AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Digital Fairness Through Simplification

Reinforcing Consumer Protection Without Regulatory Overload

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €4 trillion in 2023, directly supports more than 4.6 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

As the European Commission pursues its simplification agenda, it should prioritise strengthening existing consumer protection laws rather than creating new overlapping obligations. To protect consumers online, increase regulatory certainty and consumer trust and ease administrative burdens for businesses, the Commission's digital fairness strategy should focus on:

- **Avoiding regulatory overlap:** new rules risk duplicating obligations, increasing legal complexity and undermining regulatory certainty.
- **Promoting simplification and competitiveness**: digital fairness proposals should align with the Commission's simplification agenda, fostering innovation and EU competitiveness.
- **Supporting evidence-based policy:** new measures should be based on an updated Digital Fitness Check, supported by data and real market need, targeting clearly harmful practices.
- **Ensuring consistent application of existing consumer protection laws**: existing EU laws already address key digital fairness concerns such as dark patterns, deceptive design, subscription traps and targeted advertising.
- **Strengthening enforcement:** gaps in consumer protection arise from inconsistent enforcement, not a lack of legislation. Proper enforcement should be the EU Commission's top priority, producing deterrent effect across the Single Market.
- **Encouraging public-private solutions:** Issue guidance, explore self-regulation and partnerships between regulators, industry and consumer groups as more agile alternatives to legislation.
- **Preserving innovation incentives:** avoid prescriptive design mandates such as mandatory one-click cancellations that risk constraining service design and innovation in user experience. Instead, principle-based, cross-sector standards offer the flexibility for digital businesses to address digital fairness concerns effectively while continuing to innovate.

Any future digital fairness laws should support proportional, targeted measures that complement current legislation without reopening settled areas of the digital rulebook. Particular attention should be paid to enforcement, legal certainty and risk-based intervention to ensure simplification.

Introduction

New digital fairness legislation aims to address the possible harmful effects of digital practices such as dark patterns and online profiling, despite the EU's significant body of existing consumer protection and digital laws. The introduction of this legislation contradicts the EU's ongoing efforts to simplify and streamline EU regulation to support competitiveness and innovation in the region. Existing EU digital and consumer protection laws already offer reliable standards for transparency and appropriate remedies.

The EU already has a comprehensive consumer protection and digital regulatory legal framework in place, which includes instruments such as the Unfair Commercial Practices Directive (UCPD), the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), the Artificial Intelligence Act (AIA), the Audiovisual Media Services Directive (AVMSD), and the

Political Advertising Regulation (PAR). Together, these laws collectively address many of the concerns identified in a potential DFA's scope. For example:

- Existing laws comprehensively cover concerns outlined in the digital fairness fitness check, from withdrawal rights to contract terms as well as extensive case law and decisions for those instances where unfair contract terms are used.
- Basic principles around aggressive commercial practices or undue influence, or more generally misleading practices, are already in place and enforced across the EU.

Rather than introducing new layers of regulation, regulatory efforts and public resources should focus on coherent, consistent and effective implementation and enforcement of existing laws. Many digital consumer protection laws are recent and still in the early phases of implementation. For example, the 2019/2161 Modernisation Directive, [1] which was designed to update consumer protection rules for the digital age, is still undergoing national transposition and implementation in several Member States.[2]

In its 2024 review, the Commission acknowledged that it is too early to assess the full impact of the Modernisation Directive.[3] Since its adoption in 2019, the Modernisation Directive has been complemented by the Digital Services Act (DSA), the Digital Markets Act (DMA), the Artificial Intelligence Act (AIA) and updates to the General Product Safety Regulation (GPSR) and Product Liability Directive (PLD). Given this evolving landscape, regulatory stability and enforcement should be prioritised over legislative expansion. Overlapping or duplicative rules risk undermining legal certainty, increasing compliance costs and discouraging innovation.

