24 October 2025

Centre for Information Policy Leadership Submission to the European Commission's Call for Evidence on the Digital Fairness Act

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to provide input to the European Commission's call for evidence[2] on the Digital Fairness Act (DFA).

CIPL supports the Commission's commitment to strengthening the high level of consumer protection in the digital environment. As the Fitness Check of EU Consumer Law on Digital Fairness concluded, it is imperative that: "existing consumer protection rules remain relevant and necessary to ensure a high level of consumer protection and effective functioning of the digital single market".[3] However, we believe that these goals could be achieved more effectively through targeted, strategic interventions within the existing legal framework rather than through a new, standalone legislative act.

We recommend that, rather than adding further complexity to the digital legislative landscape by creating a new Digital Fairness Act, the European Commission should:

- **Ensure coherence in the existing framework:** The issues raised under the proposed DFA are already covered by existing instruments, including the GDPR, DSA, DMA, AI Act, DA and UCPD. The Commission should focus on ensuring consistency and coherence between these laws rather than creating new obligations that risk duplication or confusion.
- **Strengthen enforcement and compliance support:** Priority should be given to consistent, effective enforcement of existing laws across Member States and to engagement with organisations, particularly small and medium-sized enterprises (SMEs), to promote a clear understanding and application of existing obligations.
- **Provide updated interpretative guidance:** The Commission should clarify areas of uncertainty by updating existing guidance and developing additional materials where needed to reflect evolving technologies and business models.
- **Conduct robust impact assessments:** Before considering any further legislative initiative, the Commission should carry out comprehensive, evidence-based assessments of potential economic and compliance impacts, with particular regard to SMEs.
- **Use legislative amendment only as a last resort:** Where genuine legal gaps are identified, these should be addressed through narrowly targeted and proportionate amendments to existing legislation rather than through a new standalone act.

---

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] European Commission, "Commission Launches Open Consultation on the Forthcoming Digital Fairness Act," Digital Strategy, July 17, 2025, https://digital-strategy.ec.europa.eu/en/consultations/commission-launches-open-consultation-forthcoming-digital-fairness-act.

[3] European Commission. *Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness*. Brussels, October 3, 2024, 707d7404-78e5-4aef-acfa-82b4cf639f55_en.

The recent reports by Enrico Letta[4] and Mario Draghi[5] have identified the proliferation of overlapping digital regulations, persistent regulatory fragmentation, and the associated continued increase in compliance costs for organisations as key impediments to growth and innovation in the EU. The European Commission itself has acknowledged in its *Competitiveness Compass* the growing regulatory complexity that businesses operating online face.[6]

A joint letter from the European Council President, Antonio Costa, and 19 EU Heads of State and Governments, also explicitly calls for a *substantial change of course* to restore Europe's competitiveness. In particular, the open letter calls for: "**self-restraint when it comes to new legislation, which should anyway come with strengthened impact assessments. <…> Nothing less than a cultural change is needed. Europe must limit itself to the bare minimum of new regulation in full compliance with the principles of subsidiarity and proportionality**".[7]

Instead of new regulations, simplification and coherence must become the mindset to create a predictable innovation-friendly environment that can, at the same time, guarantee a high standard of consumer rights. Any new proposal should be supported by a current comprehensive and evidence-based impact and necessity assessment that must be able to point to an actual legal lacuna.

Against this backdrop, CIPL urges the Commission to carefully assess the viability and added value of the DFA.

CIPL sets out below a series of more detailed observations in response to the issues identified in the explanatory memorandum accompanying this Call for Evidence, with our response also reflecting the EU survey elements published by the European Commission[8].

[4] Enrico Letta, *Much More Than a Market: Speed, Security, Solidarity – Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens*, Brussels, Council of the European Union, April 2024, https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf.

[5] European Commission, *The Future of European Competitiveness: Report by Mario Draghi*, Brussels, September 3, 2024, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

[6] European Commission, *Competitiveness Compass*, Brussels, January 29, 2025, https://commission.europa.eu/topics/eu-competitiveness/competitiveness-compass_en.

[7] Ibid.

[8] European Commission. *Public Consultation on the Digital Fairness Act (OPC_DFA)*. EUSurvey, https://ec.europa.eu/eusurvey/runner/OPC_DFA?surveylanguage=en.

