



Cloudflare Position Paper: The EU Digital Networks Act

Introduction

Cloudflare supports the European Commission's objective to foster a competitive, secure, and resilient European Digital Single Market. As the Commission has recognized, the next frontier of European innovation depends on a fundamental shift towards distributed, highly interconnected edge networks. Cloudflare shares the Commission's goal of ensuring that European citizens and businesses have access to high-speed, reliable connectivity.

As the leading connectivity cloud company operating one of the world's largest and most interconnected networks, Cloudflare is well-positioned to play a critical role in realizing the Commission's goal of creating an innovative, prosperous, and connected society. Cloudflare's network distributes computing power as close as possible to end users, accelerating the development of breakthrough digital technologies and empowering industry, government, and citizens to leverage transformational digital tools like artificial intelligence. By processing data at the edge, companies like Cloudflare enable, at low cost, real-time AI inference, low-latency industrial automation, and enhanced cybersecurity protections. These services have the power to close the EU's innovation gap and empower a new generation of high-growth European startups and enterprises.

Certain provisions in the EU Digital Networks Act (DNA) proposal, however, would stifle the ability of Cloudflare and similar cloud computing entities to help the Commission achieve these important goals. Despite the Commission's statement that it "does not seek to regulate cloud services," several measures would extend telecommunications-style regulation to the cloud and content-delivery sectors, curtailing the deployment of new innovative services and undermining the EU's effort to be a leader in the digital age.

Specifically, the possible inclusion in the General Authorization regime (article 9) of innovative connectivity platforms such as content delivery network (CDN) services and cloud infrastructure – which enable European businesses and startups to scale and digitize their workloads – would increase their regulatory burden and impose on them one-size-fits-all telco-style rules that are ill-suited for these types of providers. Such an expansive scope of the DNA ignores the distinct role the entities play in the Internet ecosystem, complementing last-mile connectivity providers by facilitating the secure and efficient distribution of Internet traffic, before it reaches the ISPs.

Moreover, the potential application of a mandatory dispute resolution mechanism (article 189), the introduction of "ecosystem cooperation" guidelines (article 191), and "voluntary

conciliation" mechanisms (articles 191-193) collectively threaten to disrupt the well-functioning market for IP interconnection, subject CDNs and similar services to unnecessary and overly burdensome regulatory obligations, and create a *de facto* network usage-fee framework. The DNA further risks undermining the benefits of distributed networks and the resilience of the Internet in Europe by artificially reducing the number of interconnections and creating a two-speed Internet.

An innovative and competitive digital ecosystem needs the right conditions to flourish. To better achieve the Commission's aims and to avoid imposing unnecessary costs and burdens on European end users and SMEs, we urge policymakers to refine the DNA to ensure that it targets actual market failures where regulatory intervention is needed rather than imposing burdens on well-functioning and competitive interconnection markets. Our specific recommendations on the DNA proposal are outlined below.

Scope of General Authorisation: Avoiding a "One-Size-Fits-All" Approach, Burdensome Obligations and Mandatory Dispute Resolution

The DNA's General Authorisation regime applies to public providers of "electronic communications networks" (ECNs) and "electronic communications services" (ECSs) and defines those terms consistent with the 2018 European Electronic Communication Code (EECC). Cloud infrastructure and CDN services are not included in the EECC's definitions.

Despite using similar definitions for ECNs and ECSs as the EECC, the DNA contains additional references that could make providers of cloud infrastructure and CDN services subject to the General Authorisation regime. Specifically, article 9(2) states that the General Authorisation regime applies to ECNs and ECSs "used, wholly or mainly, for the purpose of providing electronic communications services or information society services available to the public." Recitals 5 and 16, moreover, refer to a digital ecosystem that is more expansive than ECNs, but at no point does the DNA make clear what entities are part of these digital networks. These and other similar references risk making providers of CDN and cloud services subject to burdensome and innovation-hindering regulatory obligations.