The existing EU consumer and digital legislation already offers a harmonised framework across Member States. While concerns about regulatory fragmentation are valid, the emergence of 27 divergent approaches stems not from a lack of legislation, but from inconsistent enforcement. To avoid fragmentation, efforts should focus on ensuring consistent application and enforcement of these rules, rather than creating parallel obligations under a new instrument. Specifically, this could be actioned through targeted guidance and improved coordination would be more effective than introducing new, overlapping rules.

Policymakers should take a risk- and evidence-based approach that supports consumer trust and economic competitiveness, not unnecessary complexity. Digital fairness should be viewed through a simplification lens: as an opportunity to cut red tape and boost the competitiveness of the European economy.

This paper outlines practical, proportionate approaches based on the existing legal framework to address digital fairness challenges while maintaining regulatory coherence.

---

[1] 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 of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance)

2 Cf i.a. Recital 17, 27, 30, 31

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0258R%2801%29&qid=1726811961274

Digital fairness: challenges and solutions

Dark patterns

The use of manipulative or misleading interface design – commonly referred to as dark patterns – is already addressed comprehensively under existing EU law. While the term itself is not uniformly defined in legislation, the relevant practices fall squarely within the scope of several legal instruments.

- Unfair Commercial Practices Directive (UCPD) (Directive 2005/29/EC): This directive prohibits misleading and aggressive business-to-consumer commercial practices. Annex I provides a list of practices deemed unfair in all circumstances, many of which cover typical dark pattern techniques.

- Digital Services Act (DSA) (Regulation (EU) 2022/2065): Article 25 explicitly prohibits online platforms from using deceptive design patterns that impair user autonomy, particularly in consent and choice architecture.

- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679): GDPR reinforces consumer protection by requiring transparency and lawful consent for data processing (Articles 5, 6, 7, and 12–14). Misleading consent mechanisms – often implemented via dark patterns – are not compliant with the Regulation.

- Artificial Intelligence Act (AI Act): Articles 5(1)(a) and 5(1)(b) prohibit AI systems that use subliminal techniques or manipulative practices likely to cause physical or psychological harm, especially when exploiting vulnerabilities related to age, disability or social/economic status.

- Digital Markets Act (DMA) (Regulation (EU) 2022/1925): Article 13 includes anti-circumvention provisions to prevent gatekeepers from bypassing legal obligations, which may include deploying dark patterns to manipulate user behaviour.

- Data Act (Proposal for a Regulation on harmonised rules on fair access to and use of data, COM/2022/68 final): Recital 38 addresses the need to prevent dark patterns when designing user interfaces, particularly in the context of consent and data sharing by data holders and third parties.

- Consumer Rights Directive (CRD) (Directive 2011/83/EU), as amended by Directive (EU) 2019/2161: The recent amendments explicitly prohibit the use of dark patterns in financial services contracts, including at the point of contract conclusion (Article 16(e)).

These legislative tools, taken together, form a coherent and layered approach to addressing problematic design practices in the digital environment. The regulatory challenge lies not in the absence of applicable rules, but in fragmented implementation and enforcement across the EU.

Recommendations:

⇨ Prioritise coordinated enforcement: ensure that national authorities apply the UCPD and DSA consistently across Member States when addressing dark patterns.

⇨ Clarify legal interplay: issue consolidated guidance on how the UCPD, DSA, GDPR, DMA and other instruments interact in cases involving manipulative design, to provide legal certainty for businesses and regulators.

⇨ Promote practical cooperation: encourage dialogue between regulators, industry and civil society to develop illustrative use cases, compliance benchmarks and best practices

Overuse of digital products, services and content

Creating engaging digital products and services to win and maintain a customer base is the fundamental aim of any economic operator. This is legitimate and reflects the freedom to conduct a business as enshrined in EU law.

Many providers of online services have developed tools to help consumers manage their online engagement, including screen time reminders, parental controls and management of content. A wide range of tools are already available at the device and application level, including screen time reminders, notification controls, autoplay toggles and read receipts settings. Additionally, parental controls provide effective safeguards for managing their children's online activity, ensuring healthy digital engagement.

