May 2, 2022

Comments to the EDPB consultation on Guidelines 3/2022 on dark patterns in social media platform interfaces

Introduction

Access Now, Simply Secure, and the World Wide Web Foundation welcome the opportunity to comment on the version of the Guidelines 3/2022 on dark patterns in social media platform interfaces. Access Now is an international civil society organisation that defends and extends the digital rights of users at risk.[1] We work on data protection and privacy worldwide and we maintain a presence in 13 locations around the world, including in the policy centres of Washington DC and Brussels.

Simply Secure is an international civil society organisation, headquartered in the US, working to change whom technology serves.[2] We leverage design as a transformative practice to shift power in the tech ecosystem, working with partners to develop technology that centers people's needs and prioritises data protection, security and privacy.

The World Wide Web Foundation was established by web inventor Sir Tim Berners-Lee to advance the open web as a public good and a basic right.[3] We are an independent, international civil society organisation fighting for a world where everyone has affordable, meaningful access to a web that improves their lives and where their rights are protected.

Our organisations aim to advance essential policy changes and recommendations for enforcement practices necessary to ensure that data subjects can adequately and autonomously exercise their data protection rights in the digital world. In our submission, we will provide comments and suggested edits in a few sections of the draft Guidelines. For ease of reading, we organise these comments

[1] Access Now, https://www.accessnow.org/
[2] Simply Secure, https://simplysecure.org/
[3] World Wide Web Foundation, https://webfoundation.org/, https://techlab.webfoundation.org/

following the structure of the draft Guidelines, rather than organising them by issues. Our analyses focus on a range of topics including:

1. The importance of providing guidance framed around the interference with rights and assessing these interferences and violations,
2. Suggestions on how to present the Guidelines to be most impactful for a broad audience, and
3. How to leverage the Guidelines in the wider civil society ecosystem to contribute to changing the status quo.

Since the adoption of the draft Guidelines, the European Union co-legislators have reached a political agreement on the Digital Services Act that includes measures prohibiting certain types of dark patterns. Dark patterns promote user behaviours that run against the spirit of the General Data Protection Regulation. We welcome this clarification by the legislators and we expect these Guidelines to serve as a tool for the implementation, and future enforcement, of these measures.

General Comments

As an initial matter, we applaud how comprehensively the Guidelines outline principles for transparency, accountability, and data minimisation in the design of user interfaces, providing guidance for the application of these core principles guaranteed under the GDPR. The Guidelines serve as a checklist for identifying particular dark patterns and we believe it will be especially instructive for multi-stakeholders including social media providers, academics, civil society organisations, and designers. Most importantly, these Guidelines will increase the awareness of users regarding their rights, and the risks coming from disclosing too much data or disclosing their data in an uncontrolled way. While the list below is not exhaustive, we would like to highlight our support for the following language of the Guidelines' text:

Paragraphs 1 through 7 (Scope): We support the EDPB efforts to elaborate on the scope of dark patterns and clarify who is responsible and accountable for ensuring GDPR compliance of social media platforms. We support these paragraphs as they identify the need to implement these principles from a technical perspective. The Guidelines explicitly denote the obligations for social media providers to respect the rights to privacy and data protection and the duty owed to data subjects with reference to the principles of lawfulness, fairness, transparency, purpose limitations and data minimisation in the design of user interfaces and content presentation of web services and apps. The text also accurately highlights the relationship between data protection and consumer protection law. These are all key elements in ensuring that technology is used responsibly and does not chip away at or deteriorate user's human rights. Finally, we support the categorisation of dark patterns as a continuously evolving category.

Paragraphs 8 and 9 (Applicable Principles): We further support the EDPB referencing the obligations pursuant Article 25 of the GDPR for social media platforms to implement the principles of data protection by design and by default to provide greater control to users. This language provides a robust roadmap for social media providers. We support the need to create uniform criteria for

principles related to data protection compliance of user interfaces of online applications within the social media sector as well as the EDPB's acknowledgement that Guidelines need to be further developed to this end.

Paragraphs 10 through 15 (Accountability and Transparency): We agree that greater transparency in the design of dark patterns is needed. Companies should design their products and services with and for their most vulnerable users. This principle means, at a minimum, providing easy-to-understand and transparent interface designs that preserve user autonomy and agency. We strongly support these provisions as it holds those companies that do not design their products in such a way accountable.

Paragraphs 16 to 17 (Data Protection by Design): We commend the EDPB's explicit mandate that data processing and the options available to data subjects be provided objectively neutrally, avoiding any deceptive or manipulative language or design.[4] We also support paragraph 16 of the Guidelines explicit outline of the "key elements that controllers and processors have to take into account when implementing data protection by design regarding a social media platform," including the principle of fairness.

