CCIA Europe Response to the European Commission's Public Consultation on the Digital Fairness Act

Navigating the Digital Fairness Act

October 2025

The Computer & Communications Industry Association (CCIA Europe) welcomes the opportunity to contribute to the Digital Fairness Act's (DFA) development. The Association believes that a coherent legislative framework, combined with effective enforcement, is essential to empower consumers and ensure they fully benefit from the Single Market.

At the same time, it is important to recognise the EU already has a robust legal framework for consumer protection. Therefore, CCIA Europe considers that the DFA should prioritise strengthening enforcement, harmonising existing initiatives, and aligning today's framework with the broader simplification agenda – rather than adding new layers of rules.

As the European Commission explores various options for the announced DFA initiative, CCIA Europe respectfully offers the following feedback.

I. Strengthening the EU's enforcement capabilities

Consistent application and coordinated enforcement of existing rules will strengthen consumer protection across the EU, while providing legal clarity for business and consumers.

Recommendations:

1. Improve regulatory coordination
2. Enhance consumer literacy

II. Adopting a proportionate and evidence-based approach

Any new measures proposed should be clearly justified with concrete, measurable evidence of a problem and its impact. The DFA should be principle-based and adaptable to different online services – ensuring proportionality, flexibility, and future-proof application.

Recommendations:

3. Respect technological and channel neutrality
4. Recognise improvements in transparency and responsibility

III. Prioritising simplification and harmonisation

Simplifying the EU regulatory framework to boost Europe's competitiveness should guide any new initiatives under the DFA. The evaluation of consumer law, starting with digital fairness, is a chance to clarify existing rules rather than adding new, duplicate provisions.

Recommendations:

5. Focus on consistent enforcement to fight dark patterns
6. Avoid duplication in addressing addictive design
7. Recognise personalisation's value to consumers
8. Prioritise horizontal measures across the Single Market

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes this opportunity to provide feedback to the European Commission's public consultation on the Digital Fairness Act (DFA). The Association believes that the current EU legal framework for consumer law is already comprehensive and provides a strong level of protection to European consumers, both in the online and offline world.

We support the Commission's goal of achieving a harmonised legislative framework for consumers at the EU level, as long as it avoids creating new barriers or legal uncertainty for businesses operating across borders.

As the EU's digital rulebook continues to expand – with landmark legislation like the Digital Services Act (DSA), Digital Markets Act (DMA), AI Act, and General Data Protection Regulation (GDPR) already in place – CCIA Europe considers it essential for any new initiative under consideration to build on this strong existing framework.

That is also why the announced DFA should avoid adding new layers of complexity or duplication that could further undermine legal certainty and stifle innovation.

To build on the Commission's preparatory work for the Digital Fairness Act, CCIA Europe respectfully offers the following feedback, structured around three core principles:

I. Strengthening the EU's enforcement capabilities
   1. Improve regulatory coordination
   2. Enhance consumer literacy

II. Adopting a proportionate and evidence-based approach
   3. Respect technological and channel neutrality
   4. Recognise improvements in transparency and responsibility

III. Prioritising simplification and harmonisation
   5. Focus on consistent enforcement to fight dark patterns
   6. Avoid duplication in addressing addictive design
   7. Recognise personalisation's value to consumers
   8. Prioritise horizontal measures across the Single Market
      - Average and vulnerable consumers
      - Burden of proof
      - Fairness by design

I. Strengthening the EU's enforcement capabilities

Consistent application and coordinated enforcement of existing rules will strengthen consumer protection across the EU, while providing legal clarity for business and consumers.

Insufficient and fragmented enforcement, combined with a lack of legal certainty, currently undermines the effectiveness of consumer protection rules throughout the EU. Instead of adding new layers of complexity, CCIA Europe believes the focus of the announced DFA should be on empowering regulators and businesses to ensure that existing rules are enforced consistently.

This approach is also better suited to quickly address concerns about actors who consistently and actively fail to comply, while serving as a deterrent across the market. Two main aspects should be considered to achieve better enforcement.

