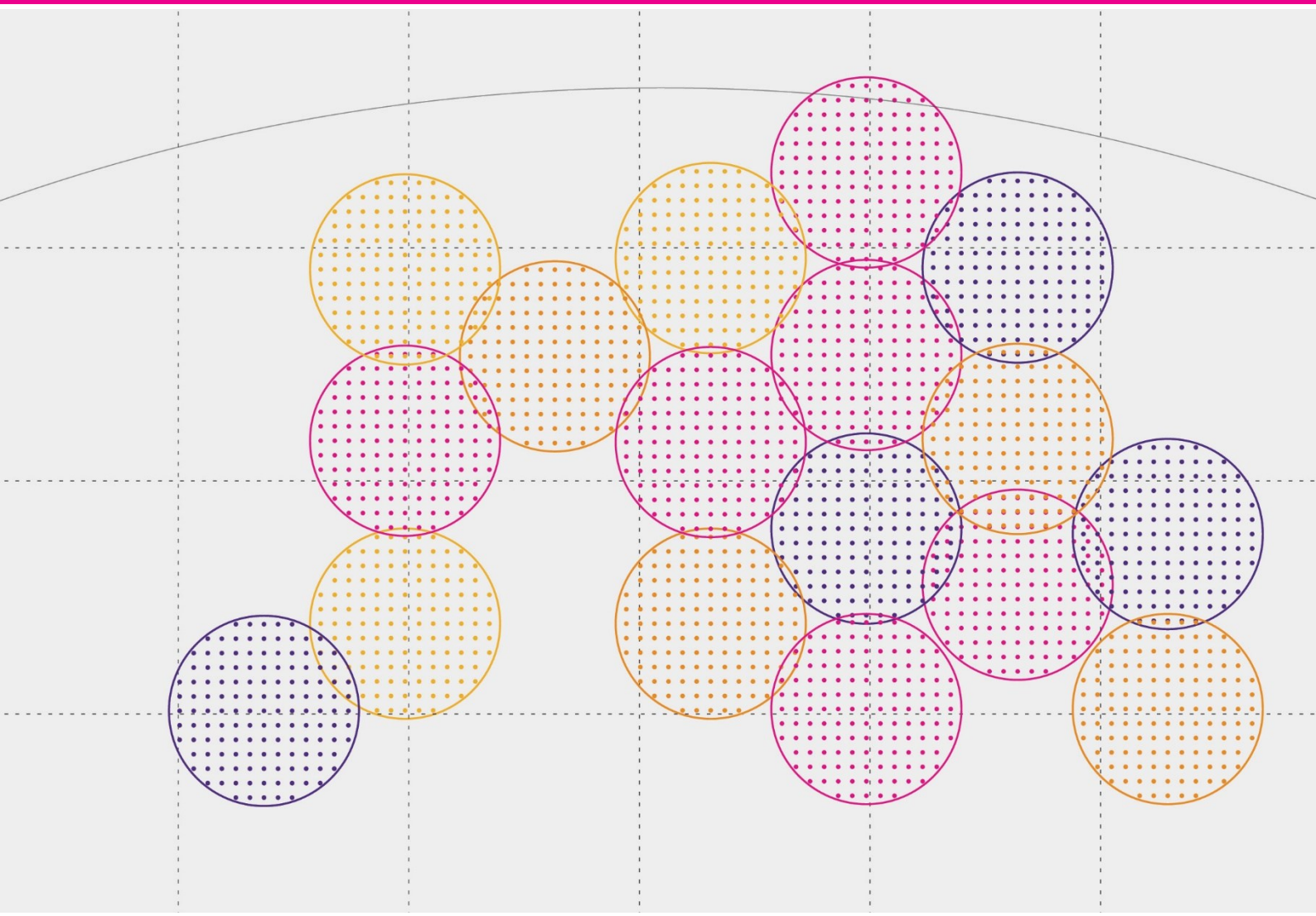
Consequences of EC proposals to extend regulatory scope to the entire digital economy

June 2024

Aude Schoentgen, Benoît Felten



plumconsulting.co.uk

About Plum

Plum offers strategy, policy and regulatory advice on telecoms, spectrum, online and audio-visual media issues. We draw on economics and engineering, our knowledge of the sector and our clients' understanding and perspective to shape and respond to convergence.

