European Democracy Shield

Feedback to the call for evidence on the European Democracy Shield

May 2025

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the opportunity to contribute to the European Commission's call for evidence on the European Democracy Shield proposal. Building on the European Democracy Action Plan (EDAP) and the Defence of Democracy Package is crucial to guarantee that the biggest risks to democracy are tackled and election integrity is guaranteed.

The Commission's upcoming Communication is timely, in particular amidst rising concerns over hybrid threats, foreign interference, and information manipulation. CCIA Europe welcomes the Democracy Shield's emphasis on a whole-of-society approach built on four pillars, in particular the recognition that safeguarding elections requires ecosystem-wide collaboration.

CCIA Europe and its Members have long supported efforts to safeguard electoral integrity and promote transparency in the digital space. Indeed, the Association has actively engaged in the development and implementation of key legislation, such as the Digital Services Act (DSA) and the Regulation on transparency and targeting of political advertising, as well as supporting non-legislative initiatives such as the EU Code of Practice on Disinformation.

We believe that the Democracy Shield should build on this existing framework and help reinforce trust in democratic institutions, without undermining fundamental rights or reducing legal certainty for digital services providers.

On the following pages, you will find CCIA Europe's contribution to the call for evidence, highlighting four core elements:

I. Reinforce the regulatory architecture and avoid duplications
II. Safeguard freedom of expression and information
III. Strive towards a proportionate, risk-based, and future-proof approach
IV. Target responsibilities and guarantee transparency in electoral processes

I. Reinforce the regulatory architecture and avoid duplications

The European Commission has rightly identified the need to better protect the European Union against foreign information manipulation and interference – including by fighting against disinformation and threats to the integrity of elections and democratic processes, a goal that is widely shared by CCIA Europe and its Members. In this context, the EU already possesses a powerful framework to help tackle this challenge, and this framework should remain the legal basis for addressing any threats to democracy. It includes:

- The Digital Services Act (DSA)[1], which imposes due diligence and transparency obligations on providers of intermediary services as well as comprehensive, horizontal risk assessment and mitigation measures for very large online platforms (VLOPs) and very large search engines (VLOSEs) in the context of election integrity and disinformation and beyond.
    - The Commission's guidelines under the DSA[2] for the mitigation of systemic risks online for elections, with specific guidance addressed at VLOPs and VLOSEs for the European Parliament elections in June 2024.
- The Regulation on transparency and targeting of political advertising[3], which provides a targeted framework to guarantee transparency in political advertising across the EU, helping citizens make informed decisions during electoral periods.
- The European Media Freedom Act (EMFA)[4], aimed at safeguarding media freedom, media pluralism, and editorial independence in the EU.
- The Code of Conduct on Disinformation[5], a novel and innovative framework to address the spread of disinformation. This Code – agreed upon by a broad cross-section of stakeholders, including but not limited to online platforms, search engines, fact-checking and civil society organisations – was first established in 2018 and further strengthened in 2022. Recently, it has been recognised as a Code of Conduct under the DSA.

In light of the above, CCIA Europe considers it essential to avoid overlapping or inconsistent requirements and duplication of existing measures, fostering the consistent application of the risk-based approach already enshrined in Article 35(1) of the DSA. Departing from this

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available here: https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[2] European Commission Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes, available here: https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes
[3] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202400900
[4] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), available here: https://eur-lex.europa.eu/eli/reg/2024/1083/oj
[5] 2022 Code of Practice on Disinformation, which was integrated into the framework of the DSA as a Code of Conduct on Disinformation on 13 February 2025: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

would only create regulatory fragmentation, particularly problematic given the inherently cross-border nature of digital services and foreign attempts at information manipulation and interference. Any additional measures considered under the European Democracy Shield should be carefully scoped to complement the DSA and the Code of Practice on Disinformation, rather than creating inconsistent rules.

Whereas online platforms have robust processes in place to prevent and respond to risks related to elections; cooperation, empowerment, and capacity building among all relevant stakeholders will be essential to meet the European Democracy Shield's overall goals.

