OPEN _FUTURE

FOSTERING PLURALITY, INTEGRITY AND SAFETY IN DIGITAL PUBLIC SPACES

Policy Building Blocks for the Digital Commons #4

OPEN FUTURE POLICY BRIEF

Authors: Aditya Singh & dr Zuzanna Warso

9 APRIL 2026

ABOUT THIS POLICY BRIEF

NGI Commons (Open Source and Internet Commons for Europe's Digital Sovereignty) project is funded by the European Union's Horizon Europe research and innovation programme under Grant Agreement number 101135279. This work has received funding from the Swiss State Secretariat for Education, Research, and Innovation (SERI).

Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

The text of this document is based on a report—Deliverable 3.4—submitted to the European Commission as a deliverable of the NGI Commons project. It is part of a series of policy briefs to inform advocacy on Digital Commons and digital sovereignty in the context of the upcoming Multiannual Financial Framework (2028–2034). All NGI Commons deliverables are available on the project website.

Open Future is a European think tank that develops new approaches to an open internet that maximize societal benefits of shared data, knowledge and culture. Open Future advocates for Digital Commons—characterized by distributed production, collective governance, and shared stewardship—as offering the most viable path towards a resilient digital ecosystem.

Aditya Singh is a Senior Policy Analyst at Open Future with expertise in digital rights, data governance, and technology ethics. His doctoral research on agricultural data governance informs his interests in commons, food systems, and knowledge infrastructures.

dr Zuzanna Warso is the Research Director at Open Future. She has fifteen years of experience with human rights research and advocacy. In her work, she focuses on the intersection of science, technology, human rights, and ethics. She holds a Ph.D. in International Law from the University of Warsaw.

INTRODUCTION

Digital sovereignty, understood as the ability of states, organizations, and individuals to independently shape and control their digital environments, has become a central concern for the European Union. Risks to sovereignty include threats to the integrity of public discourse and democratic processes.

Social media platforms, where much of contemporary social and cultural exchange occurs, have become vectors for misinformation, electoral interference, and harm to marginalized communities. The risk lies not only in non-European jurisdictional control, but in a surveillance-driven business model that structurally amplifies these harms. Addressing these risks requires, in addition to regulatory oversight, alternatives that are rooted in public value. This brief proposes a framework for public investment in interoperable, commons-based communication infrastructures that foster plurality, integrity, and safety in public discourse, instead of engagement and virality.

PROBLEM DEFINITION: COMMUNICATION PLATFORMS AS VECTORS FOR THREATS TO SOVEREIGNTY

Digital sovereignty must include protecting the integrity of, and fostering plurality in, digital public spaces. In the context of social media, two key risks to sovereignty remain: reliance on communication infrastructures that non-EU jurisdictions can surveil and disrupt access to, and platforms becoming vectors for electoral interference and coordinated influence.

Dominant platforms profit from enclosure, large-scale surveillance, opaque algorithmic curation, and behavioural manipulation. These dynamics are structural features of their business models, contributing to social polarization, information disorder, labour rights violations, and a degraded digital public space.1

Developing alternative platforms—with infrastructure hosted in the EU—may mitigate geopolitical risks, but does not address this misalignment with public interest. Even when regulated, the business models of current platforms relegate the democratic quality of discourse or the protection of fundamental rights as considerations secondary to core commercial objectives. This undermines their character as spaces where much of contemporary democratic and social exchange takes place.

This has enabled dominant platforms to be frequently weaponized by well-resourced actors to launch coordinated campaigns of influence and harm, including interference in democratic processes and the amplification of harmful content, often targeting minorities.2 Protecting the

---

[1] Keller, P., and Warso, Z. (2023). Digital Public Space Primer. Open Future. Available at: https://openfuture.eu/publication/digital-public-space-primer/.

[2] See for instance: Hybrid Election Integrity Observatory (2026). Dutch Parliamentary Elections 2025 Report. Available at: https://www.heio.nl/wp-content/uploads/2026/01/260115-HEIO-Final-Report.pdf.

integrity of these spaces is therefore not only a matter of consumer choice or digital regulation, but of societal resilience.

To date, the EU's focus has been on regulating the negative impacts of platform dominance rather than establishing structural alternatives. Regulation can introduce important safeguards—such as transparency and accountability in algorithmic systems, access to platform data and source code for increased scrutiny, and impact assessments to evaluate systemic risks. However, while a robust regulatory framework can mitigate harm, it cannot substitute for public stewardship and governance of core communication infrastructure. Regulation operates within the constraints of existing platform architectures and incentives. It does not fundamentally restructure how digital public spaces are organized, nor does it create viable alternatives to dominant models.