About this study

This study funded by Google and supported by CCIA examines the potential impacts of the regulatory changes proposed by the EC in its White Paper "How to master Europe's digital infrastructure needs?".

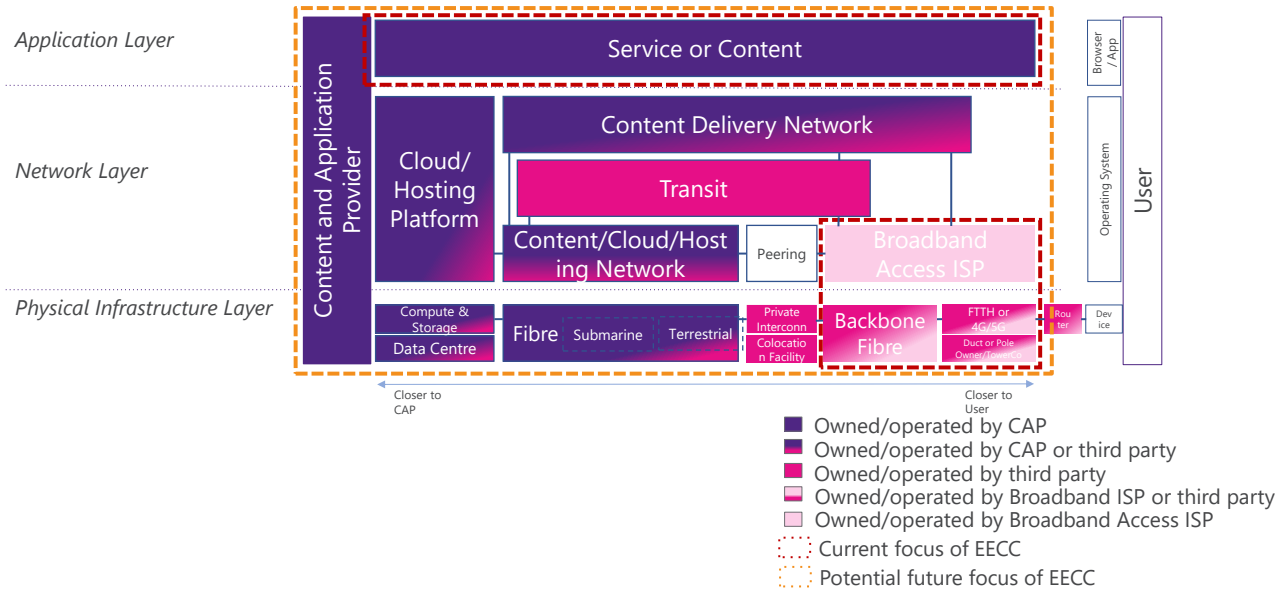
Plum Consulting
59 rue de Ponthieu
Bureau 326
75008 Paris
E info@plumconsulting.co.uk

Contents

Summary

The European Commission's White Paper "How to master Europe's digital infrastructure needs?" included, amongst other measures, proposals to expand the regulatory reach of the European Electronic Communications Code (EECC) to a large number of players currently not in scope of regulation, including most if not all participants to the digital economy, whether they would operate public or private networks. Figure one highlights the sections of the ecosystem currently not in scope of the EECC that would fall under its regulatory mandate should such proposals be adopted. It should be noted that just because part of the digital economy doesn't fall under EECC supervision doesn't mean it isn't regulated by other regulatory frameworks.

Scope of current EECC scope and proposed expansion



The EC White Paper proposes to expand the regulatory reach of the EECC in three main ways:

- It proposes extending the regulation of public telecom to private networks and other digital economy services.
- It suggests establishing a formal resolution mechanism on interconnection disputes despite acknowledging that these are very rare.
- It suggests broadening the funding base of universal service funds to other parts of the digital ecosystem.

This would not only dramatically expand the number and nature of regulated entities and companies under the EECC's umbrella, it would also impose new regulatory burdens to those already regulated and all of the newly regulated entities. In particular, this would bring under the EECC scope the following:

- **Operators of private Electronic Communication Networks** who build networks for their own purposes but do not resell network services to third parties such as a global bank's intercompany network, or a video-streaming provider's datacentre-supported distribution network.
- **Providers of digital services**, who offer any sort of digital service (whether consumers directly pay for it or not) such as a rail company's website and application, aspects of a connected car service or a

videogame app. They are currently not covered by the EECC although they may be covered by other regulatory frameworks.

