certain dark patterns whose *steering effect* can be especially strong, for example, at the sign-up process stage (paragraph 39). As social media platforms may use different amounts and combinations of various dark pattern categories (Luguri and Strahilevitz, 2021) (e.g., deploying mild and aggressive dark patterns) dark patterns may cause harms. Such level of severity can be used to classify dark pattern types and their unlawfulness. The EDPB could consider discussing the attributes for such weighting and provide a scale of severity of harms regarding the dark patterns presented in the guidelines.

3.6. **Desktop websites, mobile websites, and mobile apps.** In paragraph 1, the guidelines state that they will focus on the design of user-interfaces and content presentation of **web services and apps.** Recent research found that many dark patterns vary between platforms across modalities such as desktop websites, mobile websites, and mobile apps, and that these differences expose people to inconsistent experiences of autonomy, privacy, and control which adds to the impact of dark patterns[2]. These Guidelines must explicitly state which types of modalities fall within their scope and identify the types of dark patterns to be found in each of these modalities.

4. Dark Patterns missing in the guidelines.

[2] Johanna Gunawan, Dave Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. Towards an Understanding of Dark Pattern Privacy Harms

Some important design patterns are missing from these guidelines, for example:

4.2. **Immortal accounts**. The adopted definition sets aside the common dark pattern instance connected to the *irreversible* character of personal data sharing. For instance, "Immortal Accounts" (Bösch et al., 2016) keep some user's information even after deleting the account. It would be useful to add the word "irreversible" into the definition.

4.3. **Users can be tricked by using their "muscle memory**". "Muscle memory" refers to the changing interfaces of applications which make use of the human muscles that have memory effects. After continuously repeating the same movement for many times, the muscles will eventually form conditioned reflexes. Exploiting muscle memory does not only mislead, but also coerce and trick data subjects to agree to privacy-invasive policies and even to enter directly to the marketplace of a given social media platform when that was not the primary intention. Instagram created a new layout, introducing new options (Reels and Shop) instead. Users now have a higher likelihood of unintentionally clicking on new options, simply relying on the repetitive function of their fingers nudging them to the same spot (now facilitating them to the marketplace) where other options previously existed (camera and notifications).

4.4. **The use of motion when dealing with interface-based patterns**. 'Motion onset' (Abrams and Christ, 2003) -- the first stage of motion -- captures the user's attention and can nudge the user. An example of this usage of motion can be found during the sign-up procedure of Snapchat in which a brightly colored moving circle is placed around the 'OK' selection for accepting the platform's notifications and the syncing of the user's contacts with the app. Such use of a moving circle can nudge users to receive notifications and share contacts

5. Vulnerable groups

5.1. ***All data subjects can be considered structurally vulnerable***. The need of a greater – though not better specified – protection of "*vulnerable data subjects*" is mentioned and does not only apply to children. This idea is certainly valuable in its intentions. Nevertheless, it reflects a partial view of the scope and impact of manipulative techniques on users. Assuming, *a contrario*, that there are categories of subjects able to defend themselves against these dynamics may pose the risk of not providing a sufficient minimum, and common, level of protection for all the individuals involved in the human-technology interaction. Additionally, the guidelines are invited to define data subjects as **vulnerable users of social media platforms**, instead of "a member of a target audience" (definition used in previous EDPB guidelines)[3] (EDBP Guidelines on consent, 2020).

5.2 ***Perception of dark patterns needs to be considered***. The way we perceive and interpret the world depends on our cognitive architecture, our senses, previous experiences, cultural and social environment (Blumenthal-Barby, 2016). The subjective understanding of an objective fact can alter the perception of the possible – harmful – consequences, since human beings do not actually see reality, but only the *version* of its which their mind created (Lotto, 2017). User perception is a constitutive element of the concept of manipulation and vulnerability that needs to be considered while analysing dark patterns.

[3] Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020

5.3. **Insufficiency of user awareness and vulnerability**. The mere increase of individuals' awareness of possible deceptive dynamics *might not have* a significant impact in resisting to dark patterns. Difficulty in recognising manipulation is a crucial element of manipulation itself. The main target of manipulative techniques is self-awareness, as they interfere with the decision-making process, leading to unconscious choices that the user would not have made without their influence (Coons and Weber, 2014). Furthermore, they act on cognitive biases that can make anybody potentially vulnerable (Leonard et al., 2008). As such, even aware users are still vulnerable to dark patterns.