Ultimately, overspend of time or money are highly subjective and personal concepts, which consumers should be able to manage themselves. Prohibiting certain practices or design elements could reduce consumer control and choice. Therefore, it is important to provide a set of tools enabling users (or in the case of minors, responsible adults with minors) to make and adjust these personal (and often evolving) decisions about their usage across the different services and products they use.

The DSA already mandates a strong regulatory regime to address concerns related to 'addictive design'.

- The risk assessments required for very large online platforms explicitly cover these issues, ensuring that platforms consider potential risks, including for young people, and adapt accordingly.[4]
- The DSA also mandates that platforms offer alternative recommender systems that are not based on profiling, giving users of all ages greater control over their online experiences.[5] Specifically, very large online platforms are mandated to assess and mitigate risks associated with harmful addictive mechanics, including negative mental health impacts and detrimental user-generated content.
- The transparency requirements for algorithms and content recommendation systems in Article 27 provide a foundation for addressing addictive design concerns.
- Numerous companies have also developed voluntary tools, such as parental controls, screen time monitoring, and blocking features, to assist parents in managing their children's online experiences and preventing potentially addictive and harmful practices.

[4] Articles 28, 34 and 35.

[5] Article 38.

Dialogue between policymakers and industry under the DSA has already led to positive changes in platform design, demonstrating that the existing regulation is both effective and adaptable.[6] It is crucial that any regulatory gaps are addressed not by duplicating legislation, but taking a risk- and principle-based approach, focusing on parts of the industry that are not already regulated. Creating overly broad or strict and narrow rules would over-regulate services which do not present concerns regarding addiction. This would threaten the creation of innovative services and diminish the space for competition based on service differentiation, which is an especially competitive environment.

Recommendations:

- ⇨ Focus on clear and outcome-oriented principles rather than prescriptive prohibitions. Ensure flexibility for companies in implementing measures.
- ⇨ Work with a wide range of stakeholders, including providers of relevant online services, academics, teachers and parents. Overuse of digital products should be approached from a broad perspective, looking also at the relevant economic and societal factors.
- ⇨ Avoid blanket measures such as arbitrary limits to service usage. Such measures would not work for all types of users, as different people use online services for different purposes. Policymakers should instead consider existing industry-led best practices, which have often proven effective at tackling underlying factors.
- ⇨ Conduct further research to identify the specific design features or categories of online service of most concern to the wellbeing of European citizens, while keeping in mind the substantial benefits of online services for users.

Targeted advertising and online personalisation

Personalisation organises the massive amount of information online into manageable and useful content, products and services. Consumers expect personalised experiences, from product recommendations to relevant news articles to good retail offers, while data helps companies provide timely and helpful information that improves user satisfaction. On the other hand, advertisers (businesses, publishers, charities, political parties or public services) want their advertisements to be seen by consumers most likely to be interested in their offer. Advances in advertising technology have driven enormous improvements in ad relevance, reducing advertising wastage and improving consumer experience. These advances reduce advertisers' costs to achieve the same outcome.

There is an important role for data-driven advertising in the success and competitiveness of digital services – simply put, advertising is an essential part of doing business. Personalised ads are crucial to driving growth, especially for small and medium businesses (SMBs) and publishers. **86% of EU SMBs report increased overall revenue over the past year directly attributable to using personalised digital advertising**[7]. In addition, targeted advertising enables European SMBs to scale up and reach new audiences outside of their national territories. Data and personalisation enable businesses to make informed decisions and optimise their advertising strategies. This helps businesses ensure their ads are effective, relevant, and well-timed, leading to better results and more efficient use of ad budgets. Efforts to weaken EU businesses' ability to tailor their advertising to their audience is at odds with Europe's ambition to restore and improve its global competitiveness. Government regulations

[6] See https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161.