These newly in-scope entities would be subject to notification requirements, reporting obligations, interconnection obligations, network security obligations, lawful intercept obligations, data protection obligations, consumer protection obligations and supplier limitations amongst other things.

Further, all participants in the digital economy including enterprise and consumer end-users would be impacted through higher costs due to the additional costs for delivery of traffic due to the introduction of interconnection resolution mechanisms and the additional costs for use of online services (including cloud services) as the added cost of handling the regulatory burden would need to be reflected in price increases.

The justifications offered in the White Paper for these proposed regulatory changes are debatable at best:

- The White Paper assumes a convergence between cloud and telecom services that simply does not exist. Cloud technologies are horizontal and help streamline all industry sectors, not just telecoms. Implementing cloud solutions to telecom networks is no more a convergence between cloud and telecoms than implementing cloud solutions to banking is a convergence between cloud and banking;

- the White Paper argues that online services in general and cloud in particular are unregulated when they are in fact subject to a wide range of regulatory frameworks other than the EECC, such as the Digital Markets Act (DMA), the Digital Services Act (DSA), the EU Data Act, the Network & Information Systems Directive (NIS2), the European Cybersecurity Scheme for Cloud (EUCS) and many more;

- the White Paper affirms that there is an imbalance in regulation between telecoms and cloud when in fact the EECC's recently revised framework determines how Number Based Interpersonal Communication Services (NBICS) and Number Independent Interpersonal Communications Services (NIICS) are regulated to ensure no such imbalance. It fails to provide examples of such imbalances;

- the White Paper recognises that there are few interconnection disputes but nonetheless argues for a formal dispute resolution mechanism, which would enshrine the notion of paid interconnections as a norm as opposed to the current and effective norm of free peering;

- the White Paper argues for broader ecosystem contributions to Universal Service funding in order to meet the digital decade targets even though Universal Service is not currently used to fund network deployments and could not be reformed by the time these targets need to be met.

Implementation of the regulatory scope proposed in the White Paper would have massive and damaging impacts on the global electronic communications ecosystem in Europe.

By **significantly increasing the cost of being regulated**, it would create inflationary pressure on all of the ecosystem's participants from end users to enterprises to service providers. These cost increases would reverberate throughout the industry as price increases, slowing down adoption of technology solutions and generally increasing the cost of participation in the digital economy.

It would **generate further Internet fragmentation** by establishing a set of specific rules in Europe that would not only act as a deterrent for non-European companies to enter the market but could also lead to geo-political instability as Europe breaks off from the commonly agreed and effective network interactions mechanisms.

It would **hamper European innovation** as the cost of complying with regulation for start-ups and innovators degrades business models and deters investors. Furthermore, cutting-edge non-European technology would be slower to penetrate the European market as cost of doing business there would become less attractive.

Finally the proposals in the White Paper raise very concrete questions about the **ability of the EC and of National Regulatory Authorities to expand the scope of their regulatory activities** so widely. There are already pushbacks by EU governments asking for more time to implement the slew of recent new legislation touching on the digital economy, it is therefore doubtful that vastly expanding the scope of regulation to the entire Internet ecosystem is a workable proposition from that point of view either.

1 Introduction

On February 21st, 2024, the EC published a White Paper entitled "How to master Europe's digital infrastructure needs?" and issued a call for consultation for the end of June. While the document covers a broad range of topics and makes a number of specific proposals, it is also somewhat vague in its goals and the justifications for its proposed changes. Some of these changes, as currently written, would have enormous implications on the digital ecosystem with potentially damaging impacts. The present analysis attempts to clarify the meaning of these proposals and the potential impacts, were they to be implemented.