1. Improve regulatory coordination

A significant challenge in current application of EU consumer rules is related to the proliferation of different enforcement authorities with varying degrees of expertise and significant differences when it comes to the mechanisms and tools at their disposal.

To avoid overlaps and uncertainty, we firstly need a clearer and more centralised approach to enforcement. The European Commission should be ambitious in strengthening the Consumer Protection Cooperation (CPC) network and cooperation within it.[1] Following the 2022 public consultation on strengthened enforcement cooperation,[2] and given the CPC network's proven ability to quickly and effectively address cross-border infringements, the Commission should start promoting enhanced enforcement action, particularly against non-compliant actors.

CCIA Europe also supports the idea of enhancing inter-authority coordination and establishing clear protocols for joint investigations. There is no need to develop further legislative tools; action can be taken now to reinforce the CPC networks' capabilities.

Secondly, unified training for enforcement authorities would be helpful to increase awareness of the latest developments in the digital space and ensure authorities are up to date with the most recent technologies for enforcement and prosecution of crimes. To make this happen, regular exchange of best practices among regulators should be fostered, guaranteeing a coordinated approach.

Offering compliance training for businesses – directly offered and administered by the same authorities – could be helpful to enhance compliance, rather than opting for formal

[1] Through the updated Consumer Protection Cooperation Regulation (EU) 2017/2394, national authorities are empowered to detect irregularities and take speedy action against rogue traders. Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws, available here: https://eur-lex.europa.eu/eli/reg/2017/2394/oj

[2] European Commission's public consultation on consumer protection - strengthened enforcement cooperation, open from 28 September 2022 to 21 December 2022, available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13535-Consumer-protection-strengthened-enforcement-cooperation_en

enforcement actions. An example of this approach is the network of regulators that was established by the French SREN bill, promulgated in May 2024.[3] This framework formalises cooperation between all key national bodies (Digital Services Coordinators, data protection authorities, consumer protection bodies) to allow sharing of expertise and to ensure a consistent enforcement of digital laws.

2. Enhance consumer literacy

CCIA Europe has consistently advocated for empowering consumers through education and digital literacy campaigns. We consider this to be key to driving economic growth, innovation, and sustainability across the European Union in the future. Such an approach requires whole-of-society efforts that include increasing investment in education and media literacy, and providing European consumers with the right tools to navigate a constantly evolving digital environment.

Therefore, education and digital literacy campaigns should be fostered by the European Commission and Member States alike. These initiatives should be tailored to different skill levels and demographic groups to ensure all types of consumers across the EU are adequately covered. Particular attention should also be paid to vulnerable consumers, such as older people and young users of online services, who may have more specific needs in terms of literacy.

As part of these literacy campaigns, establishing structured feedback loops with providers of online services would also help EU policymakers better understand emerging trends and risks. Indeed, many providers already invest in literacy campaigns to empower consumers and increase their knowledge about the tools at their disposal when problems arise online.

II. Adopting a proportionate and evidence-based approach

Any new measures proposed should be clearly justified with concrete, measurable evidence of a problem and its impact. The DFA should be principle-based and adaptable to different online services – ensuring proportionality, flexibility, and future-proof application.

CCIA Europe firmly believes that any new legislation in the field of consumer protection and 'digital fairness' needs to be based on concrete, measurable evidence and that any measures considered need to be proportionate to the identified problems. The online ecosystem is incredibly diverse, and counts a wide range of different players and business models. Therefore, any proposal must be justified by substantiated evidence of consumer detriment not being adequately addressed through existing legislation – it also has to be workable in practice and adaptable to the different business use cases, instead of just adding new layers of complexity.

To date, the European Union has around 100 tech-focused EU laws, and over 270 regulators active in digital networks across all Member States.[4] We believe a proportionate

[3] French law number 2024-449 aimed at securing and regulating the digital space, from 21 May 2024, available here.