5.4. ***Age vs vulnerability***. Contrary to what is often believed, one of our studies (Bongard-Blanchy et al., 2021) demonstrated that younger generations can detect dark patterns better than older ones – probably because of a higher digital literacy and frequency of use of platforms. This suggests that age is not the only factor that plays a *significant role* in self-protection. The Guidelines do not mention specific methods of access to information for children as proposed already by other DPAs, such as the ICO[4] and other stakeholders[5].

5.5. ***Vulnerability as a concept.*** It would be advisable to pay more attention to the analysis of the very concept of vulnerability, which could become a criterion for evaluating the techniques applied by social media platforms. Specifically, the integration of the so called "anthropology of vulnerability" approach could be considered (Coeckelbergh, 2013). This would mean to start from the assumption that vulnerability is an irreducible characteristic of humanity, which cannot be eliminated. Nonetheless, it could become a useful element to define which technologies to limit, in a human-centred development perspective. More precisely, we should be able to select which vulnerabilities – and thus which risks – we are willing to embrace, to allow a responsible design and usage of social media interfaces, and which ones to steam, for they could represent an evident or too risky harm for individual privacy and psychological integrity.

5.6. ***Other vulnerable groups.*** The guidelines are absent regarding elderly people and other vulnerable groups -- digitally challenged, low income, people with cognitive disabilities, visually impaired persons, etc. which may be disproportionately affected because they can have a limited physical and/or mental bandwidth to respond/react to dark patterns. People with mental illness, asylum seekers or the elderly have been named as "segments of the population requiring special protection," by the Article 29 Data Protection Working Party[6] that states that these groups can also be vulnerable data subjects.

6. Combined legal fields and plural enforcement regime

Combined legal fields. The EDPB underlines that dark patterns may violate not only the GDPR provisions, but also the consumer protection regulation (paragraph 4). Other domains are also

[4] Information Commissioner's Office. (2020, September). *Age appropriate design: a code of practice for online services* (2.1.128). https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf; Information Commissioner's Office (ICO), 'What should our general approach to processing children's personal data be?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/

[5] Dorine Dollekamp and Tommy Fitzsimons, 'Children and Data Protection' (Consumentenbond, 2021) < https://ilplab.nl/wp-content/uploads/sites/2/2021/04/Rapport-Children-and-Data-Protection-Justification.pdf >

[6] 29 Working Party (WP 248) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017

impacted by dark patterns such as competition law, and fundamental human rights, including ethical principles such as autonomy. Consumer (BEUC, 2022) and competition authorities (ACM of the NL and UK) issued reports on dark patterns, touching also upon data protection aspects, including on social media UI. It would be useful if **the EDPB could align with taxonomies and guidelines on online choice architecture manipulative practices issued by other stakeholders**. For instance, the UK Consumer and Market Authority (CMA) [12] presents an in-depth analysis of online manipulation overing three main aspects within online choice architecture, also applied to social media, e.g., i) choice structure (Defaults, Ranking, Bundling, Choice overload and decoy, Sensory manipulation, Sludge, Dark nudges, Forced outcomes), ii) choice information (Framing, Complex language, Information overload), iii) Choice Pressure (Scarcity and popularity claims, Prompts and reminders, Messengers, Commitment Feedback, Personalisation).

7. Assessment of the lawfulness and the need for criteria.

7.1. **Criteria or measurable thresholds.** The Guidelines should consider introducing a measurable threshold to help social media providers when drawing the line between permissible persuasion and dark patterns that violate users' autonomy (Mathur et al., 2021). Although the guidelines mention in paragraph 11 research methods that can be used to demonstrate GDPR compliance, it is not defined what metrics or criteria would suggest the existence of a dark pattern when, for instance. The Guidelines should consider introducing a measurable threshold or criteria to guide both designers and DPAs.

Example 1: A dark pattern could be established based on a user study showing that a *significant minority of users* have been *misled (FTC, 2022)* by an element of the UI into making an unintended decision in regards of their personal data, which would not require a comparison between two UI.

7.2. **Obligation of means**. The guidelines could provide an obligation of means (as happens with the Guidelines 4/2019 on Article 25) referring to KPIs controllers could use to demonstrate effective implementation of data protection principles.

7.3. **Data protection principles.** Section 2 (paragraphs 8 - 17) provides for a translation of some of the data protection principles into the UI of social media platforms (fairness, accountability, transparency, and data protection by design). We invite the EDPB to provide for a more granular operationalization for the exposed principles and to include other important principles under Article 5 (1) applied to the UI of social media and to dark patterns, e.g., data minimization (which includes proportionality and necessity); purpose limitation (and purpose specification principle), accuracy and 'integrity and confidentiality. This extension to missed principles will enable a better interpretation and application of such principles in concrete cases.

