



Response to the consultation on the upcoming Digital Fairness Act

MTE welcomes the opportunity to provide feedback on the Commission's consultation on the upcoming Digital Fairness Act (DFA). We are happy to be able to provide the perspective of a diverse range of mid-sized companies seeking to ensure that the regulatory approach is consistently proportionate, adaptable and relevant to all the online players in scope and ensures a harmonized, consistent and clear legal framework for businesses.

Dark patterns

The Fitness Check identified the need for a more coherent and structured regulatory response to the issue of dark patterns, which are a growing concern across digital services. Indeed, dark patterns are currently tackled inconsistently throughout the EU legislative framework - notably in Article 25 Digital Services Act (DSA), Article 6(1) Unfair Commercial Practices Directive (UCPD), Article 5(1) AI Act and the General Data Protection Regulation (GDPR). While this framework provides ample rules, the lack of consistency and harmonization across intersecting areas of regulation - including the absence of a common definition of "dark pattern" - creates some operational and legal uncertainty for certain providers.

The term "dark pattern" may be currently used as a catch-all concept, encompassing a wide variety of user interface practices, some of which may have significantly different purposes, contexts, and impacts on users.

We believe that this existing lack of consistency could be addressed through non-binding guidance on the basis of the definition already provided in Article 25(1) of the DSA, clarifying that it applies only to practices for which there is evidence of negative effects on users.

Addictive design

We disagree that further rules on so-called addictive designs are needed in the DFA. Concerns about addictive designs should be considered from a risk-based perspective under the DSA, which tackles them both in the draft guidelines on the protection of minors under Article 28(1) of the DSA, and VLOP-specific obligations on systemic risks and their mitigation. The Commission has notably already launched investigations relative to addictive designs under the DSA.



Features such as continuous scroll, autoplay or notifications are part and parcel of contemporary user experience design and are not inherently harmful. Over-regulation in this space could prevent platforms from promoting beneficial increases to user engagement, for example by rewarding users for walking. In this example, streaks are seen as an achievement and reward users that have been physically exercising on a daily basis - users are never penalized for having broken a streak. The efficiency of an incentive-based digital nudge in increasing healthy and environmentally-friendly behavior has notably been supported by [scientific studies](#). Furthermore, it is important to highlight that "streaks" or other rewards are a core part of how consumers engage with these platforms and they provide delight, fun and an appreciated challenge for users. Users have demonstrated a desire for these features and enjoy engaging with them.

Creating additional horizontal rules and applying them to a broader range of services without accounting for the level of service risk and outcome for users would have unintended consequences by imposing disproportionate cost and burden on low-risk services and eliminating features that many users find useful and desirable (indeed, many users expect some of these features as a baseline offering). For example, the same underlying technology enables online news services to offer EU consumers a more varied diet of curated content across news, entertainment and sport, and this has positive consumer benefits by exposing consumers to different political and cultural viewpoints. Further unnecessary regulation would be contrary to the DFA's stated objective of only addressing existing gaps. Instead, effective implementation and oversight of the existing DSA is the preferred solution.

As for recommender systems, those are subject to restrictions under the DSA that were driven primarily by concerns related to specific, large social media companies' content curation practices. However, we emphasize that personalization offers significant benefits - recommending content that is known by a service to be both safe and high-quality, helping users find content and information that is relevant to their expressed interests, inspiring new ideas, boosting workflows, fostering communities, enabling user-driven assessment of content quality, and ensuring age-appropriate experiences for younger users. Examples by some of our members show that highly personalized recommender systems can actually reduce addictive patterns by prioritizing quality over engagement, providing users control over their feeds, and avoiding viral content amplification. As such, we would particularly caution against ideas such as mandating the switching off of personalization-based recommender systems by default. A blanket and undifferentiated solution would fail to recognize the benefits of personalized practices valued by consumers - and indeed



expected by them – which are offered by numerous services, including many of our members.