Distinct Technical Roles: Bringing CDNs and cloud infrastructure within scope of article 9 fails to account for the important technical and functional differences between the services Cloudflare and similar entities provide versus the transmission of electronic signals that is enabled by telecommunications networks. Whereas such networks provide connectivity to end users through physical infrastructure, Cloudflare is a connectivity cloud company that layers on top of the physical network to enable secure, efficient, and sustainable content delivery to telecommunications providers' networks and their end-users through distributed caches and points of presence. In other words, Cloudflare provides security, performance, and reliability services that *complement* the networks of

telecommunication providers. Companies like Cloudflare play no role in providing the underlying physical connectivity to the end-user but rather provide a wide range of benefits to the overall distribution and security of Internet traffic, facilitating telcos' primary task of delivery of content to users.

The Risks of Mandatory Dispute Resolution: If they would be found in scope of article 9, providers of cloud infrastructure and CDN services may also be subject to the mandatory dispute resolution mechanism outlined in article 189 of the DNA. As with the voluntary conciliation mechanism discussed below, a mandatory dispute resolution mechanism risks creating a backdoor to force Cloudflare and other application service providers to pay "network usage fees," thus becoming what the telecommunications industry has described as one of "the possible tools for direct compensation."¹ As Stanford Professor Barbara van Schewick has explained²: "An arbitration mechanism is just another way of introducing network usage fees on multiple sectors and consumers."

Cloudflare Recommendation:

Clarify the Scope: The Regulation must make clear that the scope of articles 9 and 189 do not apply to CDNs or cloud infrastructure.

Simplification vs. Administrative Burden

Cloudflare supports the aim of the DNA to "simplify and streamline" EU legislation to reduce administrative burdens, including through the creation of a Single Passport mechanism (article 10) for General Authorization, whereby a provider need only notify one national regulatory authority of its intent to provide services in any of the Member States. While Cloudflare supports the Commission's simplification agenda, extending the DNA's scope to the cloud and CDN sectors achieves the opposite.

Regulatory Redundancy and Uncertainty: If the DNA were to regulate CDN or cloud services the same as (public) ECNs, the DNA proposal would subject them to overlapping and potentially duplicative regulatory regimes, creating ambiguity and confusion. In particular, article 9 imposes resiliency and preparedness requirements to ensure connectivity in the event of a man-made or natural disaster, and articles 4 and 5 impose resilience obligations on a broad set of actors. Many of these security and resiliency

¹ Axon Partners, *Europe's internet ecosystem: socio-economic benefits of a fairer balance between tech giants and telecom operators*
<https://connecteurope.org/insights/reports/europes-internet-ecosystem-socio-economic-benefits-fairer-balance-between-tech>

² Van Schewick, Barbara, *EU Telecoms' Newest Proposal to Force Websites to Pay Them Is Just As Terrible As Their Previous One*, Center for Internet and Society (June 2023),
<https://cyberlaw.stanford.edu/blog/2023/07/eu-telecoms-newest-proposal-force-websites-pay-them-just-terrible-their-previous-one>

obligations already apply to CDN and cloud computing services pursuant to the Network and Information Security 2 (NIS2) Directive, and the DNA lacks clarity about how these regulatory frameworks interact. This redundancy risks increasing administrative burdens for entities like Cloudflare without having any beneficial effect on network resiliency.

Harmful and Burdensome Regulatory Requirements: The DNA's regulatory obligations impose new compliance costs, reporting requirements to the new Office for Digital Networks (ODN), and mandatory engagement in regulatory proceedings. Other obligations, if applied to companies like Cloudflare, such as the requirement in article 9(2) to prevent electromagnetic interference, would require us to take action that we lack the technical capability of performing. Article 9(4)(e) could further impose new obligations on CDN services and private networks to intercept and make available to law enforcement information about its users based on different laws in the Member States in which the services are offered. In addition to creating new burdens to comply with different laws in each of the Member States, these types of new collection and retention obligations would fundamentally alter Cloudflare's trust-based relationship with customers.