[4] The Draghi report on EU Competitiveness - 'The Future of European Competitiveness. Part A: A competitiveness strategy for Europe', September 2024, available here.

approach is thus necessary going forward, particularly given the comprehensive legal framework that already exists to protect consumers. To name a few, the following current rules already contribute to ensuring strong consumer protection:

- The Omnibus Directive of 2019 served to update key consumer protection laws already in existence (the Unfair Commercial Practices Directive, Consumer Rights Directive, and Unfair Commercial Terms Directive), in order to align them with digital developments and enhance enforcement tools.[5] Among others, the Directive introduced transparency requirements applying to online search ranking parameters, price reduction, and consumer reviews. In 2024, the European Commission issued an implementation report indicating that in those Member States where the rules have been transposed, the situation has improved.[6]

- The General Data Protection Regulation (GDPR) of 2016 provides a comprehensive legal framework to ensure the protection of personal data.[7] The Regulation requires lawful consent, as well as transparency for data processing purposes, and introduces strict obligations on businesses regarding data collection, processing, and storage. It also introduces limitations as to what is allowed, and what is not, when it comes to consent mechanisms – de facto prohibiting deceptive design patterns.

- The Digital Services Act (DSA) of 2022 is a landmark legislation that increases online platforms' transparency and accountability for the content hosted by them, protecting users' fundamental rights.[8] The DSA also explicitly prohibits online platforms from using deceptive or manipulative patterns, and it requires increased transparency about online advertising and recommender systems.

The above is far from a comprehensive overview, as a myriad of other digital legislative tools have an impact on and increase consumer protection.

However, the GDPR and the DSA in particular have created a culture of responsibility among businesses and users which is still evolving today. At the same time, they have empowered users by reinforcing their rights and providing them with new tools to fight against potential abuses. This culture of responsibility and empowerment is still in development, as the effects of these laws are being felt progressively by both users and businesses. Therefore, proposing new rules, when we still don't have a full understanding of the overall impact and change that these legal frameworks are bringing about (both for businesses of all sizes and characteristics, and for users), would be premature.

---

[5] 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 (Omnibus Directive), available here.
[6] Report from the Commission on the implementation of 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, available here.
[7] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), available here.
[8] Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC(Digital Services Act), available here.

When it comes to considering new instruments, CCIA Europe believes it is necessary to first carry out a comprehensive assessment of the existing regime. Further research on the economic and social impact that existing legislation has on consumers and businesses would be strongly advisable. Once measurable problems are identified and evidence is gathered about the need for new instruments, the main principles to follow when developing any measures are listed below (recommendations 3 and 4).

3. Respect technological and channel neutrality

CCIA Europe believes that any new instruments considered should avoid prescribing a one-size-fits all approach or specific technological solutions. As demonstrated by the GDPR and the DSA, legislation based on principles makes a difference. And for that, it is necessary to set clear objectives, allowing businesses to find the best ways to achieve them.

In this regard, respect for technological and channel neutrality is a must if we want to guarantee a proportionate, future-proof and evidence-based approach. For example, instead of mandating a physical 'cancellation button,' any instruments considered under the announced DFA should focus on ensuring that the process of unsubscribing is as easy as subscribing.

Similarly, prescriptive requirements for customer support channels, such as mandating a phone number, may ignore more effective, digital solutions such as in-app help functions that provide 24/7 support and traceable communication. Further, design requirements for online sellers should also remain channel neutral: physical first-party retail stores aren't required to disclose their shelf placement or the logic behind their store layout to customers, and this principle should remain the same online. Considering prescriptive requirements that are tied to current technology also risks stifling innovation and quickly becoming obsolete.

4. Recognise improvements in transparency and responsibility

In recent years, many online services have increased transparency when it comes to topics such as personalised commercial practices, influencer marketing, online subscriptions, pricing practices, and digital contracts. It is clear that the market is responding to consumers' demands, as part of a wider culture of responsibility that has been developing in Europe.

For example, when it comes to influencers, many online businesses already have systems in place for creators to indicate when certain content is sponsored. Self-regulation also plays a crucial role in maintaining high standards of transparency and responsibility within the digital market ecosystem.