This brief sets out a series of proposals on spending priorities related to Digital Public Space in the upcoming Multiannual Financial Framework. It presents a framework for fostering an ecosystem of interoperable social networking architectures, with public-interest feed curation and public provisioning of core hosting and safety infrastructures.

PROPOSED INTERVENTION

Incumbent platforms entrench their position by leveraging network effects and closed ecosystems, where leaving a platform entails losing content, history, connections, and audiences. The alternative is not to replicate another platform, but to enable an ecosystem where diverse services can emerge, and where proprietary infrastructure no longer cements dominance.

Emerging protocol-based networks such as Mastodon (based on ActivityPub) and Bluesky (based on the ATProtocol) demonstrate the potential of decentralized and federated approaches. ActivityPub's federated model allows users to choose among independently operated servers that each manage their own moderation and hosting, while still interoperating through a shared protocol. The ATProtocol enables users to port their identities and content across providers, and to choose between different hosting providers, moderation services, and content feeds.

These architectures point towards a restructuring of social networking as a user-directed assembly of interoperable services, rather than a vertically integrated platform controlled by a single entity.

At the same time, these approaches face structural constraints in the form of network effects and first-mover advantages enjoyed by incumbent platforms. This points to the need for technical and policy interventions that both enable interoperability with dominant platforms—supporting the emergence of alternatives—and ensure resilience against the rise of new incumbents.

Advocacy around algorithmic pluralism demonstrates that elements of the existing regulatory framework—particularly under the DSA and DMA—can be leveraged to support a transition

towards more interoperable and user-directed architectures, including enabling choice between algorithmic recommender systems and third-party curation services.3

Supporting Plurality and Public Interest Curation

Many of the harms associated with current platforms stem from the engagement-driven logics of surveillance-based advertising, which optimize for attention capture. These dynamics systematically reward outrage, polarization, and virality.4

Interoperable networks and algorithmic choice give users greater agency over their information environments, while enabling a wider range of actors to provide curation and recommendation services. Just as media pluralism is essential to democracy, algorithmic pluralism should be embedded in the infrastructure of search, recommendation, and social feeds, strengthening the resilience of the information ecosystem.5 Users must be able to understand, choose, and switch between the systems that shape what they see, much like choosing between different media outlets.

At the same time, meaningful plurality requires not only user choice, but genuine diversity in the business models and incentives shaping these systems. This includes a variety of commercial, subscription-based, non-profit, and publicly funded approaches.

Non-profit and publicly backed models, in particular, can support forms of algorithmic curation that do not depend on engagement maximization or virality. Public broadcasters, with their long tradition of public-interest curation, could play a key role here.6 Commons-based models offer further alternatives, grounded in participatory and community-led governance.

Public funding can therefore play a pivotal role in sustaining an ecosystem of diverse algorithmic curation providers, particularly where commercial incentives fail to deliver outcomes aligned with public interest.

---

[3] People vs Big Tech (2023). Algorithmic Plurality: A Pro-Competitive Solution to Build Healthier Social Media Networks. Available at: https://peoplevsbig.tech/algorithmic-plurality-a-pro-competitive-solution-to-build-healthier-social-media-networks/.

[4] Milli, S., Carroll, M., Wang, Y., Pandey, S., Zhao, S., and Dragan, A. D. (2025). Engagement, user satisfaction, and the amplification of divisive content on social media. PNAS Nexus, 4(3), pgaf062. https://doi.org/10.1093/pnasnexus/pgaf062.

[5] Christian Fuchs and Klaus Unterberger, eds., The Public Service Media and Public Service Internet Manifesto (2021), https://doi.org/10.16997/book60. This collection proposes adapting the institutional logic of public service media (public funding, editorial independence, and accountability) to the digital sphere, offering a normative framework for developing non-commercial, democratic alternatives to dominant platform infrastructures.

[6] CBC/Radio-Canada (2024). Public Spaces Incubator announces two-year partnership extension and addition of Australian and German public broadcasters ABC and ARD. Press release. Available at: https://cbc.radio-canada.ca/en/media-centre/public-spaces-incubator-two-year-partnership-extension-announcement.