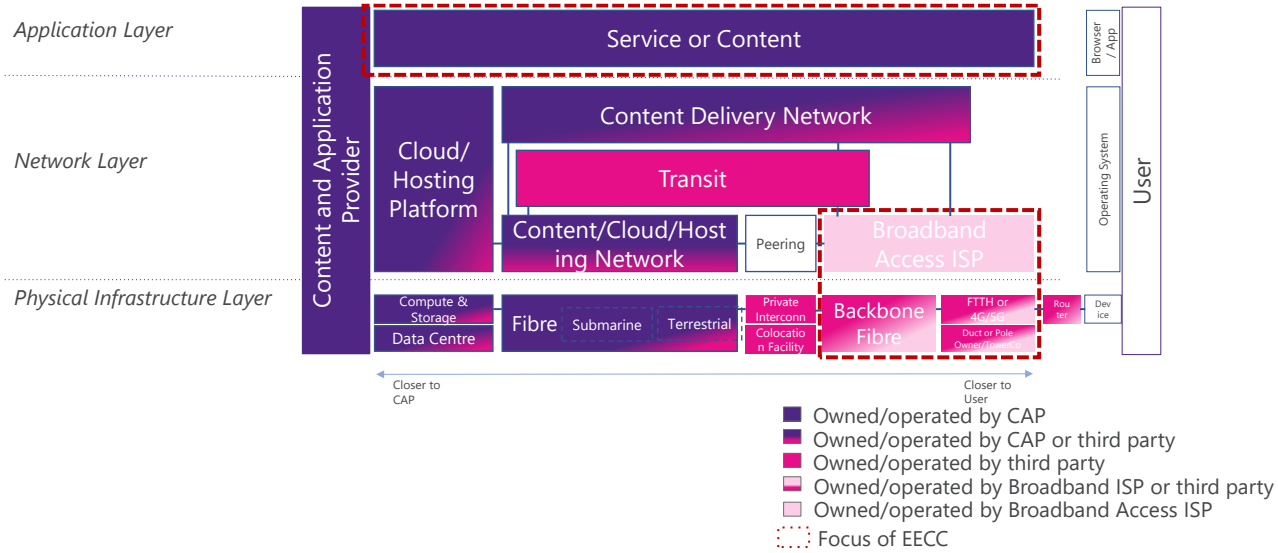
The methodology for this document was to analyse all aspects of the EC White Paper that may impact the broader digital economy, and particularly that may impact companies or entities currently not in scope of the European Electronic Communications Code. By necessity, Plum Consulting's analysis includes elements of interpretation since the White Paper's proposals were sometimes unspecific in their definitions and measures. When in doubt, our interpretation was as broad as possible to include all potential risks from such expanded regulatory measures.

This report has been funded by Google and supported by CCIA. All researchers are granted editorial independence.

2 How the internet works

Some of the comments and propositions in the European Commission (EC) White Paper seem to describe aspects of the Internet or make assumptions about the Internet that do not match reality. It seems therefore necessary to present at a very high level how the Internet works so as to clarify any such misrepresentations.

Figure 2.1: Internet ecosystem map and scope of current EECC regulation



The Internet is a collection of autonomous networks, that choose to interconnect with each other following certain standards to provide their customers with a global reach, general purpose "inter-network". It is based on layered principles where operations in higher layers are independent of lower layers. Protocols in each layer are generally based on open standards. The Internet is highly distributed in control and management, hence incredibly resilient and reliable.

The layered principle of the Internet supports open innovation, where any user anywhere can pay for a connection to any network connected to the rest of the Internet and begin accessing or offering services or content to anyone, anywhere, without requiring permission from, or payment to, any intermediate network.

In this respect the Internet is fundamentally different to centrally controlled vertically integrated services developed by telecom operators, which had a tight coupling between network and services - e.g. France's Minitel, or Prestel in the UK. Due to the gatekeeper role of the managing operator, the lack of flexibility and openness of these services meant they were unable to flourish, thrive and adapt, and these services did not survive contact with the white heat of innovation of the Open Internet.