Programmes and tools developed by industry are essential for equipping content creators with the necessary knowledge and resources to guarantee responsible advertising and marketing practices. The European Commission should therefore focus further efforts on empowering consumers, educating content creators about how to use digital services in a

safe and self-determined way, as well as holding creators and advertisers accountable – rather than shifting the responsibility to intermediaries.[9]

A recent survey of 10,500 Europeans revealed that consumers have observed positive patterns over the past year, such as improvements in transparency and fairness. Examples of these positive patterns include easy-to-access unsubscribe buttons and explanations for why email addresses are required (both observed by around 40% of consumers), fraud warnings, or clearly labelled social media advertising and influencer partnerships.

European consumers are also quick to take action against practices deemed as negative: around 90% of consumers reported having unsubscribed from unwanted email lists in the past year, 77% had disabled cookies to limit data tracking, 76% unsubscribed from paid services they found deceptive, and 65% had left a negative review.[10]

Overall, consumers seem to consider personalisation of online services useful, and reward brands that combine personalised experiences with transparency and fairness. They are also digitally savvy and willing to take action against companies that fail to act responsibly. If additional measures in this area were to be considered, a risk-based approach should be prioritised, focusing on increased transparency and user choice, instead of introducing measures that would limit user experience.

III. Prioritising simplification and harmonisation

Simplifying the EU regulatory framework to boost Europe's competitiveness should guide any new initiatives under the DFA. The evaluation of consumer law, starting with digital fairness, is a chance to clarify existing rules rather than adding new, duplicate provisions.

The rapid increase in EU tech legislation has resulted in a regulatory environment that is challenging to navigate and produces significant overlaps and inconsistencies across key legal instruments.[11] These instruments include the General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA),[12] Unfair Commercial Practices Directive (UCPD),[13] Unfair Terms Directive,[14] Consumer Rights Directive (CRD),[15] and Artificial Intelligence Act (AI Act).[16]

[9] The European Commission has, for example, developed an Influencer Legal Hub, which includes helpful resources for influencers in Europe, and has been developed in collaboration with academic exports and the European Union Intellectual Property Office.
[10] Findings from a consumer survey by Nextrade Group, commissioned by CCIA Europe. Results can be found here and easily filtered through the interactive dashboard.
[11] As highlighted already in CCIA Europe response to the European Commission's public consultation on the upcoming digital omnibus simplification package. This response refers to numerous instances of overlaps within already existing EU digital rules and is available here.
[12] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), available here.
[13] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive'), available here.
[14] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, available here.
[15] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights (Consumer Rights Directive), available here.
[16] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), available here.

In fact, many of the concerns identified in the 2024 fitness check (e.g. dark patterns, misleading practices by influencers, or addictive design)[17] are already addressed by existing – and in many cases, recent – legislative instruments such as the aforementioned DSA, GDPR, and UCPD – as well as in guidance from both the Commission and the European Data Protection Board (EDPB).[18] By way of example, what follows is a non-exhaustive overview of legislation that already regulates some of these practices.

5. Focus on consistent enforcement to fight dark patterns

A number of EU laws address dark patterns today. The DSA states that "providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."[19] This prohibition extends to practices such as providing "more prominence to certain choices, repeatedly requesting decisions if a user has already made one, or making service termination more difficult than subscription."

The UCPD specifies that a commercial practice shall be deemed misleading if its "overall presentation" deceives, or is likely to deceive, the average consumer. This stands, even if the underlying information is factually correct, provided the practice causes or could cause the consumer to make a transactional decision they otherwise would not have.[20]

The AI Act prohibits AI systems that deploy "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm."[21o]

Furthermore, the EDPB Guidelines on Deceptive Design Patterns provide comprehensive guidance on recognising and avoiding 'deceptive design patterns' in social media platform interfaces that infringe on GDPR requirements.[22] These patterns aim to influence users into making unintended, unwilling, and potentially harmful decisions regarding their personal data, often in the platform's interest. The EDPB draft Guidelines on the interplay between the DSA and the GDPR also refer to the effective bases already established by the existing legal framework.[23]

---

[17] Commission Staff Working Document Fitness Check on EU consumer law on digital fairness, available here.
[18] 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, available here; Guidelines 3/2022, on Dark patterns in social media platform interfaces: How to recognise and avoid them, 02 May 2022, available here.
[19] Article 25(1) DSA
[20] Article 6(1) of the UCPD: Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive), available here.
[21] Article 5(1)(a) AI Act
[22] EDPB Guidelines 03/2022 on Deceptive Design Patterns in social media platform interfaces: how to recognize and avoid them, available here.
[23] EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR, available here.