[7] Source

that limit the responsible use of data-driven advertising - and the ability of advertisers and businesses to learn from ad measurement - risk weakening economic competitiveness. The negative impacts linked to a reduction in the efficiency and effectiveness of advertising would not only be limited to commercial relationships, but would also negatively impact the free, organic and open nature of the internet. Specifically, services and products that are currently available free of charge may be forced to shift to subscription-based funding in order to test and scale.

Tailored advertising is also already sufficiently regulated under EU law, particularly concerning vulnerable audiences and data protection:

- **Digital Services Act (DSA) -** The DSA prohibits targeted advertisements to children (Article 28) and the use of sensitive data for advertising (Article 26). To further support implementation, the EU Commission is currently exploring a code of practice for online advertising. On personalised recommender systems, under the DSA, online platforms are already required to assess and adequately mitigate risks stemming from their recommender systems, including risks for the mental health of users and the dissemination of harmful content arising from the engagement-based design of these algorithms. Moreover, DSA Article 27 requires providers of online platforms that use recommender systems to explain, "in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters", in their terms and conditions.
- **General Data Protection Regulation (GDPR) -** GDPR provides strong safeguards for legitimate personalisation. Articles 5 and 6 define lawful data processing, Articles 12 and 13 set strong transparency rules, Article 21 grants consumers the right to object to direct marketing, and Article 22 protects against fully automated decision-making. These provisions ensure transparency and user control while allowing businesses to process data responsibly. The GDPR also includes rules on accountability, fairness, transparency, legal bases, and automated processing to ensure that personalization does not lead to negative outcomes from a fundamental rights perspective.
- **Digital Markets Act (DMA)** -The DMA requires consent before data can be combined or cross-used by traders designated as gatekeepers between Core-Platform Services. This provides another control for users in the way data can be used for advertising. Gatekeepers are also not allowed to process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper, unless consent is given.
- **Consumer Rights Directive (CRD)** – the CRD mandates transparency with regards to the personalisation of online experiences.
- **E-Privacy Directive & Member State rules -** Under the e-privacy directive and respective Member State guidelines, individuals are provided transparency and required to consent to the use of their online data collected through cookies and other tracking technologies.

Recommendations:

- Avoid implementing policy measures that would prohibit or severely limit online and personalised advertising .
- Known consumer issues related to digital advertising should be evaluated under the existing EU laws, if necessary, rather than via new digital fairness instrument.
- Policymakers should only introduce new legal requirements associated with digital fairness where there are proven deficiencies in existing laws. Further, before expanding the existing digital consumer law rulebook, the European Commission should issue additional guidance about

definitions such as a personalised offer and what are the actual benefits of these offers to consumers and European economy in general.

Commercial practices and influencer marketing

The UCPD, DSA and AVMSD clearly outline the obligations of content creators and 'influencers' engaging in commercial promotions, including transparency and accountability. The DSA and AVMSD provisions also outline strict advertising standards to which influencers must adhere,[8] and explicitly forbid hidden advertising, misleading claims and the purchase of 'likes' or 'followers'.[9] Additionally, targeting children with advertising or persuading parents to make purchases on their behalf is illegal.

A report by the EU Audiovisual observatory clarifies that vloggers/influencers' 'content can be qualified as audiovisual media services if they meet the legal requirements under the AVMS Directive'. Moreover, as clarified in the UCPD guidelines of 2021, professional influencers (who then qualify for the definition of traders) are required to individually label paid promotions in a clear and direct manner such that consumers must take no additional steps to find the applicable disclosures.[10] This guidance holds both influencers and brands accountable and provides specific instructions on preventing inappropriate advertising directed at children.

Consumers are increasingly aware of influencer marketing and understand that product and service endorsements are often part of commercial agreements. Given this awareness and the existing regulatory framework outlined above, it is unclear why new rules would be necessary. Efforts should focus on improving better education for influencers and brands to be aware of their obligations and implementing legislation consistently, alongside stricter enforcement of existing regulations.