Further, the evolving threat of hybrid interference, including through deceptive content generated by malicious actors using artificial intelligence (AI) tools, should be addressed with guidance that is flexible and adaptable to the nature of the different online services, in order to remain responsive to future risks.

A coherent legal framework is essential to guarantee adequate compliance and enforcement, especially for emerging online platforms and small and medium enterprises (SMEs), which often lack the resources to navigate a patchwork of rules.

II. Safeguard freedom of expression and information

As the Commission notes, information manipulation is a powerful tool for those who aim to erode the foundations of democracy. However, when countering these threats, respect for freedom of expression and information, media pluralism, and open debate remains equally important.

CCIA Europe supports the goal of enhancing election integrity and transparency. Many of our Members already implement robust content-moderation systems, with a combination of automated tools, human review, and specific policies in electoral periods (such as fact-checking partnerships and tools to disclose advertising). Nevertheless, content moderation during elections remains highly sensitive, and the line between harmful and legal speech is often legally and culturally nuanced.

In order to maintain the legitimacy of democracy safeguards, CCIA Europe believes that content-moderation expectations under the upcoming Democracy Shield should be clearly defined and limited to transparency requirements when it comes to harmful content (such as coordinated disinformation campaigns, deceptive foreign interference, or content that threatens democratic integrity). Online platforms should not be expected to act as arbiters of speech or political legitimacy, but should rather continue enhancing their already robust moderation systems that are transparent, proportionate, and contestable.

Fact-checking practices should remain plural and adaptive, recognising the diversity of approaches across platforms and the challenges posed by considerations such as scale, bias, and freedom of expression. CCIA Europe considers that initiatives that encourage user participation, and which are empowerment-based, should be promoted to fight misinformation.

Further, due process, appeal mechanisms, and transparency for users affected by content-moderation decisions are already mandated in the DSA and the political advertising regulation. Further measures should thus be avoided for the sake of clarity. This would also

avoid creating an incentive for online service providers to opt for over-removal of lawful content, particularly during politically sensitive periods, such as elections.

To ensure plurality and preserve democracy, users of online services must be able to engage with a variety of online voices. Mandating moderation of content that is not clearly defined as illegal risks undermining the democratic values that are meant to be protected and that characterise the European Union. Protecting elections while preserving freedom of speech is not contradictory, rather these are mutually reinforcing goals that require a public sphere that relies on trust and respect for individual rights.

In the EU, the EMFA already establishes a common framework for media services, including measures that seek to protect media providers and journalists from political interference. Considering its entry into application will only start in August 2025, it would be prudent for the EMFA implementation to be a reality before considering any additional layer of measures that may be duplicative.

III. Strive towards a proportionate, risk-based, and future-proof approach

Building societal resilience in the long term requires a whole-of-society approach that goes beyond online services. This also depends upon education, media literacy, and providing Europeans with adequate tools to navigate a digital environment that is constantly evolving. That is why CCIA Europe supports the Commission's focus on digital and media literacy, as critical thinking and informed civic engagement are essential to an informed society.

Policy proposals to promote resilience should therefore firstly be proportionate to the risks. Digital services differ vastly in terms of design, function, reach, and risk profile. While social media platforms may be more impacted when it comes to the spread of disinformation, other services such as online marketplaces, search engines, cloud infrastructure providers, and file-sharing services have a different role in the information ecosystem.

Adopting a risk-based approach that focuses on metrics – such as an online service's actual impact on public discourse or its technical capacity to implement mitigation measures – is essential to guaranteeing the right actors are asked to put in place the necessary measures.

Moreover, the Democracy Shield should ensure flexibility in implementing mitigation measures in line with Article 35(3) of the DSA, i.e. allowing platforms to test and adapt their responses based on the nature and capabilities of their service. At the same time, reinforcing structured cooperation between Member States, civil society, and international actors (e.g. NATO, G7) will be essential in tackling evolving threats such as malicious actors that use AI to generate disinformation.