The layers and elements that make up the Internet include, from the lowest layer:

- At the physical infrastructure layer are the servers, submarine cables, terrestrial fibre, Internet Exchange switches, Wi-Fi routers and mobile phone base stations - provisioned by European and non-European telecom operators, cloud or hosting providers, infrastructure investors, private network operators, or end-users.
  - This physical layer can include sub-layers - for example in a Fibre to the Home (FTTH) service, one company may own the duct to a property, another company may own the fibre that runs through the duct to the property, and a third company (the ISP) may provision services over the fibre. In a 4G

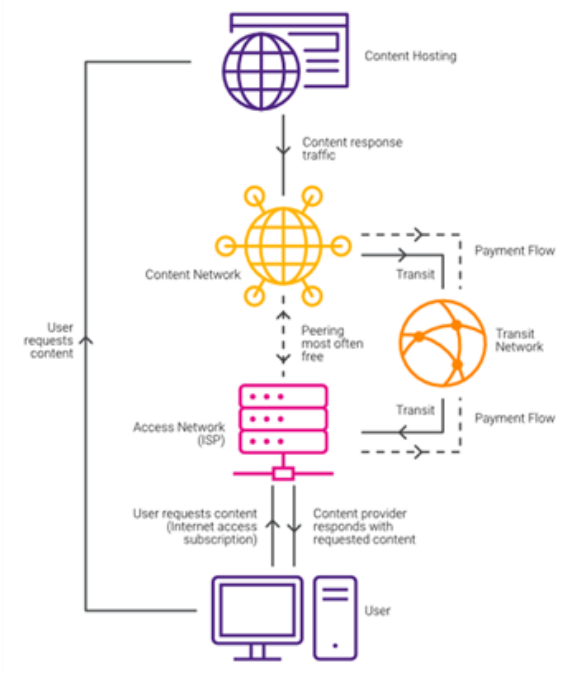
or 5G mobile service, one company may own a mobile tower, another owns the spectrum and antennae on the tower and the powered equipment that runs them, and a third company may provide service to users over the infrastructure.

- At the network layer, physical infrastructure is joined together, and using standardised protocols makes a coherent single network that is managed by a single entity. This can span an area ranging from a home or campus to a continent or more. A network offers connectivity for a set of users or systems connected to it.

For the purposes of enabling the Internet, networks are organised into "Autonomous Systems" (ASes), and it is these ASes choosing to interconnect with each other that enables a network to offer its users and customers connectivity to the whole Internet.

This interconnection is a layered system as well. A user will typically buy a connection to a single ISP. Effectively the user is buying a "transit" service - transit being "a connection to any other point on the Internet". For the user's ISP to be able to offer transit to users, they also need to buy transit from a wholesale network provider with a wider network reach. The ISP can also, if they wish, agree to "peering" with another network, which enables them and the other network to exchange traffic with each other without both having to go through their paid transit connections. This provides mutual benefits, saving both operators money and improving performance for both networks' users, so the vast majority of peering has traditionally been "settlement free". Through a mixture of peering and transit, ISPs and wholesale network providers can reach the whole Internet (Figure 2.2). There are a set of around a dozen wholesale network providers that have sufficient reach and widespread peering arrangements that they do not need to buy any transit at all to reach every point on the Internet - these are known as "Tier 1" providers[1].

Figure 2.2: Information flows on the Internet



On top of these various networks, Content Delivery Networks (CDNs) operate, which are virtualized networks that help to distribute popular content closer to where users are, to optimise delivery and improve performance for