We also note that the provisions on dark patterns under the DSA are still under implementation by online platforms, and the European Commission has so far not issued any guidance on this matter. If the Commission determines that no further guidelines are necessary to clarify the application of Article 25 DSA, this strongly suggests that the legal text is sufficiently clear and robust to address problematic dark patterns.

Therefore, proposing new legislative action on dark patterns through the announced Digital Fairness Act would be both premature and duplicative, undermining the existing, strong regulatory framework and causing legal uncertainty for businesses.

CCIA Europe considers that the primary focus of any upcoming initiative should be on consistent enforcement of the above framework. Additional guidance in order to ensure consistent interpretation of this framework would also be welcome, in particular to clarify the boundaries between dark patterns and permissible design practices. The Commission should also focus on specific actions to encourage consumer awareness and literacy efforts to address and reduce dark patterns.

6. Avoid duplication in addressing addictive design

When it comes to addictive design, the DSA mandates providers of very large online platforms and very large online search engines to "assess systemic risks", which include the "serious negative consequences to a person's physical and mental well-being."[24] This also covers risks stemming "from online interface design that may stimulate behavioural addictions of recipients of the service." The Act stipulates that targeted providers must take appropriate mitigating measures such as adapting the design of their service and online interface. They are also required to address gender-based violence and the protection of minors. Specifically on the latter, measures on how to ensure a high level of privacy, safety, and security of minors are further developed in the recently adopted guidelines on Article 28 of the DSA, published only three days before the public consultation on the Digital Fairness Act was launched.[25]

Similarly, the General Product Safety Regulation (GPSR) states that when assessing a product's safety, the health risk posed by digitally connected products should be considered – including the risks to mental health, especially of vulnerable consumers such as children. Manufacturers of digitally connected products likely to impact children already must ensure their products meet the highest standards of privacy and "safety by design", a core requirement across the GPSR.[26]

The AI Act also prohibits the use of any AI system that exploits the vulnerabilities of a person because of their age, disability, or specific social or economic situation, in a way that is likely to cause them significant harm.[27]

CCIA Europe believes that further research is necessary to identify specific design features that cause most concern. We welcome the European Commission's initiative to conduct an EU-wide inquiry into digital wellbeing and would encourage the Commission to include a wide variety of stakeholders in the discussions – including providers of relevant online

[24] Article 34(1)(d) DSA
[25] Commission publishes guidelines on the protection of minors, 14 July 2025, available here.
[26] Article 5(2)(f) of Regulation (EU) 2023/988 on general product safety (GPSR), available here.
[27] Article 5(1)(b) AI Act

services, researchers, academics, teachers, and educators. This inquiry should be broad, and also look into all the relevant economic and societal factors impacting the well-being of users of online services.

Hence, the announced DFA should avoid duplication and build upon industry's best practices, taking a flexible risk-based approach that focuses on empowering the individual user with more options, instead of introducing broad restrictions for everyone. Blanket measures such as arbitrary limits on the use of online services should be avoided, as they may not be suitable for all users and could lead to a diminished online experience for everyone.

7. Recognise personalisation's value to consumers

Personalisation is a feature valued widely by European consumers[10] that helps users effectively navigate vast quantities of information online. It also serves as an essential tool for online services to create safer and more predictable digital environments, particularly for younger users.