Secondly, a principle-based approach is required to guarantee adaptability. Emerging threats such as deepfakes or deceptive AI-generated content should be addressed through principles, shifting away from overly prescriptive frameworks. In this context, best practices such as industry memoranda of understanding[6], labelling standards, watermarking, or trust

[6] An example of best practices can be found in the 'Tech Accord to Combat Deceptive Use of AI in 2024 elections', which sets expectations on how to manage risks arising from deceptive AI election content. More information available here.

indicators should be promoted. This would also help correctly identify where the gaps might be and how to better address them in future EU strategies.

Thirdly, the European Democracy Shield should advance innovation and flexibility in civic tools, AI safety mechanisms, and promote educational partnerships to achieve a truly resilient society.

The EU's legislative framework already provides a structure that is adaptable to the evolving categories of risk, through the provisions in the DSA, as well as other rules such as the General Data Protection Regulation (GDPR). In this context, the European Democracy Shield should act as a flexible tool for cooperation in light of technological evolution, particularly in new domains such as generative AI. Emerging risks, such as AI-generated misinformation or synthetic media impersonating political actors, must certainly be tackled, but without resorting to prescriptive or inflexible measures that would quickly become outdated.

IV. Target responsibilities and guarantee transparency in electoral processes

A dynamic democracy depends on the active and informed participation of its citizens. Digital services have transformed civic engagement, enabling anything from online petitions to the organisation of political rallies and real-time election information.

CCIA Europe believes that trust and transparency are key to making meaningful participation a reality. To that end, it is necessary to clarify the responsibilities of political actors, campaigners, and advertisers. These parties are best placed to disclose information regarding the content and targeting of their messages, their intentions, and their sponsors – instead of having intermediaries be responsible for such disclosures. In turn, online services should then be able to rely in good faith on the declarations provided, without shifting investigative duties onto intermediaries.

Moreover, when asked to disclose data or further information regarding content moderation decisions, these requests must meet the strongest data protection safeguards. This in order to guarantee respect for privacy, proportionality, and commercial confidentiality, in line with the respective requirements under both the GDPR and the DSA.

The participation of citizens in democratic processes is crucial, it must be inclusive and rights-based. Any future initiatives built under the European Democracy Shield should avoid requirements that could have chilling effects, are overly burdensome on users and businesses, or could inadvertently discriminate against access to political speech online.

The protection of civil society actors and journalists is also key, in line with the Commission's plans for a Civil Society Strategy. CCIA Europe's Members often collaborate with these stakeholders, and consider their protection to be integral to achieving a resilient democratic ecosystem.

By way of example, our Members already provide reliable information (such as details about voter registration and election results), offer cybersecurity services free of charge to activists, NGOs, and journalists, and even election security for government websites.[7]

To reinforce the democratic ecosystem, it is essential to strengthen capacity-building for actors beyond online services, including election authorities, civil society, and media. The Commission should actively support civic-dialogue tools and platforms that are open to everyone and welcome engagement. Think, for example, of election hubs, media literacy campaigns, voter information, and partnerships with election bodies as well as NGOs – all contributing to ensure resilient and inclusive participation.

Conclusion

CCIA Europe strongly supports the Commission's goal of better protecting and promoting democracy, as well as reinforcing the integrity of elections and societal preparedness at large. The Democracy Shield represents an opportunity to consolidate progress already made in the past years.

For it to be successful, the Shield must consolidate and build on the robust frameworks that we have in place, but also make sure it upholds fundamental rights (such as freedom of expression and information) and reinforces the shared responsibilities across the information ecosystem.

Threats such as disinformation and foreign information manipulation and interference can only be tackled jointly. This requires combining the best efforts of online services with the promotion of education and media literacy across the entire EU, along with strengthening cooperation among all societal actors involved in safeguarding our societies.

CCIA Europe and its Members remain committed to supporting the European Commission in shaping and implementing a proportionate, future-proof strategy that will ensure democracy in Europe remains open, inclusive, and resilient in the digital age.

[7] Strengthening cyberresilience for journalists, NGOs and activists, as well as for government websites in time of elections remains crucial when tackling threats of external interference in European elections.

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