Impact on Innovation: Cloudflare's network supports millions of SMEs and developers. These entities benefit from having access to large-scale, fast, reliable, and distributed edge compute and network infrastructure, and they depend on distributed edge networks to adopt and deploy AI technologies at scale. Increasing the regulatory costs and burdens on Cloudflare and other providers of distributed edge network services would adversely affect affordability and availability of services for European developers who rely on them to scale. By imposing significant administrative costs on services like Cloudflare's that act as a catalyst for innovation, the DNA is far more likely to impede rather than accelerate the ability of European companies to compete in the digital ecosystem.

Cloudflare Recommendation:

Focus on True Simplification: Regulatory reform should focus on streamlining rules for traditional telcos to facilitate fiber and 5G rollout, rather than expanding the regulatory net to capture successful digital services that are driving Europe's digital transformation.

Preserving the Success of IP Interconnection: Opposing "Network Fees" by Any Name

The DNA proposal introduces Article 191, requiring BEREC to publish guidelines on "facilitating ecosystem cooperation" between ECN providers and undertakings in "closely related sectors." These guidelines must expressly cover "technical and commercial matters" related to traffic delivery. Furthermore, Article 192 establishes a "Facility for voluntary conciliation" where National Regulatory Authorities (NRAs) mediate commercial disputes between telcos and other actors. BEREC is also directed to publish periodic

reports on ecosystem cooperation and the functioning of the voluntary conciliation facility.

Cloudflare strongly opposes regulatory intervention in the IP interconnection market. The Commission's own findings, supported by BEREC's 2024 IP Interconnection Report³, confirm that the market for transit and peering is healthy, competitive, and marked by falling prices.

Risk of "Backdoor" Network Fees: While the DNA stops short of mandating direct payments, Articles 191 and 192 create a regulatory framework for "fair contribution" debates. Any mechanism designed to resolve claims between Internet service providers (ISPs) and other entities like cloud services and CDNs presupposes that the latter are obligated to pay at least some amount for interconnection, bypassing the question of whether any payment is warranted in the first place. As we have stated previously⁴, arbitration or conciliation mechanisms regarding interconnection are simply a "network fee through the backdoor." Such a fee, moreover, would be inconsistent with the EU-US agreement⁵ reached last summer in which the EU stipulated that it would not maintain or introduce network usage fees.

Voluntary in Name Only: While Article 192 is labeled "voluntary," the involvement of NRAs and BEREC in commercial negotiations, as well as the public release of period reports, would create immense political and regulatory pressure on cloud service and CDN providers to pay termination fees. The proposal would likely shift leverage away from competitive market dynamics toward regulated settlements, incentivizing large ISPs to create artificial congestion to trigger the conciliation mechanism to seek payment from application services rather than investing in their networks.

Harm to the Open Internet Ecosystem: Currently, the vast majority of Internet traffic exchange (approximately 99%⁶) relies on settlement-free or low-cost peering. Articles 191 and 192 would disrupt the functioning of this ecosystem by creating a regulatory wedge between partners in these efficient relationships, increasing transaction costs, and

3

<https://www.berec.europa.eu/en/all-documents/berec/reports/berec-report-on-the-ip-interconnection-ecosystem>

⁴ Cloudflare contribution to the European Commission Call for Evidence on the Digital Networks Act, July 2025

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14709-Digital-Networks-Act/F3575496_en

⁵ Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade, Eur. Comm'n, Directorate-General for Trade & Economic Security, Aug. 21, 2025, https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en

⁶ Packet Clearing House, 2021 Survey of Internet Carrier Interconnection Agreements <https://www.pch.net/resources/Papers/peering-survey/PCH-Peering-Survey-2021/PCH-Peering-Survey-2021.pdf?>

ultimately raising prices for European consumers and businesses that depend on cloud and content providers to scale and grow. As Cloudflare described in a 2023 blog post,⁷ enabling a structure for network fees also risks creating a two-tier interconnection system, whereby large content providers who can afford to pay these fees to telecom operators can deliver faster interconnection than smaller ISPs and smaller content providers and cloud services, who don't have the same deep pockets. This would create an invisible fast lane where wealthy platforms can provide a smoother interconnection path for one group of consumers, resulting in slower, more congested lanes for everything else. It would furthermore impose high barriers to entry for small providers, disincentivize innovation and efforts to bring content closer to users, and deteriorate the Internet experience for users across the EU⁸.