8. Privacy Policies and information provision

Parag 19 mentions that users are asked to confirm that they have read the privacy notice and agree to the terms of use of the social media platform.

8.1. **State of the art methods.** The EDPB could recommend that social media platforms should adopt state of the art methods to design user-centred privacy policies, e.g., i) summaries in layman's

terms, ii) use of visuals such as clips or pictures, iii) different information types to create 'textured agreements' (Kay and Terry, 2010) and [7] which are visually redesigned agreements that employ visual design techniques such as typography and layout and have been deployed to increase the reading time, iv) color-coding could enhance an individual's perception of sensitivity of the data users share (Terpstra et al.,2020).

8.2. ***Multi-channel information.*** *Also, the Italian DPA (Garante Privacy, 2021) refers to the need of a* **multi-channel information notice (eg., by video, pop-up, vocal interaction, virtual assistants, call, chatbots, etc.).** *"Accordingly, the controller should decide the design that works best to ensure completeness, clarity, efficacy, and accessibility. It shall be the responsibility of the data controller to take all appropriate measures to ensure that the information contained in the banner is accessible without discrimination to persons with disabilities who require specific assistive technologies or configurations"*

9. Emotions in persuasive design

9.1 **Fear of Missing Out.** Emotional Steering integrated in social media platform interfaces can result in the development of FoMO-Centric platforms. The **Fear of Missing Out ('FoMO')** is "*a pervasive apprehension that others might be having rewarding experiences from which one is absent*." The phenomenon of FoMO seems to be relevant to social media engagement and has been presented as a 'mediator' associating psychological needs deficits with the use of social media.[8] Concerning the sign-up process, platforms can force users to reveal more personal data by triggering their automatic and unconscious thinking. We consider that the Guidelines should consider this practice of FoMO-centric designs.

9.2. **Emotions in persuasive design.** Interaction design, and design in general, build on triggering emotions on users (Norman, 2004), therefore it is problematic to regulate how emotions are used in the design process. It is not clear where the line of persuasion and manipulation is from the design perspective, nor what the role of emotion plays in it. Consequently, these guidelines aim to target patterns in design that are unlawful according to different regulations, but they do not state how the use of emotions can be unlawful. Considering that deception is already illegal under GDPR and the Consumer Rights Directive, the use of emotions should be unlawful when it is '*misleading or deceptive.'* Establishing an unclear criterion about the use of emotions may potentially hinder the right of creation that designers have associated with their moral rights according to intellectual property laws.

10. Editing issues

[7] Kay, M., & Terry, M. (2010). *Textured agreements: re-envisioning electronic consent.* SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security, 1–13. https://doi.org/http://doi.acm.org/10.1145/1837110.1837127); Kiley Schmidt, 'Empowering users to understand their online privacy rights and choices through an interactive social media sign-up process (2018) https://conservancy.umn.edu/bitstream/handle/11299/196363/Empowering%20users%20to%20understand%20their%20online%20privacy%20rights%20and%20choices%20through%20an%20interactive%20social%20media%20sign-up%20process..pdf?sequence=1&isAllowed=y

[8] Wastin, F., Chiasson, S. (2019). Opt Out of Privacy or "Go Home": Understanding Reluctant Privacy Behaviours through the FoMO-Centric Design Paradigm. Association for Computing Machinery, 57-67. https://doi.org/10.1145/3368860.3368865

If the guidelines are to be adopted, it is commended to regard the following editing issues to provide more readability to the readers.

- **Missing links.** In paragraph 2, the guidelines stated "the perfect interface should be highly personalized, easy to use and multimodal' with a reference link. However, the page does not exist in that link. So, all links and references should be checked to see if they are working and updated.
- **Examples.** The examples given should be presented after a paragraph that refers to that example, and not before, in priority order, to avoid confusion about where the example belongs to. (e.g., Example 29 refers to paragraph 100, though it is presented after paragraph 99); this applies to all the guidelines.
- **Long and repetitive paragraphs.** The guidelines and some paragraphs are unnecessarily long and with diverse types of information – whereas guidelines should be crisp and clear, e.g., paragraph 26. Several dark patterns are mentioned in different case scenarios, like language discontinuity; language and textual aspects are spread over the 64 pages of the document), off-putting and hard to read, and hard to navigate.
- **Some paragraphs are not enumerated,** which, among others, does not facilitate their localization, see for example the beginning of page 14 (ii. Withdrawal of consent – Article 7(3) of the GDPR).
- **Authentication of social media platforms**. From paragraphs 30 to 33 the guidelines comment on aspects regarding authentication according to the data minimization principle; however, the guidelines should align with the same comments and practices provided under the Guidelines for the Right of Access, as of today under the EDPB analysis, instead of providing diverging instructions.