Recommendations:

- ⇨ Ensure a proportionate liability regime for brands and agencies (i.e. brands and agencies should not be obliged to monitor compliance requirements of those influencers who are promoting their brands' products but do not have a direct or any type of bilateral contractual relationship with them).
- ⇨ Harmonise rules and levels of enforcement between Member States. Current national variance indicates that influencer marketing issues may lie more with enforcement and guidelines rather than intervening with a new law (such as the DFA).
- ⇨ Use any future rules to address influencers prompting counterfeit sales.

8 Art. 26(2) DSA requires online platforms to provide consumers with a functionality to declare whether the content they provide is or contains commercial communications. They must also ensure that other recipients of the service can identify in a clear and unambiguous manner and in real time, including through prominent markings, that the content is or contains commercial communications. Art. 28b(2), Directive (EU) 2018/1808 applies to video content and requires online service providers to inform users clearly when programmes or user-generated videos contain commercial communication, and to provide the means for the user who upload user-generated videos to declare the videos contain audiovisual commercial communications.

9 Purchasing of fake likes and followers is a prohibited practice in point 22 of the UCPD blacklist.

10 The 2021 UCPD guidance clarified that influencers must individually label paid promotions (no vague hashtags or extra steps to find disclosures), holding both influencers and brands accountable. It also gives guidance on unacceptable advertising toward children.

Digital contracts and subscriptions

In the growing digital economy, users have been able to acquire digital services by many different means, ranging from free (ad-based) to freemium to paid or subscription-based offers. Users have many options to choose from, and providers of digital products, content and services have the opportunity to make a value proposition to potential customers. This has brought enormous value to the EUS digital economy, ranging from video-platforms to application stores to social media.

Under existing rules, consumers can cancel subscriptions/contracts without unnecessary burdens or steps. Under the CRD, traders must provide a clear and easily accessible withdrawal mechanism, such as buttons, for distance contracts concluded online. Free trials are an important way for developers to test a digital service in the market and make a unique value proposition to users. Requiring payment details up front is an important security tool to avoid abuse of the digital service and verify the age of the customer. Users already receive clear information about entering a paid contract as well as reminder emails.

Policymakers should recognise the benefit to consumers of flexibility in the existing consumer protection framework and avoid legislation that imposes prescriptive product design, given that there are so many different types of online platforms and services, all with their own specificities. Provided that users can easily exercise their rights and consumer protections are in place, innovation in the consumer space should be allowed to flourish. Companies should be incentivised through light-touch regulation to create simple and user-friendly consumer journeys that make it attractive for consumers to use their service. This would not be possible if specific 'one-size fits all' solutions, like a one-click cancellation button or measures regarding the frequency of notifications were imposed. Prescriptive restrictions that do not have a clear evidence basis may have a chilling effect on innovation incentives in this space, as well as being unworkable for many digital platforms to implement. If any new rules were to be implemented, they would need to be proportionate and acknowledge the specificity of each sector. For example, for audiovisual content streaming, any new rules should consider the high upfront investments in content production and acquisitions, and the specificities of the distribution model, which usually includes unlimited access to the service with the ability to consume large amounts of content in short periods.

Pricing

Information to consumers about price reductions is regulated by the Price Indication Directive, recently reviewed by the Modernisation Directive. Ensuring consumers are not misled by fictive price reductions was the key goal of the amendment, introducing an obligation to show the lowest 30-day price in the case of strike-through prices. As this obligation was added by way of an EU Parliament amendment, no impact assessment was ever conducted about this regulatory requirement.

A stable legal framework, legal certainty and a high level of harmonisation is needed around pricing rules and their enforcement, because many consumers shop cross-borders and can easily compare prices between retailers, online or offline. A targeted amendment of the Price Indication Directive would be a more timely and effective approach to ensuring consumers have adequate information about pricing.

Definitions of average/vulnerable consumer, and reversal of the burden of proof

As discussions evolve around updating consumer protection in digital contexts, some proposals have suggested shifting the burden of proof onto traders in cases involving complex technologies like AI-driven personalisation. While intended to enhance accountability, such a shift would likely result in significant administrative burdens and legal uncertainty.