Cloudflare recommendation:

Delete or significantly amend Articles 191, 192, and 193. The DNA should not regulate "commercial matters" in a market where no failure exists. Creating a new facility to address interconnection disputes, which are already subject to competition law and existing dispute resolution mechanisms under the Open Internet Regulation, would hinder the DNA's goal of streamlining regulation and spurring European innovation. Similarly, the review clause related to the voluntary conciliation mechanism should be removed as it implies that the system could be changed into a mandatory scheme unilaterally by the European Commission.

Conclusion

Cloudflare stands ready to assist the Commission in achieving the Digital Decade targets, including through passage of DNA legislation that will foster an innovative and well-connected digital ecosystem. To make this happen, the Commission should ensure that the DNA's scope is focused on last-mile network operators. Extending its reach beyond such operators will create regulatory confusion and impose compliance costs on services that have no role in providing telecommunications access, will increase red tape and administrative costs for businesses and regulators, and will drive up costs for small businesses and startups wanting to use innovative digital services. Furthermore, the DNA's proposed imposition of ecosystem cooperation and a voluntary conciliation mechanism (Articles 191 and 192) risks breaking the Internet's successful interconnection model. We respectfully request that the co-legislators reject attempts to regulate the commercial relationship between networks and content providers, ensuring the Internet remains open, competitive, and affordable for all Europeans.

⁷ <https://blog.cloudflare.com/eu-network-usage-fees/>

⁸ See also a 2025 study on this topic from Plum Consulting <https://plumconsulting.co.uk/study-on-the-negative-impacts-of-mandated-dispute-resolution-in-ip-interconnection/>

About Cloudflare

Cloudflare, Inc. is the leading connectivity cloud company. It empowers organizations to make their employees, applications, and networks faster and more secure everywhere, while reducing complexity and cost. Powered by one of the world's largest and most interconnected networks, Cloudflare blocks billions of threats online for its customers every day.

Cloudflare uses our global network, with a presence in over 335 cities in more than 125 countries, to offer a variety of services. Our robust suite of cloud-based cybersecurity services include services to make websites, applications, and networks faster and more secure such as comprehensive DDoS protection, a Web Application Firewall (WAF), and advanced bot management. Cloudflare also provides Zero Trust solutions for secure access to internal applications, all leveraging its expansive global network for performance and resilience.

In addition, our global network powers innovation through our developer platform, which enables developers to build and deploy applications at the edge, without needing to run their own servers. Our network includes GPUs, allowing developers to run generative AI inference and agentic AI tasks globally. Our customers' traffic is processed at the data center closest to the user, with no backhauling or performance tradeoffs, and the delivery of this traffic can be localized according to our customers' preferences. This means our edge-computing power brings latency-sensitive AI and cloud workloads closer to end-users.

To further its mission to "help build a better Internet," Cloudflare makes its services widely available. Cloudflare service offerings range from enterprise services, used and trusted by 36% of the Fortune 500, to free and low-cost services that provide an important and accessible option for necessary cybersecurity services for millions of individuals, nonprofits and SMEs. Recently we have put even more of an emphasis on supporting startup and small business communities, including many [European startups](#), by expanding free developer tools, which make it easier for anyone to build full stack, AI-enabled applications directly on Cloudflare's network. We have also invested in programs to help developers like [Cloudflare for Startups](#), [Workers Launchpad](#), and the [Dev Alliance](#).