Supporting Resilient Infrastructure

Public interest curation, on interoperable networks, may still require a core of publicly provisioned infrastructure. Even on interoperable networks, dominant providers and chokepoints can emerge, based on the resources and coordination needed to run infrastructure as the network scales. Control over critical infrastructure can then translate into power over other functions that depend on it, such as curation and moderation.

The experience of ActivityPub and the ATProtocol illustrates these dynamics. Providers of resource-intensive infrastructures can consolidate influence over the information environment. Although there is an increasing proliferation of alternative hosting and indexing infrastructure on ATProtocol, there remains a substantial, network-wide reliance on Bluesky PBC's core indexing and moderation infrastructure.7

Content moderation is equally critical in digital public spaces, serving user safety, regulatory compliance, and resilience against coordinated misinformation and harm.8 Actors that provide trust and safety infrastructure can leverage this role to exert broader control over the network. For instance, on ActivityPub, large servers concentrate moderation authority in ways that undermine the network's decentralized architecture.9

This demonstrates how commercial actors can retain de facto norm-setting power across an ecosystem, even where the protocol itself is open, when they provision infrastructure critical to the network.

As interoperable networks scale, the sustainability models for provisioning hosting infrastructure remain nascent and largely untested. Where commercial models do emerge, they risk reintroducing incentives around surveillance-based advertising, attention capture, and engagement optimization. Public investment in non-commercial infrastructure is a mechanism to ensure the sustainable provision of core infrastructures and the resilience of the network against new forms of capture.

Public Coordination for Safety

Social media has become a powerful vector for threats to sovereignty, democratic resilience, and the health of public discourse. Even though they have frequently failed to meaningfully safeguard against such threats, dominant, centralized platforms are able to develop internally coordinated responses to them.

---

[7] The venture-backed corporation based in the United States that leads the development of the Bluesky app on ATProtocol.

[8] Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. New Haven, CT: Yale University Press.

[9] Spencer-Smith, C., & Tomaz, T. (2025). Labour pains: Content moderation challenges in Mastodon growth. Internet Policy Review, 14(1). https://policyreview.info/articles/analysis/content-moderation-challenges

In the context of coordinated cross-infrastructure and cross-protocol threats—harassment campaigns, disinformation operations, electoral interference—there may be no actors with the capacity and mandate to respond at ecosystem scale.10 On open protocols, individual providers may address threats within their own systems, but lack the network-wide insight and capacity to identify and address coordinated activity across infrastructures or protocols. In addition, much of the moderation work on open protocols currently relies on volunteers—creating a dynamic analogous to that of critical open source projects: essential infrastructure sustained by individual commitment but chronically under-resourced.11 Commercial actors may have little incentive to address these gaps, given the coordination and costs involved.

Current trust and safety architectures—such as shared CSAM hash databases, Non-Consensual Intimate Imagery alerts, illegal content takedown mechanisms, trusted flagger programs—have all been designed for a small number of large, vertically integrated platforms.12 These systems presuppose an infrastructure that decentralized networks usually lack, and may require additional coordination to ensure the safety and integrity of the networks.

The dominance of commercial platforms has had the consequence of externalizing and privatizing these functions, subordinating them to commercial logics and business models that undermine incentives to act in the public interest, while exposing the inherent limitations of regulatory oversight.

This points to the safety and integrity of digital public spaces as fundamentally a public responsibility. Like physical infrastructure that enables communication and exchange, digital public spaces require sustained investment, alignment with democratic values, and public oversight and coordination to remain safe, accessible, and resilient.

FIT WITH THE MULTIANNUAL FINANCIAL FRAMEWORK

The integrity and plurality of digital public spaces depend not only on regulation, but on the availability of underlying infrastructures that are governed in the public interest. From this perspective, digital public spaces should be understood as a form of Digital Commons: shared communication infrastructures whose value derives from collective use, democratic governance, and long-term stewardship rather than exclusive ownership or extractive business models.

The proposals set out in this brief map onto several instruments within the upcoming MFF.

---

[10] Kalidindi, K. (2025). Moderating cross-platform and cross-instance abuse on decentralized networks. Tech Policy Press. https://www.techpolicy.press/moderating-crossplatform-and-cross-instance-abuse-on-decentralized-networks/.

[11] Rozenshtein, A. Z. (2024). Moderating the Fediverse: Content moderation on distributed social media. In K. Langvardt & J. Hurwitz (Gus) (Eds.), Media and society after technological disruption (pp. 177–192). Cambridge University Press.