1. Dark Patterns

To the extent that a proposed Digital Fairness Act (DFA) aims to address dark patterns, CIPL would like to emphasise that these practices are already covered, either directly or indirectly, under the existing EU regulatory framework, including:

- General Data Protection Regulation (GDPR)[9],
- Digital Services Act (DSA)[10],
- Digital Markets Act (DMA)[11],
- Artificial Intelligence Act (AI Act)
- Data Act (DA)[12]
- Unfair Commercial Practices Directive (UCPD) [13],

In addition, the European Data Protection Board (EDPB) has provided *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces*[14], which specifically address manipulative interface design practices. Further interpretative and enforcement guidance has also been issued by other EU and national bodies.[15]

---

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 4 May 2016, http://data.europa.eu/eli/reg/2016/679/oj.

[10] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27 October 2022, http://data.europa.eu/eli/reg/2022/2065/oj.

[11] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 October 2022 on contestable and fair markets in the digital sector (Digital Markets Act), Official Journal of the European Union L 265, October 27, 2022, https://eur-lex.europa.eu/eli/reg/2022/1925/oj/.

[12] European Parliament and Council of the European Union. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal of the European Union, L 322, 22 December 2023, https://eur-lex.europa.eu/eli/reg/2023/2854.

[13] European Parliament and Council of the European Union. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance). Official Journal of the European Union, L 149, 11 June 2005, https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng.

[14] European Data Protection Board. *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces*, 24 February 2023, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

[15] *European Commission, Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021/C 526/01), OJ C 526, 29 December 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021XC1229%2805%29;* BEUC. *Better Safe Than Sorry: Position Paper on How to Keep Children Safe Online in the EU*, 18 February 2025, https://www.beuc.eu/position-papers/better-safe-sorry; OECD. *Dark Commercial Patterns*. OECD Digital Economy Papers, No. 336, October 2022, https://doi.org/10.1787/44f5e846-en; European Commission, "Consumer Protection Cooperation Network", https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en.

Examples of EU Digital Acquis Laws Addressing Dark Patterns
GDPR While the GDPR does not explicitly refer to dark patterns, the Regulation as a whole provides a comprehensive framework to address manipulative design practices. Provisions such as Article 5(1)(a) on fairness, Article 12 on transparency, Article 5(1)(b) on purpose limitation, Article 5(1)(c) on data minimisation, Article 6 on lawfulness of processing, Article 7 on consent, Article 22 on automated decision-making, and Article 25 on data protection by design and by default, collectively form a robust foundation to address dark patterns.
DSA The DSA explicitly prohibits dark patterns. Recital (67) of the DSA defines dark patterns as practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Additionally, Article 25 DSA prohibits online interface designs that deceive, manipulate, or impair users' ability to make free and informed choices.
DMA The DMA also contains provisions to prevent manipulative design, particularly through its anti-circumvention measures. For example: • Article 13(4) of the DMA prohibits gatekeepers from engaging in any behaviour that undermines effective compliance with the obligations, regardless of whether that behaviour is of a contractual, commercial, or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design. This broad wording directly targets practices akin to dark patterns that could undermine the effectiveness of the DMA's obligations. • Recital (131) further clarifies this, stating that such behaviour includes the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice.
AI Act The AI Act refers to dark patterns in the context of prohibiting AI practices that use subliminal, manipulative, or deceptive techniques to distort behaviour and undermine informed decision-making (Article 5(1)).
UCPD The UCPD introduces explicit prohibitions and transparency requirements for specific manipulative and misleading commercial practices, without explicitly referring to dark patterns. For example: • Misleading commercial practices are prohibited if they contain false information (Article 6(1)), or hide material information[16] or provide it in an unclear, ambiguous, or untimely manner (Article 7(1) and 7(2)). • Aggressive commercial practices are prohibited if they significantly impair the average consumer's freedom of choice through harassment, coercion, or undue influence (Article 8). • Recitals 19, 20 and 21 (as amended by the European Parliament and the Council)[17] refer to the impact of ranking on consumers and stress the need for transparency, noting that parameters

[16] Material information includes the (i) main product characteristics, (ii) the geographical address and the identity of the trader, (iii) the price inclusive of taxes, (iv) the arrangements for payment, delivery, performance and the complaint handling policy and (v) the right of withdrawal or cancellation (Article 7(4)).

[17] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC, and 2011/83/EU as regards the better enforcement and modernisation of Union consumer protection rules, Official Journal of the European Union L 328, 18 December 2019, https://eur-lex.europa.eu/eli/dir/2019/2161/oj.

determining ranking include algorithmic sequencing, rating or review mechanisms, and visual highlights.
DA The DA also addresses manipulative practices and dark patterns: • Recital 51 defines dark patterns as design techniques that push or deceive consumers into decisions that have negative consequences for them. • The DA also imposes specific prohibitions on third parties (Article 6 (2a)) and data holders (Article 4 (4)) regarding manipulative practices and data use to protect user autonomy and market fairness. Both are prohibited from using dark patterns by ensuring they do not make the exercise of choices or rights by the user unduly difficult (e.g., by offering choices to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a user digital interface or a part thereof).