Paragraphs 29, 30 and 106 (Data minimisation): Privacy and data protection are fundamental rights in the EU and data minimisation is a core principle to realise these rights. The Guidelines state in clear terms that social media platforms should collect only the data that is objectively necessary for a specific purpose. Expansive data collection has caused significant harm, and risk of harm, for people. These harms range from the more obvious identity theft and physical harms to less obvious examples, such as relationship harms (due to loss of confidentiality), emotional or reputational harms (due to private information becoming public), or chilling effects on speech or activity (due to a loss of trust in government or other organisations). Minimising the amount of data companies collect is one of the best, most human rights-respecting ways, to prevent data and privacy violations and harms.

Recommendations

As expressed in the International Conference of Data Protection and Privacy Commissioners' resolution on "privacy as a fundamental human right and precondition for exercising other fundamental rights," privacy and data protection rights are fundamental to enabling the fulfilment of other rights such as human dignity, freedom of expression, freedom of association and freedom of thought and belief.[5] In the draft Guidelines on dark patterns, the EDPB concretely explains the interactions between privacy and data protection rights with other fundamental rights, particularly within paragraphs 1 to 3 of the sections entitled "Scope." This context is essential to understanding the importance of the draft Guidelines, not only for the protection of the rights to data protection but also

[4] *Paragraph* 16
[5] ICDPPC, *International Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights*
https://edps.europa.eu/sites/edp/files/publication/resolution-on-privacy-as-a-fundamental-human-right-2019-final_en.pdf

for compliance with human right laws, including obligations under the General Data Protection Regulation.

We recommend that the EDPB considers expanding the scope of its Guidelines. We propose that the Guidelines apply not only to social media platform services but also to dark patterns used to mislead data subjects purchasing products on either a website or mobile application. This includes dark patterns found in video games and shopping websites. Together with this extended scope, we recommend that the Guidelines be published so that they are accessible to technical product teams and legal teams addressing GDPR obligations and requirements. As currently written, the Guidelines have extensive guidance on content writing, e.g. tone, clarity, simplicity of language as well as interaction design, but they would not be entirely accessible by those actually building the social media products. By adding annexes, examples, and a developer guide, these Guidelines could help to bridge the gap between legal teams who primarily focus on GDPR implementation and product teams focused on the user experience of the social media platforms.

Much effort has gone into defining and identifying various types of dark patterns and creating taxonomies and tracking examples.[6] Some highlight the characteristics of particular dark patterns, while others describe how dark patterns influence users.[7] While defying any definition, one can understand a "dark pattern" or "deceptive design" as a user interface design or language choice in a product or service that influences a person's decision.[8] Often, people are influenced to make decisions against their interest and/or in the provider's interest, potentially by drawing attention to, or reducing attention to, particular options, statements, or other aspects of the service.

We want to draw attention to recent developments in the taxonomy of dark patterns. The phrase itself, the term "dark pattern" coined in 2010 has recently come under scrutiny for association with "dark" as bad,[9] and multiple actors[10] including the originator of the phrase have updated the term to "deceptive design." However, this document employs the 2010 phrase to align with current regulatory and legislative discussions.

---

[6] Arunesh Mathur, et al., *What Makes a Dark Pattern... Dark?*, CHI Conference on Human Factors in Computing Systems (CHI '21) (May 8–13, 2021), https://arxiv.org/pdf/2101.04843.pdf

[7] *Id.*; Daniel Susser, et al., *Online manipulation: Hidden Influences in a Digital World*, Georgetown Law Technology Review 4.1 (2019), https://philarchive.org/archive/SUSOMHv1; Chris Baraniuk, How 'Dark Patterns' Influence Travel Bookings, BBC (Dec. 12, 2019), https://www.bbc.com/worklife/article/20191211-the-fantasy-numbers-that-make-you-buy-things-online

[8] The original definition from Harry Brignull is "Dark Patterns are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something." DarkPatterns.org, https://www.darkpatterns.org. As of April 28, 2022, this website, along with the term 'Dark Pattern,' has changed to https://www.deceptive.design/, due to the problematic nature of the connotation inherent in the original term that may be discriminative to certain populations.