[12] Lai, S., & Roth, Y. (2024). Online safety and the "great decentralization": The perils and promises of federated social media. Tech Policy Press. https://www.techpolicy.press/online-safety-and-the-great-decentralization-the-perils-and-promises-of-federated-social-media/.

The objectives of this intervention align closely with the broader goals of the **European Competitiveness Fund** proposed within the next Multiannual Financial Framework, as well as calls from Digital Commons communities for an EU-level Sovereign Tech Fund (STF). Both initiatives emphasize strategic investment in technological sovereignty and resilience. The integrity and plurality of digital public spaces are essential components of sovereignty and must be recognized as such within the Union's investment frameworks.

The ECF's **Digital Leadership** window is the most direct vehicle for investment in interoperable communication infrastructures. Funding should be channeled toward the provisioning of resource-intensive infrastructures where commercial capture poses sovereignty risks, such as core hosting infrastructure and trust and safety infrastructure. This could be sustained through a Sovereign Tech Fund-style instrument to better address issues related to the under-resourcing of open protocol infrastructure.

Horizon Europe, and instruments modelled on the NGI initiative, remain important vehicles for research and innovation in decentralized infrastructures, commons-based governance, and algorithmic transparency

AgoraEU is meant to support the "pillars of strong democracy, including culture, media, and civil society," while addressing threats such as declining media pluralism and disinformation. This brief's objectives of supporting democratic digital spaces align closely with this mission, making AgoraEU the appropriate home for funding public-interest curation providers—including public broadcasters developing algorithmic curation services, and commons-based or non-profit recommendation infrastructure.

Through **Global Europe**, the EU can co-develop democratic models related to hosting and content infrastructures internationally, recognizing the global nature of Digital Public Spaces (and threats to them), and the need to uphold plurality across cultural and political contexts.

The **Single Market Programme** can support standardization efforts, national coordination, and capacity building for the adoption of interoperable and open digital infrastructures.

LEGAL AND POLICY CONTEXT

The **Digital Services Act (Regulation (EU) 2022/2065)** establishes transparency, accountability, and oversight obligations for online platforms, especially 'Very Large Online Platforms.' These provisions establish a baseline for oversight but focus primarily on mitigating harms from dominant private actors rather than enabling the creation of structural alternatives. The DSA's provisions on systemic risk mitigation and algorithmic transparency can serve as the foundations for further investment in public interest infrastructures that operationalize these principles by design.

The **Digital Markets Act (Regulation (EU) 2022/1925)** includes obligations for gatekeeper platforms, particularly regarding interoperability, access, and data portability, supporting the development of a more plural and competitive ecosystem. Article 7 (Interoperability of Number-

Independent Interpersonal Communication Services) and Article 6(9) (data access for business users) provide a legal precedent for unbundling platform functions and enabling competition in algorithmic and moderation services.

The proposed review of the DMA specifically requires the European Commission to assess whether greater interoperability requirements should extend to providers of social media services. This offers a window to institutionalize algorithmic plurality and provide users with access to third-party feed curation and moderation tools.

The **EU Democracy Shield**, proposed by the Commission as part of a broader response to information manipulation and interference, establishes a framework for coordinated action to protect democratic processes and public discourse. Where the Democracy Shield addresses threats to democratic resilience at the level of detection and response, the proposals set in this brief provide a complementary structural layer: communication infrastructures that are, by design, less susceptible to capture and manipulation, and governed in ways that are accountable to democratic values.

The **European Media Freedom Act (Regulation (EU) 2024/1083)** establishes safeguards for media pluralism and transparency of media ownership, and introduces requirements to ensure that state actors and large platforms do not interfere unduly in editorial freedom. Its emphasis on protecting the integrity of the media landscape provides a framework for extending similar principles to the governance of digital public spaces, which can be seen as structural enablers of media pluralism and independence.

The proposed **Digital Fairness Act** (forthcoming) seeks to adapt core EU consumer protection principles to contemporary digital practices. It targets manipulative interface design and seeks to strengthen transparency obligations for personalized recommendations, pricing, and rankings, including those driven by social media algorithms. The DFA can reinforce the case for social media infrastructures that are non-manipulative, auditable, and respect user autonomy. This supports the broader shift toward public-interest alternatives where content curation and algorithmic systems are transparent and accountable by design.

RESOURCE REQUIREMENTS AND FUNDING INFRASTRUCTURE

Building on existing estimates for large-scale digital infrastructure serving tens of millions of users, and aligning with the objectives of the European Competitiveness Fund (ECF), an indicative budget of €100–150 million over seven years is recommended to establish and sustain public digital infrastructures that underpin digital public space. This figure reflects the ambition to serve a population of more than 450 million citizens across multiple languages, while also integrating civil society and public media partnerships on a European scale.