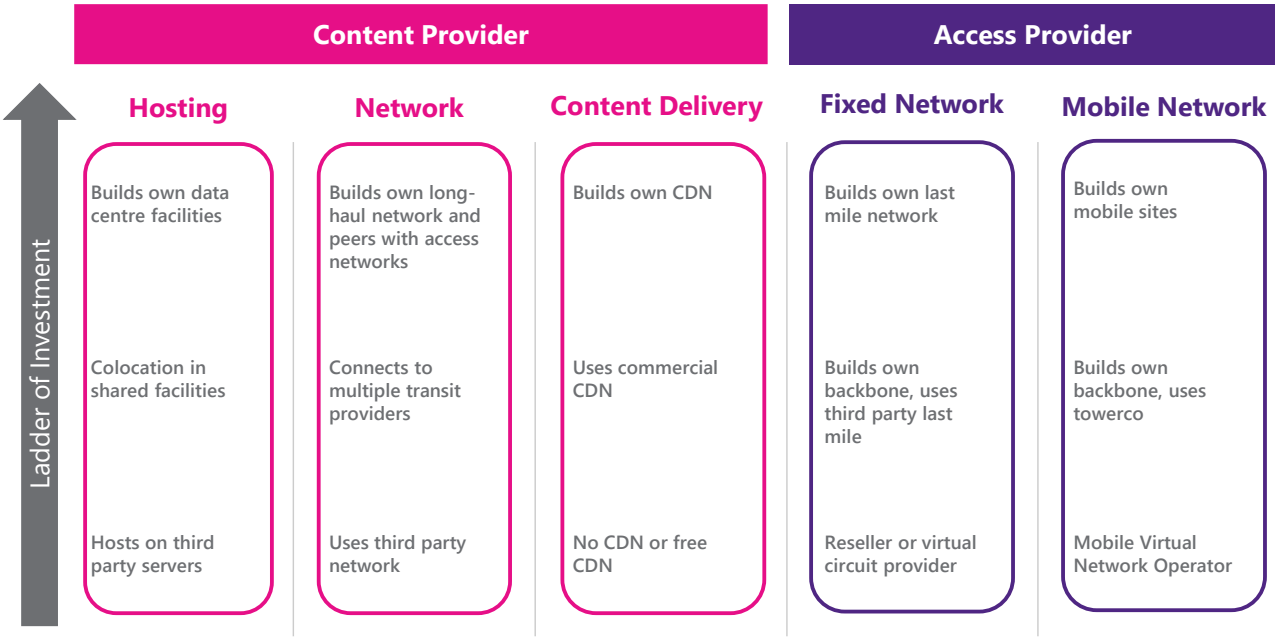
[1] https://en.wikipedia.org/wiki/Tier_1_network

users. If thousands of users are all watching the same streaming TV show, this can be delivered from CDN servers inside the ISPs network or another location closer to the users than delivering all the video streams from the central data centre. This provides efficiencies and cost savings for the content provider, intermediate networks and the broadband ISP.

At the application layer, due to the work of the network layer, services or content located at any point on the Internet can communicate with users anywhere else on the Internet. There can be multiple application layers - for example a HTTP (web) request may contain a higher-layer API request that lets you adjust the temperature on your Internet-connected thermostat from an app on your phone.

As can be seen from the above diagram (Figure 2.1), content providers can choose to buy services or build infrastructure for hosting and connectivity elements. Like access providers, content providers climb the "ladder of investment" (Figure 2.3) for hosting, connectivity, or CDN services, as their needs grow, capabilities expand, and they outgrow third party providers.

Figure 2.3: Ladder of investment for various digital economy components



The vast majority of this system is dynamic and highly competitive. The biggest bottleneck or gatekeeper risk typically occurs closest to the user, at the level of the Internet access service, where end-users can only reach content on the Internet through the providers of the 'last mile' access service. This is also where investment required to build a network is high, but where revenue is reliable and stable over a longer period of time. Users may only have a choice of one or a few ISPs, depending on how their telecoms market is structured and the infrastructure that is available where they are located. In addition (or perhaps because of this) users are also often locked into relatively long-term contracts with their ISP, not able to switch providers quickly if they encounter a problem, so a user is essentially "captive" to an ISP for the period of their contract. This is one reason why access ISPs, fixed and mobile, are subject to consumer protection and ex ante competition regulation such as in application of the European Electronic Communications Code (EECC)[2]. Other parts of the infrastructure close to

[2] E.g. "In addition to replacing and repealing existing legislation, the directive introduces a series of new objectives and tasks : Strengthened consumer rules aim to make it easier to switch between service providers and offer better protection, for example, for people who subscribe to bundled services. Consumers will benefit from a similar, higher level of protection across the EU.", summary of Directive (EU) 2018/1972

users may be subject to wholesale access regulation if they are found to hold Significant Market Power - for example on markets for access to ducts and poles, wholesale local access provided at a fixed location, and wholesale high quality access.

Thanks to competitive market conditions, other parts of the Internet infrastructure ecosystem are typically not actively regulated. Broadband ISPs will build their network to major cities where a number of wholesale network operators have Points of Presence (PoPs) in different carrier-neutral colocation and interconnection facilities, and when looking for transit, ISPs will typically have a wide choice of operators competing for their business.

ISPs can also choose to peer with other networks, especially if they connect to a local Internet Exchange Point (IXP), where a number of networks can come together to peer traffic with each other. Peering is a voluntary activity - as long as a network has a transit provider, they have a connection to every point on the Internet, so peering is simply a technical and commercial optimization. If a network does not wish to peer - and there may be valid commercial, technical, or legal reasons why not - as long as they have adequate transit capacity to serve their users with a high quality of experience, there is no reason why they need to.