Personalised advertising, for instance, plays a critical role in ensuring that consumers are shown relevant content, while enabling businesses to optimise contained marketing budgets.[28] From a regulatory perspective, personalisation is already heavily governed by a multi-layered safety net, which includes the GDPR, DSA, DMA and AI Act. For instance, the DSA bans targeted advertising based on sensitive data and prohibits all targeted advertising directed at minors.

The principle of transparency in the GDPR requires information to be "concise, easily accessible, and understandable", and for the controller to take appropriate measures to provide any information relating to processing to the data subject "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[29] The GDPR also defines profiling and mandates controllers to provide data subjects with information about "the existence of automated decision-making, including profiling, and meaningful information about the logic involved, its significance, and envisaged consequences."[30]

The Consumer Rights Directive and the UCPD also set out a number of requirements for algorithm and ranking transparency in a product's interface.

More concretely, the DSA imposes significant transparency obligations on online platforms. For example, they are required to provide "meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters".[31] Online platforms are also required to clearly set out in their terms and conditions the main parameters of their recommender systems, and explain any options to modify or influence these parameters.[32] Moreover, very large platforms and

[28] The Impact of Digital Advertising on Europe's Competitiveness: A Study on the Role of Digital Advertising in Europe', report by the Centre for Information Policy Leadership (COPL) and Public First, available here.
[29] Article 12 GDPR
[30] Article 13 GDPR
[31] Article 26 DSA
[32] Article 27 DSA

search engines must also offer "at least one option for each of their recommender systems which is not based on profiling."

Further, under the DMA, gatekeepers must secure standardised consent following the tenets of the GDPR to process personal data for online advertising, particularly when this data is sourced from users of third-party services.

The AI Act emphasises transparency as a key ethical principle to ensure trustworthy AI, by stating that "high-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately."[33]

Finally, the Data Act also states that information on data holder's use of data for purposes like improving product function or developing new services must be transparent to the user, with any changes requiring informed agreement.[34]

8. Prioritise horizontal measures across the Single Market

Beyond specific practices like dark patterns, addictive design and personalisation, the discussions around digital fairness often suggest addressing broader horizontal concepts intended to address perceived asymmetry between consumers and online services.

Nevertheless, introducing new and vague obligations – such as broadening the definition of vulnerable consumer, considering a general reversal of the burden of proof, or mandating abstract 'fairness by design' mandates – risks creating significant legal uncertainty and regulatory fragmentation.

To genuinely address digital asymmetry without sacrificing legal clarity, the focus should remain on harmonising and strengthening enforcement across the Single Market of the existing rules that are already established in the EU digital rulebook in a principle-based and actionable way.

Below follows a more detailed overview regarding some of the actions considered by the European Commission in the context of the consultation on the Digital Fairness Act.

Average and vulnerable consumers

CCIA Europe believes that the current principle-based definitions of 'average' and 'vulnerable' consumers, derived from existing EU legislative frameworks and case law, already provide the necessary legal certainty and proportionality.[35] These concepts are crucial to enable enforcement authorities and courts to account for common and foreseeable vulnerabilities, without imposing unworkable obligations on online products and services, such as requiring them to anticipate every individual's unique or momentary circumstances.

---

[33] Article 13(1) AI Act
[34] Recital (25) Data Ac.
[35] The concept of "average consumer" in EU law is defined under the Directive 2005/29/EC, on Unfair Commercial Practice and repeatedly reaffirmed in EU case law, such as in Case C-646/22 Compass Banca, available here and other cases including Lloyd, Darbo and Douwe Egbers, available here, here and here.

The suggestions under consideration for the announced Digital Fairness Act should not create additional uncertainty. More concretely, suggestions to broaden the definition of 'vulnerable' to include subjective or situational factors – such as emotional distress or negative mental states – would undermine the foundational concept of the 'average' consumer and greatly reduce predictability for businesses operating across the Single Market.

Basing restrictions on such unclear terms does indeed entail considerable risks. Contrary to the goal of data minimisation under the GDPR, online services would likely be forced to process significantly more data, including potentially sensitive data points, simply to identify vulnerable consumers in a dynamic manner. Any such expansion would conflict with the data and user protection principles enshrined in both the GDPR and DSA.