CIPL recommends that policymakers focus on ensuring better and more consistent enforcement of existing EU and national rules, rather than creating new legislation. The EU already possesses a comprehensive and well-equipped legal framework, including the GDPR, DSA, DMA, UCPA, DA and AI Act, to address various aspects of dark patterns. Introducing a new legislative instrument would not add substantive value in this context; rather, it would increase complexity and regulatory overlap, creating further compliance burdens for organisations.

Given the EU's mixed record in resolving overlaps and inconsistencies across its digital regulatory framework, CIPL cautions that additional legislation could exacerbate these tensions. Instead, clear regulatory guidance should be the next step to promote consistent interpretation and enforcement across Member States.

Accordingly, CIPL urges the European Commission to avoid duplicating existing obligations and instead focus on clarifying overlaps and promoting coherent enforcement across the current framework. Additionally, CIPL believes that the EU should take a holistic perspective when regulating dark patterns, taking into account online and offline practices. This is because many practices that are labelled as dark patterns online are accepted marketing techniques offline.

2. Addictive Design

To the extent the Commission is considering further legislating on addictive design features, CIPL would like to point out that this topic is already addressed under the DSA, DMA and the AI Act, each of which contains provisions that touch upon or mitigate risks associated with addictive or manipulative design practices.

For example, the DSA considers addictive design in the context of risk assessments for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). Recitals 81 and 83 of the DSA identify online interface designs that may stimulate behavioural addictions as a systemic risk. Furthermore, Article 34(1)(d) requires VLOPs and VLOSEs to identify, analyse, and assess actual or foreseeable negative effects in relation to minors, including risks arising from online interfaces that may cause addictive behaviour.

The AI Act prohibits AI systems that exploit vulnerabilities related to age, disability, or social or economic situation in ways that are likely to cause significant harm, including through addictive or manipulative design (Article 5(2)).

Both DSA and DMA introduce requirements for recommender systems, which could be linked to addictive design:

- **Transparency and control over recommender systems (DSA):** Online platforms using recommender systems must clearly set out, in plain and intelligible language, the main parameters used in those systems and provide users with options to modify or influence them. For VLOPs and VLOSEs, at least one recommender system option must be available that does not rely on profiling. This requirement enhances user autonomy by enabling consumers to exercise greater control over how content is prioritised and presented, *reducing the risk of manipulative engagement-driven design*. Design features that deceive or manipulate users, distort or impair their ability to make informed decisions, or otherwise subvert their autonomy are therefore covered by the DSA.
- **Protection of minors (DSA):** The DSA explicitly recognises the risks posed by interface designs that exploit the weaknesses or inexperience of minors, or that may cause *addictive behaviour*. Providers of platforms accessible to minors must therefore implement appropriate and proportionate measures to ensure a high level of privacy, safety, and security for children.
- **Fair design and user autonomy (DMA):** The DMA prohibits gatekeepers from treating their own services more favourably in ranking, indexing, or crawling—provisions that also extend to recommender systems where these are used to promote a gatekeeper's own products or services. While the DMA does not explicitly reference addictive behaviour in adults, it prohibits conduct that "subverts or impairs user autonomy, decision-making, or choice" through interface design.

Taken together, the existing regulatory framework already provides mechanisms to address concerns around addictive design, particularly through consumer protection provisions and systemic risk management, with a strong emphasis on protecting minors. In parallel, many organisations are proactively addressing digital well-being by integrating tailored features across their services and devices to promote balanced and responsible usage. Policymakers should recognise and leverage these industry-led best practices when assessing whether additional regulation is necessary. Any initiatives must strike a balance between privacy, safety, and user autonomy to access legal and appropriate content.

3. Unfair personalisation practices

CIPL believes that personalisation, *per se*, is not inherently harmful to consumers. On the contrary, personalisation can enhance user experience, support access to free online content, and drive economic growth.[18] Personalisation improves user engagement by offering more relevant and curated content as opposed to random or even inappropriate or potentially harmful content.

[18] Centre for Information Policy Leadership and Public First. *The Impact of Digital Advertising on Europe's Competitiveness: A Study on the Role of Digital Advertising in Europe*. March 2025, cipl public first the impact of digital advertising eu competitiveness study mar25 .pdf. The study also highlights the substantial economic contribution of personalised advertising to small and medium-sized businesses (SMBs) across the EU. Specifically:

- 86% of EU SMBs reported increased revenue due to personalised advertising;
- 80% reported attracting more customers;
- Limiting personalisation would lead to challenges in customer acquisition (73%), higher marketing costs (38%), reduced revenue (46%), and potential price increases (47% of SMBs, 51% of large advertisers).