[Specific features in digital products, such as in video games](#)

We would like to underline that the existing horizontal consumer protection framework (in particular Article 5 and Annex I point 28 UCPD prohibiting direct exhortations towards children, as well as Article 7 UCPD and article 6(1) Consumer Rights Directive (CRD) including information requirements on the price and main characteristics of the product) remain fully applicable to in-game purchases. The Consumer Protection Cooperation (CPC) Network is currently discussing with industry its 'Key Principles on Virtual In-game Currencies', on the basis of which the video games industry is developing practical proposals to provide consumers with meaningful transparency over the purchases they are making. Whilst we agree that this transparency is important, and is valued by consumers, we believe that the EU should prioritize the enforcement of existing rules, instead of proposing additional, potentially overlapping rules on an already complex issue, which would likely go against the overarching goals of simplification, harmonization and legal certainty. Moreover, the approach taken in the CPC principles runs counter to the current, accepted approach under consumer law that use of in-game currencies to purchase other in-game items is digital content, rather than a real-money transaction. Moving to classify this as a real-money transaction is not only a mischaracterization of this user interaction, it would also be highly disruptive to users' experience. It would entail several additional steps, such as delivering pre-contractual information at each point they might choose to use their in-game currency, without any meaningful addition to their overall protection as a consumer.

Similarly on the specific issue of the protection of minors relative to video games, the legal landscape is already comprehensive and complex, notably with the existing provisions in the DSA and its Article 28 guidelines on the protection of minors. As such we wish to underline that any provisions included in the DFA should be without prejudice to the guidelines so as to avoid conflicts and overlaps for those services who could have functionalities that would fall under both.

On the issue of in-app purchases, it should be highlighted that many actors in the ecosystem including some of our members already have parental controls in place for spending, as well as the possibility for parents to set parameters. Generally speaking, in-app purchases and currencies have pro-consumer benefits: they make for a more seamless, immersive and interesting gaming experience that is separate from the commerce



environments in which players can make transactions. Virtual currencies play an important role in this, enabling in-game experience that consumers appreciate, and allowing users to engage in a way that would not otherwise be possible with a real money purchase (for example through sub 1 euro value transactions). Adding requirements for pre-contract information at every point where a user redeems a virtual currency would significantly impact this experience for consumers. Moreover, services which have closed-loop systems in place, meaning that users cannot “cash out” of the virtual in-app currency, are widely appreciated by users who see it as a natural and welcomed part of their experience with a service. Mechanisms that enable users to progress more rapidly in a game are inherent to the economic model of freemium games. At the same time, it should be highlighted that companies already have measures in place to avoid the creation of addictive behaviors.

Overall, it is also important to bear in mind that the videogames sector is a varied ecosystem with different players across the gaming industry taking different approaches to in-service currencies and purchases. Therefore, a one-size-fits all would neither be proportionate nor flexible to allow for innovation. We would also like to emphasize Europe’s leadership in the video games industry, and the potential risks that regulation could pose to Europe’s competitiveness in this sector.

Unfair personalization practices

We note that existing regulatory frameworks, in particular the GDPR (Recital 38, Articles 8, 22) and the DSA (Articles 28, 38) already provide strong safeguards in this area. These include rules on transparency, profiling, lawful bases for processing, user consent, and recommender system transparency. Article 5(1)(b) AI Act also prohibits AI systems that exploit vulnerabilities of an individual due to a range of protected characteristics. In addition, the personalization of advertising is specifically addressed in the GDPR, ePrivacy Directive, UCPD, CRD and the Regulation on the Transparency and targeting of political advertising (TTPA).

Importantly, both the GDPR and the DSA include specific provisions aimed at protecting minors, such as limitations on profiling and targeted advertising for children, and reinforced transparency obligations.

Introducing additional horizontal prohibitions on personalization - without clearly articulating how they complement existing obligations - may create regulatory overlap and lead to legal uncertainty for service providers. It also risks ignoring the many benefits that



consumers gain from personalization such as making information more discoverable, saving time and receiving vouchers and other financially beneficial offers.

[Harmful practices by social media influencers](#)

Despite this issue already being tackled in the UCPD, several member states including France, Spain, Germany and Hungary have already or are in the process of adopting further rules regulating influencer marketing. In order to avoid a fragmentation of the rules and to ensure legal clarity and certainty, we would be supportive of a light-touch, EU-wide framework clarifying definitions and obligations for players concerned. Notably, we would support initiatives aimed at raising awareness and providing educational material to influencers, who may not be aware of their own obligations and of their status as traders under the UCPD.