References

Acquisti, A. et al. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. 50 ACM Computing Surveys 1.

Abrams, R. A., Christ, S. E. (2003). Motion Onset Captures Attention. Psychological Science, 14(5), 427–432, p.431. https://doi.org/10.1111/1467-9280.01458; See also Smith, K.C., Abrams, R.A. (2018). Motion onset really does capture attention. Atten Percept Psychophys 80, 1775–1784, p. 1728. https://doi.org/10.3758/s13414-018-1548-1

Bertolini A., Carli R., Human-Robot Interaction and User Manipulation, International Conference on Persuasive Technology, Springer, 2022.

BEUC, "DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS Recommendations for better enforcement and reform, 2022, https://www.bec.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf

Blumenthal-Barby, J.S., Biases and heuristics in decision making and their impact on autonomy. The American Journal of Bioethics 16(5), 2016, pp. 5-15

Bongard-Blanchy K., Rossi A., Rivas S., Doublet S., Koenig V., Lenzini G., "I am Definitely Manipulated, Even When I am Aware of it. It is Ridiculous!"-Dark Patterns from the End-User Perspective, In: Designing Interactive Systems Conference 2021, 2021, pp. 763-776

Bösch, Christoph, Erb, Benjamin, Kargl, Frank, Kopp, Henning and Pfattheicher, Stefan. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns" Proceedings on Privacy Enhancing Technologies, vol.2016, no.4, 2016, pp.237-254. https://doi.org/10.1515/popets-2016-0038

Coeckelbergh M., Human being@ risk: Enhancement, technology, and the evaluation of vulnerability transformations, Vol. 12. Springer Science & Business Media, 2013.

Coons C., Weber M., Manipulation: theory and practice, Oxford University Press, 2014

Distler, V. et al. 2020. The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. New Security Paradigms. Workshop. (ACM 2020). http://dl.acm.org/doi/10.1145/3442167.3442173 (Accessed 5 February 2021).

Federal Trade Commission. The FTC's Endorsement Guides: What People Are Asking. https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking

Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph, and Toombs Austin L. 2018. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI '18). ACM, New York, NY, USA, Article 534, 14 pages. https://doi.org/10.1145/3173574.3174108

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020

Hassenzahl Mark The hedonic/pragmatic model of user experience in Towards a UX manifesto. Conference: Proceedings of the 21st British HCI Group Annual Conference on HCI 2007: HCI...but not as we know it - Volume 2, BCS HCI 2007, University of Lancaster, United Kingdom, 3-7 September 2007 10.14236/ewic/HCI2007.95

Leonard T.C., Richard H., Thaler, Cass R., Sunstein, Nudge: Improving decisions about health, wealth, and Happiness, 2008

Lotto B., Percezioni, come il cervello costruisce il mondo, Bollati Boringhieri, 2017

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

Mantelero A., Esposito M. S., An evidence-based methodology for human rights impact assessment (HRIA) in the development of ai data-intensive systems, Computer Law & Security Review 41, 2021

Mathur, A., Kshirsagar, M., & Mayer, J. (2021, May). What Makes a Dark Pattern. . . Dark? Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, p. 19. https://doi.org/10.1145/3411764.3445610

Norman, D. A. (2004). Emotional design: Why we love (or hate) everyday things. New York: Basic Books.

Rennekamp, K. (2012). Processing Fluency and Investors' Reactions to Disclosure Readability. Journal of Accounting Research, 50(5), 1319–1354. https://doi.org/10.1111/j.1475-679X.2012.00460.

Raz J., The morality of freedom, Clarendon Press, 1986

Rossi A and others, 'When Design Met Law: Design Patterns for Information Transparency' [2019] Droit de la Consommation = Consumenterecht : DCCR 79

Rudinow J., Manipulation, Ethics 88(4), 1978, pp. 338–347

Terpstra, A., Schraffenberger, H., Grassl, P. 2020. Think before you click: How reflective patterns contribute to privacy. Radboud Repository. https;//repository.ubn.ru.nl/bitstream/handle/2066/246490/246490.pdf?sequence=1&isAllowed=y (accessed 2 May 2022).

The European Consumer Organisation. (2022). “DPs” and the EU consumer law acquis, p. 12. https://www.beuc.eu/publications/dark-patterns-and-eu-consumer-law-acquis/html