[9] *See* M. J. Kelly, *What are deceptive design patterns?*, Mozilla, "You may notice we use "deceptive design patterns" rather than "dark patterns" throughout this article. While the latter is commonly used and has been for years, the phrase also reinforces the idea that being 'dark' is 'bad,' which is directly tied to white supremacy." (May 5, 2021), https://blog.mozilla.org/en/internet-culture/mozilla-explains/deceptive-design-patterns/

[10] The World Wide Web Foundation, *Deceptive Design: Moving Towards Trusted Design Patterns* (2022), https://techlab.webfoundation.org/deceptive-design/overview

The EDPB should also consider modifying the proposed definition of dark patterns in the Guidelines to address the consequences of dark patterns on vulnerable groups as well as intent behind the practice of deceptive designs. However, we suggest the following modifications, reflected in bold, to expand on the effectiveness and consequences of dark patterns:

> *4. In the context of these Guidelines, "dark patterns" are considered interfaces and user experiences implemented on social media platforms that ~~lead~~* ***attempts to influence*** *users into making unintended, unwilling and potentially harmful decisions****, often toward a decision that is against the users best interests and in favour of the social media platforms interest,*** *in regards ~~of~~* ***to*** *~~their~~* ***the users*** *personal data. Dark patterns aim to influence users' behaviours and can hinder their ability "to effectively protect their personal data and make conscious choices"4, for example by making them unable "to give an informed and freely given consent". This can be exploited in several aspects of the design, such as interfaces' colour choices and placement of the content. Conversely, by providing incentives and user-friendly design, the realisation of data protection regulations can be supported****. Dark Patterns are effective at influencing data subjects choice, decision-making, and behaviour, even when they are mild. Even minor dark patterns, which apply comparatively less pressure to a person to influence their decision, including by only changing the colour of one option or highlighting some words, can affect individual choice.***

In section 3 of the Guidelines on the "emotional steering," we suggest modifying paragraph 40. Dark patterns are especially effective against a wide range of data subjects, not limited to children, including the elderly, vulnerable data subjects or non-tech savvy data subjects. We propose language to clarify the effectiveness of dark patterns on social media platforms and the importance of providing clear protections around the use of dark patterns, as follows:

> *40. In the light of the above, Emotional Steering at the stage of the registration with a social media platform may have an even higher impact on children,* ***the elderly, vulnerable data subjects and non-tech savvy data subjects*** *(i.e. provide more personal data due to lack of understanding of processing activities), considering their "vulnerable nature" as data subjects.* ***Dark patterns like emotional steering are especially effective against vulnerable data subjects and the elderly.*** *When social media platform services are addressed to children,* ***the elderly or vulnerable individuals,*** *they should ensure that the language used, including its tone and style, is appropriate so that ~~children, as r~~ecipients of the message~~,~~ easily understand the information provided.31 Considering the vulnerability of children,* ***the elderly and other vulnerable data subjects,*** *the dark patterns may influence ~~children~~* ***data subjects*** *to share more information, as "imperative" expressions can make them feel "obliged" to do so to "appear popular among peers".*

Finally, we support the language of paragraph 106 highlighting the principle of data minimisation under Article 5 (1) (c) GDPR. We would, however, suggest the following modifications to improve the text:

106. "Each controller is bound by the principle of data minimisation under Article 5 (1) (c) GDPR, which obliges the controller to only process personal data that are relevant and necessary in relation to the purposes for which they are processed. Moreover, against the background of the accountability principle in the sense of Article 5 (2) GDPR, the controller is responsible for, and must be able to demonstrate compliance with the principles laid down in Article 5 (1) GDPR, such as the principle of data minimisation. ***Users should*** *not* ***be*** *pushed* ***into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data*** ~~***activating more options that are more data sharing invasive, this dark pattern does not seem to go against the above- mentioned principle of data minimisation***~~*. Th*~~***us, t***~~*his pattern* ~~***is not capable of being subject to judicial review, but***~~ *should be improved in a more user-friendly and data restrictive way in order to encourage users to make use of more data restrictive options (which will be further specified in the best practice section)."*

Conclusion

Dark patterns are a serious concern for the protection of fundamental rights, as they can cause extensive harm to people, particularly vulnerable people. The Guidelines have the potential to be an essential resource and contribute to shifting industry practices. We hope that the EDPB will consider our recommendation to limit the term "dark patterns," despite this terminology being used in upcoming EU legislation. The term "deceptive design" is more culturally appropriate, user-centric, and inclusive. We are counting on your guidance and support for this lexicon shift.

To further ensure their broad impact, we encourage the EDPB to frame these in an accessible way for both legal and product stakeholders. In its totality, we are confident that these Guidelines will effectively educate users about the various dark patterns they encounter online and raise the awareness of users regarding their rights. Now more than ever, it is critical for data subjects to understand the risks associated with disclosing too much of their data and the tricks companies often deploy to extract their personal data.

We remain available for any questions you may have.

Sincerely,

Access Now
Simply Secure
World Wide Web Foundation