Personalisation is furthermore already addressed, at least in part, under existing legislation, namely the *GDPR* (Article 22), the *DMA* (Article 5(2)), and the *DSA* (Articles 26 and 28).

To the extent that the Commission is considering introducing broad or ambiguous definitions, such as "vulnerabilities", to prevent personalisation under certain circumstances, it is not clear how such terms would be defined vis-à-vis Article 9 of the GDPR, for example. **This would also introduce the potentially paradoxical situation of having to collect data on and profile an individual based on sensitive information to avoid personalisation.**

Accordingly, CIPL recommends that any new EU action in this area should build upon the existing regulatory framework rather than introduce further complexity.

4. Harmful practices by social media influencers

The European Commission notes some concerns in relation to social media influencers, including issues such as hidden marketing and the promotion or sale of potentially harmful products. The UCPD explicitly recognises that consumers increasingly rely on reviews and endorsements when making purchasing decisions. It therefore establishes specific requirements for traders who provide access to consumer reviews:

- **Authenticity of reviews**: Traders must inform consumers whether procedures are in place to ensure that published reviews originate from individuals who have actually purchased or used the products.
- **Transparency of verification**: Where such procedures exist, traders must explain how these checks are conducted.
- **Disclosure of processing practices**: Traders must clearly state how reviews are processed, for example, whether all reviews, both positive and negative, are published, and whether any reviews or endorsements have been sponsored or influenced by a contractual or commercial relationship with the trader.

The UCPD considers it an unfair commercial practice to mislead consumers by claiming that product reviews were submitted by genuine users without taking reasonable and proportionate steps to verify their authenticity. It further prohibits traders from submitting false consumer reviews or endorsements, such as artificial "likes" on social media, or from commissioning others to do so for promotional purposes. The Directive also prohibits the manipulation of consumer reviews, including the selective publication of positive feedback or the deletion of negative reviews. These provisions directly address the problem of hidden marketing and deceptive promotional practices often associated with influencer activity.

Where the promotion or sale of potentially harmful products involves deceptive marketing, omission of material information that influences a consumer's transactional decision, or aggressive selling tactics, such behaviour falls squarely within the scope of unfair commercial practices. Member States' competent authorities are responsible for assessing and addressing these infringements on a case-by-case basis. The UCPD also guarantees that consumers affected by unfair commercial practices have access to proportionate and effective remedies, including compensation for damages, price reductions, or contract termination.

Commercial practices by social media influencers, such as failure to disclose commercial intent or the promotion of misleading or harmful claims, constitute an area where coordinated EU action could reduce fragmentation across the Single Market, which currently arises from divergent national laws and

interpretations. Such coordination would provide a dual benefit: it would enhance consumer protection while also promoting regulatory harmonisation and legal certainty for market participants.

In view of the above, CIPL believes that EU action in this area should focus on providing clearer guidance and more consistent enforcement of the existing rules rather than introducing new legislation. Strengthened and harmonised implementation across Member States would support both effective consumer protection and the smooth functioning of the Single Market, which is currently challenged by overlapping and sometimes inconsistent national regulatory approaches.

5. Simplification measures

The Digital Fairness Fitness Check identified the potential for targeted simplification of EU consumer law. CIPL welcomes initiatives aimed at simplifying and streamlining EU consumer law. A well-functioning and coherent Single Market benefits both businesses and consumers alike. However, introducing a new, standalone legislative instrument increases regulatory complexity without a clearly identified legal gap would run counter to the spirit of simplification and greater legal restraint that the European Council and Member States have been advocating in relation to the Commission's work programme.

In this context, CIPL believes that the Digital Omnibus Package represents the most effective and pragmatic avenue for achieving genuine simplification in the area of online consumer protection. The proactive measures contained within this package leverage digitalisation to streamline compliance, reduce administrative burdens, and enhance regulatory efficiency. This approach aligns with the broader objectives of fostering innovation, promoting competitiveness, and strengthening consumer trust in the digital economy, without introducing unnecessary layers of new regulation.

CIPL would also like to make reference in this context to our submission for the Digital Omnibus package from 14 October 2025, which identifies the necessary elements for a successful Simplification exercise.[19]

[19] Centre for Information Policy Leadership (CIPL), Submission to the European Commission Public Consultation on the Simplification of the Digital Package and Omnibus Directive, 14 October 2025, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33088830_en.