[Issues with digital contracts](#)

Digital contracts, including subscriptions, are comprehensively covered in existing regulation, for example: Articles 7 and 9 UCPD (and 2021 guidance) specify that cancellation should be as easy as signing up; the CRD requires traders to provide upfront information about the duration of a contract and how to cancel; the DSA regulates online platform subscriptions. Additional requirements to these would create an increasingly difficult set of competing laws rendering implementation difficult for services, and also risk a less user-friendly experience for consumers. We would therefore caution against mandating additional unduly prescriptive one-size-fits-all design solutions such as cancellation buttons which could have unintended consequences such as preventing a provider from first verifying the identity of the user and taking steps to eliminate fraudulent action. We would favor instead greater effort with the implementation and oversight of existing rules focused on desired outcomes while leaving a certain degree of flexibility for digital services to achieve them. Companies often need more information from the user when it comes to cancellation, so mandating a “one click” means it won’t be adapted to various service types and could lead to costly disruptions to well-established systems and user journeys. There is also often important information to convey to a user that they need to know, such as which perks they may lose by cancelling and when this will take effect for example, similar to the disclosure of pre-contractual information during the sign-up process.

Furthermore, mandating companies to send consumers even more reminders than they already do regarding their contracts and subscriptions may be counterproductive and could lead to “reminder fatigue.” In our experience, consumers typically find that the current



system works well and would likely find extra reminders irritating, as has been shown with cookies over the years. Furthermore, mandating consent before a renewal or free trial to paid subscription conversion could result in unwanted lapses in the service, where an automatic renewal has already been accepted by the consumer upon signup.

Simplification

MTE welcomes the Commission's commitment to the EU's competitiveness goals and prioritizing the simplification of EU regulation in order to reduce unnecessary regulatory burdens and incentivize investment and growth in the single market. This is particularly important for mid-sized tech firms for whom it is vital that regulatory compliance can be managed wholly in their country of establishment and operational costs of doing business in the EU rationalized accordingly. We noted above key areas where we see existing overlapping requirements stemming from consumer protection legislation and its interaction with other existing legislation, for example, the requirement for platforms to be transparent about the parameters used in their recommender systems, which can be found in the UCPD, CRD, DSA as well as Platform-to-Business Regulation (P2B), and could be streamlined. However, we believe any issues arising can mostly be addressed via the ongoing simplification program and do not require new regulation via the DFA.

MTE would note the risk that the introduction of the DFA may run against the EU's stated intention to simplify the regulatory landscape for businesses such that economic growth can be kick-started; a key strategic goal for the region. It seems that the DFA proposals are aimed at several areas already addressed by other pieces of landmark EU regulation and, in our engagement with policymakers, the policy gap that the DFA seeks to fill has not always been clear or evidence-based. We would therefore urge the Commission to consider what can be achieved by clarifying and simplifying existing EU laws, in particular via uniform implementation and guidance in consultation with providers and other stakeholders, before pursuing the development of a new major piece of regulation, which may be unnecessary and disproportionate for digital services in the EU, in particular mid-sized and smaller providers.

We would further note that certain proposals made in the context of the DFA may conflict with specific simplification consultations, for example the review of existing ePrivacy Directive rules regarding cookies to explore what uses have become essential to providing online services today and could be considered low risk under a different legal basis. This, for instance, could allow publishers to continue to deliver online advertising to users who have rejected cookies and where there is a low risk to their privacy. Other jurisdictions -



including the UK - are similarly reviewing cookie rules to ensure requirements align with privacy risk and do not inadvertently act as barriers to sustainable consumer services and investment. Again, it would run contrary to the EU's growth strategy if we create additional rules through the DFA while a neighboring and competing jurisdiction is actively simplifying its rulebase and compliance processes.

Horizontal issues

Digital products that are not high-risk and not designed for minors, nor target them but can be accessed by them, should not be required to invest in potentially expensive age verification/age estimation technologies solely because they may contain certain engagement features (such as scroll, rewards or notifications).

Considering the DSA's Article 28 guidelines on the protection of minors as well as President von der Leyen's announcement that the Commission would be looking into imposing age verification for certain services at the EU level, we are concerned that overlegislation in this area would compound legal uncertainty. In this context, the need for a clear EU-level legal framework on this matter cannot be overstated especially as Member States are also looking to impose their own rules. In our view, the Article 28 DSA guidelines take a risk-based approach and are adaptable to each platform, and their implementation should be the priority. Given the breadth of application of the EU consumer acquis and the need for proportionality, any consideration of additional rules to protect minors under this framework must be both evidence-driven and risk-based and this would require a specific assessment which has yet to be undertaken.

Middle Tech Europe stands ready to continue engaging with policymakers on the discussions leading up to the DFA to ensure it is targeted, evidence-based, proportionate and relevant for all companies in scope.