The competitive environment is also strong for wholesale network operators, where they either build or buy trans-continental and intercontinental fibre routes of ever greater capacity, resulting in analysts such as Telegeography reporting[3] year-on-year falls in the cost per Megabit of capacity on every route since reporting began.

At the other end of the ecosystem, content and application providers may rely on a hosting or cloud provider's network for their needs, purchase transit, build their own network, or a mixture of the latter two. Even those who self-provision their network typically also purchase connections to multiple transit providers as well. The CAP may also build or buy CDN services to bring their content closer to users. A CAP will have multiple routes to deliver content demanded by an ISPs customers - either through a CDN, through direct peering, or through a number of different transit providers. Furthermore, content providers may offer services that are substitutable with just a click or a flick of a finger, so have a very strong incentive to provide the best quality of experience to users at all time - for example, if TikTok is working slowly today, users may switch over in one click / immediately to browsing Instagram. So, in contrast to regulation required at the "user" end of the Internet connection, where users are essentially captive to their ISP, regulation is not required at the "content" end.

establishing the European Electronic Communications Code (https://eur-lex.europa.eu/EN/legal-content/summary/european-electronic-communications-code.html)

[3] https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf

3 European Commission White Paper proposals

In its February 2024 White Paper "How to master Europe's digital infrastructure needs?", the European Commission (EC) pushes for broad changes in its regulatory framework that would impact the entire Internet ecosystem as described above. Most of these suggested changes are worded in vague terms, which leaves some space for interpretation. The incoming Commission will hopefully clarify its intentions and proposed regulatory changes, but in the meantime, it is important for all stakeholders involved to understand what effects the proposals as they currently stand may have on the Internet ecosystem.

In this section we will summarise the proposed changes that impact the Internet ecosystem directly, so that they are clearly laid out and can be analysed in the subsequent sections of the report.

The first and most significant proposal in the White Paper is for an extension of the scope of telecom (electronic communications) regulation to the Internet ecosystem. This is outlined in Scenario 4 of the White Paper:

> *Scenario 4: In order to address the converged electronic communications connectivity and services sector and to ensure that its benefits reach all end-users everywhere, the Commission may consider broadening the scope and objectives of the current regulatory framework to ensure a regulatory level playing field and equivalent rights and obligations for all actors and end-users of digital networks where appropriate to meet the corresponding regulatory objectives; given the likely global magnitude and impact of the technological developments and of any possible regulatory changes, a reform of the current framework needs to be properly assessed in terms of the economic impact on all actors as well as debated broadly with all stakeholders.*

The EC explains its thinking in sections 2.3.4 and 3.2.2 of the White Paper. It relies on the following arguments to justify the proposed extension of the regulatory scope. Note that few if any of these arguments are themselves backed by evidence at this stage of the EC's thinking:

- Digitisation of networks allegedly drives a convergence between what was previously considered telecom and what was considered cloud. The Commission anticipates that the future will see the emergence of a "*complex converged ecosystem*", thus arguing that the regulation currently applied to telecoms should apply to the entirety of the Internet ecosystem;

- The current EU regulatory framework for electronic communications networks, the EC further argues, "*does not establish obligations related to the activities of cloud providers and does not regulate the relationship between the various players in the new complex digital infrastructure ecosystem.*"

- In addition, the EC notes that "[Internet] *traffic transits mostly on private networks, which are largely unregulated, rather than on public ones*".

- Finally, the EC remarks that "*the electronic communications code applies most obligations to number-based interpersonal communications services, and few obligations are applied to number-independent interpersonal communications*".

While not explicitly mentioned in Scenario 4 (or indeed any other scenario), two additional points are made by the EC that seem to point at a willingness to extend the regulatory scope:

- Regarding Internet interconnection, the EC remarks in section of 3.2.2 that while there are "*very few known cases of intervention (…) into the contractual relationships between market actors (…) it cannot be excluded that the number of cases in the future will increase*". It concludes that "*policy measures could be envisaged*

to ensure swift resolution of disputes" and suggests that national regulatory authorities or BEREC could be solicited for arbitration in such disputes.