This amount is based on a co-funding structure:

- EU contribution: 60–70%

- Member state contribution: 20–30%
- Other funding (business, philanthropy, media partnerships): 10–15%

Support mechanisms should include:

- Funding for non-profit and public-interest infrastructure providers of recommender systems, hosting providers, and moderation services.
- Targeted support for civil society participation, enabling public broadcasters, libraries, academic institutions, and non-profit organizations to act as trusted nodes and curators within interoperable networks.
- Dedicated funding for coordinated integrity mechanisms, ensuring the safety, trustworthiness, and resilience of digital public spaces through shared moderation, security, and audit functions.
- Grants for federated and decentralized infrastructure development, including investments in interoperability tooling, cross-protocol communication layers, and commons-based governance frameworks.
- Capacity-building and adoption programmes for public institutions, local administrations, and civil society organizations to strengthen their ability to deploy, maintain, and participate in interoperable digital infrastructures.

POSSIBLE RISKS AND MITIGATIONS

Decentralized and federated ecosystems risk fragmentation or low adoption if they fail to match the usability and reach of commercial platforms. Addressing this requires pairing regulatory reform related to interoperability, industrial policy, and R&D funding to strengthen the ecosystem of interoperable service providers. Infrastructural funding should be combined with public sector adoption mandates: public institutions and broadcasters can anchor early adoption and generate the network effects necessary for broader uptake.

Federated and decentralized systems also remain vulnerable to coordinated abuse, given the uneven moderation capacity across providers. Mitigating this risk requires co-regulatory or federated coordination mechanisms that preserve decentralization while enabling joint responses to systemic threats.

At the same time, coordinated mechanisms for trust and safety could themselves reintroduce concentration and infrastructural bottlenecks. This could be addressed through governance structures grounded in commons-based and multi-stakeholder principles, with strong civil society representation, transparent decision-making processes, and public-interest mandates.

Providers of curation services may struggle to sustain operations without resorting to commercial models that undermine their objectives. Sustainability should therefore be built into

the funding design from the outset, through multi-year operational funding commitments, co-funding models with public broadcasters, and integration into national digital sovereignty strategies that create durable institutional adoption and support.

IMPLEMENTATION PATHWAY

This intervention requires a coordinated approach, addressing regulatory and institutional foundations in parallel with the infrastructure and investment needed to foster a thriving ecosystem.

In the near term, from 2026 onwards, the priority is to use existing regulatory instruments as levers for structural change. This entails advocacy around the enforcement and reform of the DMA and DSA, with a focus on advancing unbundling and interoperability requirements for platform services—including pushing for the extension of interoperability obligations to social media providers in the forthcoming DMA review.

In parallel, public institutions should be required to adopt and pilot interoperable platforms, creating early institutional demand. This serves a dual purpose: it demonstrates viability at scale and generates the initial network effects that alternative ecosystems need to compete with incumbent platforms. Public broadcasters and other public interest media organizations, given their existing mandates around plurality and public interest, can be seen as natural early adopters.

From 2028 onwards, and in alignment with the new MFF cycle, the focus shifts to dedicated funding and governance at scale. This includes securing dedicated budget lines within relevant MFF instruments—such as the ECF's Digital Leadership window and AgoraEU—for the sustained provisioning of core hosting infrastructure, trust and safety coordination, and public-interest curation services. The goal is to enable a diverse ecosystem of hosting providers, moderation services, and algorithmic curation providers to experiment, develop, and scale across different business models—including non-profit, cooperative, and publicly funded approaches.

Alongside this, long-term governance and coordination mechanisms need to be established to maintain the resilience and public accountability of core infrastructures over time. This includes multi-stakeholder oversight with civil society representation, and capacity-building programmes to support member states in developing and sustaining national contributions and implementations in the ecosystem. These mechanisms should be designed from the outset to be durable across political cycles, ensuring that investment in digital public space is treated as the ongoing infrastructural commitment it is, rather than a time-limited project.

Ensuring a resilient Digital Public Space is not a one-off investment but an ongoing infrastructural expense—analogous to the sustained public funding that underwrites public broadcasting, press freedom bodies, or communications regulators. This brief presents the conditions that sustained funding should enable: interoperable infrastructure that is resistant to capture; information environments grounded in public interest; and public coordination for safety and integrity.