The concept of the 'average consumer who is reasonably well informed and reasonably observant and circumspect', also taking into account social, cultural and linguistic factors, as consistently interpreted by the European Court of Justice for over two decades, has proven to be an effective, flexible and technology-neutral benchmark to achieve a high level of consumer protection while striking a balance with the promotion of free trade and the competitiveness of businesses in the Union.

Moreover, there is an additional benchmark of the 'average member of the group' that can be referred to when a trader foreseeably reaches a specific group of consumers and therefore can be expected to consider the specific characteristics thereof. This provides further safeguards when a commercial practice is directed at a group of consumers who, because of their common characteristics, do not fit in the 'average consumer' standard.

Additionally, the existing concept of 'vulnerable consumers', due to their mental or physical infirmity, age or credulity, introduces an even higher standard of protection, based on individual circumstances that are objectively verifiable and foreseeable. This standard is also reasonable for traders, who can adapt their commercial practices to ensure that vulnerabilities that are common to a group of consumers are considered.

Therefore, the continued use of concepts such as the 'average consumer', the 'average member of the group' or the 'vulnerable consumer' makes it possible to consider, in a flexible manner, common and foreseeable characteristics and vulnerabilities of consumers, without affecting legal certainty.

Amending or complementing these concepts with additional benchmarks or factors risks undermining legal certainty to the detriment of traders, who are unable, when offering their products or services to the general public, to consider the individual characteristics and personal circumstances that drive each consumer's transactional decision. Moreover, this could ultimately hamper the high level of consumer protection achieved through the use of the current concepts, since the personal characteristics of every consumer differ and vary over time and cannot be considered all at once. Such new benchmarks or factors would also require the additional collection of personal data by traders, with resulting risks to privacy as well as - in some cases - conflict with the GDPR and DSA rules preventing online platforms from collecting additional personal data on e.g. minors.

The objective to achieve a higher level of protection of consumers by considering their individual characteristics and personal circumstances can rather be achieved through other means, for example consumer information and education campaigns.

Overall, the Digital Fitness Check report recommends updating these definitions to more accurately reflect online consumer behaviour. It also suggests alleviating the burden of proof in certain cases, such as those involving complex AI-driven personalisation. This would require traders to demonstrate that their practices do not harm consumers, recognising the challenges faced by consumers in understanding algorithms and personalisation techniques.

- ⇨ Defend the existing definitions of 'average' and 'vulnerable' consumers. Widening the list of vulnerabilities to include situational vulnerabilities, such as moods, emotions, and various personal hardships, would render the well-understood concept of an 'average consumer' obsolete. It would also be disproportionate and only serve to create further legal uncertainties. This is because at any given moment an individual could be vulnerable. A clear distinction between an average and vulnerable consumer ensures a balanced approach that protects the most at risk while ensuring legal clarity. Reiterate the importance of the UCPD guidance in providing clarity in consumer vulnerabilities and support its full implementation.
- ⇨ Reversal Burden of proof: in the age of simplification, the reversal of burden of proof on digital activities would likely result in high administrative task volume and legal uncertainty. In the absence of concrete guidance and standards on how to carry this exercise out, there is a potentially counterproductive effect: to identify a vulnerable consumer means a lot more data would have to be collected to carry out verifications.

Conclusion

The EU's ambition to ensure fairness in the digital environment is best through effective enforcement of the robust digital consumer laws already in place. From dark patterns and addictive design to targeted advertising and influencer marketing, existing laws, such as the UCPD, DSA, GDPR, and others, provide comprehensive protections for consumers while supporting innovation and competitiveness. Rather than layering new digital fairness obligations that risk legal uncertainty and regulatory fragmentation, policymakers should prioritise simplification, coherence, and evidence-based approaches. This includes enhancing guidance, fostering public-private cooperation, and focusing enforcement where it is most needed.

A proposal for a future Digital Fairness Act should be seen as an opportunity to streamline, not complicate, the EU's digital rulebook - ensuring consumer protection, regulatory clarity, and sustained economic growth across Europe.