Burden of proof

CCIA Europe strongly believes that the current burden of proof rules must be upheld. Proposing a general reversal of the burden of proof for digital services would be a disproportionate step. One that risks imposing significant administrative burdens on businesses of different sizes and inadvertently stifling innovation. Such a shift is also legally challenging and would undermine the good faith principle that currently governs trade in digital products and services.

Before considering such a step, concrete and measurable evidence would be required to show that consumers and enforcement authorities are genuinely struggling to produce evidence under existing rules. To date, we have seen no such evidence.

Instead, the focus in this case should be on enhancing enforcement through existing mechanisms. For instance, providing regulators with AI-powered tools for the proactive detection of systematic abuses is a smarter, more actionable approach than unilaterally shifting the burden onto all businesses.

Fairness by design

When it comes to fairness, Europe must prioritise actionable and clear rules over abstract mandates. The concept of 'fairness' is inherently ambiguous and difficult to define in precise legal terms, making it unsuitable for new horizontal obligations. Introducing such a vague duty would create significant unpredictability and risk stifling innovation for businesses across the EU. The core tenets of 'fairness' are already embedded and sufficiently addressed in the EU's digital rulebook through: prohibitions on misleading and aggressive practices in the UCPD, requirements for transparency on commercial practices and algorithms (included in the DSA, UCPD and CRD), and principles for lawful and fair data protection (introduced through the GDPR and DSA).

These bases already provide a legal framework that is sufficient to address problematic practices without incurring in legal uncertainty and fragmentation, which a vague definition of the concept 'fairness' would introduce. For CCIA Europe, the announced DFA should avoid duplication and adding new layers to an already complex legislative ecosystem to prevent legal uncertainty and increased compliance burdens for businesses of all sizes. The focus should be targeted at addressing measurable gaps in the current framework.

On the other hand, the lack of harmonisation in consumer law, which is often implemented through Directives, is certainly a problem as it leads to legal uncertainty and market fragmentation. CCIA Europe considers the ongoing digital fairness efforts, and the closer look at consumer law, as an opportunity to consider ways to strengthen a harmonised and unified EU approach. This would reduce compliance burdens for businesses operating across the Single Market and help provide a far more seamless experience for consumers.

As shown above, many of the concerns identified for the DFA are already extensively regulated by the EU. Therefore, the Commission's focus should be to simplify and harmonise the existing framework as part of the ongoing simplification efforts, and not to create new, duplicative rules.

Conclusion

Navigating the digital world requires that consumers are empowered, businesses are responsible, and rules can foster technological innovation.

For that to happen, any new initiatives under the umbrella of the Digital Fairness Act must be evidence-based and proportionate. Research shows that consumers value the benefits of the online space and personalisation of the services they use. If the Commission considers the introduction of blanket prohibitions or mandating overly prescriptive measures, this would inadvertently harm consumers and stifle the growth of businesses that depend on these digital tools to compete.

A deep dive into the EU's digital rulebook shows that many of the practices identified in the fitness check are already extensively covered by the current framework. Instead of creating new rules that cause legal fragmentation and uncertainty, the focus should be on clarifying and enforcing what Europe already has. Likewise, we must further strengthen the EU's enforcement capabilities.

Studies show that consumers are responsive and actively push back against deceptive services, incentivising the market to strive for fairness and responsibility.[36] The most effective way forward is for the European Commission to focus on enhancing compliance, and targeting systematic and large-scale abuses on a case-by- case basis in a coordinated way.

This will have a proper deterrent effect that will permeate through the entire Single Market, contrary to new rules that would impose burdensome and potentially duplicative obligations. Indeed, Europe must continue to foster a collaborative environment where industry, regulators, policymakers, and civil society work together to ensure a digital world that is both fair and innovative.

[36] Findings from a recent survey with 10,400 European consumers in 12 countries conducted by Nextrade in July 2025 show that European consumers act against dark patterns and punish misbehaving services by refusing to continue buying from deceptive brands. More details can be found in the survey paper, published in October 2025 and available here.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org