In sections 2.3.4 and 3.2.8, the EC notes that only electronic communications operators fund universal service, notably including number-based interpersonal communications services (NBICS). This hints at a possible broadening of funding to number-independent interpersonal communication services (NIICS) or even further to all digital services, which would potentially impact the whole Internet ecosystem.

4 The proposed changes would impact orders of magnitude more companies and massively increase the regulatory burden

In summary, there are two main axes to the proposed changes in the regulatory landscape introduced by the EC's White Paper:

- first, the Commission is proposing to expand the scope of regulatory oversight and obligations beyond the current providers of communication services to a whole range of industries who are currently not part of the EECC framework;

- second, the Commission suggests the possible introduction of new regulation on both interconnection and universal service funding.

In order to examine the potential impact of such changes on both industries currently regulated under EECC and those that aren't, it's important to describe, at least at a high level, the different types of services potentially subject to this regulatory expansion. A lot of the services we will discuss are currently identified by the EECC, but not subject to most regulatory obligations. There is significant debate and detail in law as to what constitutes an ECN and an ECS[4], also what constitutes a "public" ECN/S, so we will try to take a higher level approach for the purposes of this analysis:

- Operators of public networks are those who everyone has in mind when thinking of who the EECC currently regulates. These are telecom operators offering communication services to consumers or businesses as well as certain interpersonal communication application providers. These are clearly public Electronic Communication Services (ECS) – offered to the entire public or a significant proportion thereof, over public Electronic Communication Networks (ECNs). They are currently regulated on many aspects related to the provision of the services they offer. Examples: a mobile network operator, a wholesale fibre network, a "thick" MVNO, a messaging application. Regulators focus their attention on operators in this category.

- Operators of private Electronic Communication Networks are organisations who build networks for their own purposes. These networks do not sell network services to third parties. They are currently identified in the EECC, but not subject to most of its regulatory obligations, although this varies on a country-by-country basis. They are not typically the focus of regulators' attention. Examples: a global bank's intercompany network, a video-streaming provider's datacentre-supported distribution network.

- Providers of digital services are those who offer any sort of digital service (whether consumers directly pay for it or not). Within the full scope of EECC are only a few number-bound interpersonal communication services (NB-ICS, e.g. WhatsApp or SkypeOut) and number-independent interpersonal communication services (NI-ICS). Note that there is some degree of interpretation here and attempts by regulators to include more services in EECC have proceeded through the courts for years[5]. Some services have been ruled not to be constituting the provision of electronic communications services on the basis of the nature of the activity, or on the basis of the fact that the electronic communications service is provided by an underlying ECS provider and explicitly resold or made available as part of a marketplace. They are currently not covered by the EECC although they may be covered by other regulatory frameworks. Clear examples

[4] https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-general-authorization-and-related-frameworks-for-international-submarine-connectivity

[5] https://www.twobirds.com/en/insights/2019/global/the-gmail-judgment-of-the-court-of-justice

not currently in scope of EECC would include a rail company's website and application, aspects of a connected car service or a videogame app. It is worth noting that the "end-users" that the Commission may have in mind in its Scenario 4 of expanding EECC regulation could be referring to Content and Application Providers which are identified as "end users" in the Open Internet Regulation.

- Users of a digital or network service are enterprises or individuals who consume communication networks or services but don't offer, resell, distribute or operate them. This includes potentially everyone, and these end users are not currently under regulatory scrutiny as part of the EECC.

The obligations that apply under the EECC are as follows:

- Notification requirements: regulated entities must notify themselves with telecoms regulators in each EU Member State they operate in, and pay administrative fees to that regulator;
- Reporting obligations: regulated entities must report on an annual or quarterly basis to telecom regulators in each European they operate in on revenues, customer numbers, traffic, and other metrics;
- Interconnection obligations: regulated entities currently have the right to interconnect with other regulated entities, although these obligations are largely considered to apply to voice, not IP;
- Network security: regulated entities must report and subject themselves audits on their network security measures and incidents in each EU Member State they operate in;
- Lawful intercept: regulated entities must comply with lawful intercept requirements, requests and have data retention obligations where applicable;
- Data protection: regulated entities must comply with specific telecoms sector data protection and data retention requirements;
- Consumer protection: regulated entities must comply with telecoms sector specific obligations around customer contracts and consumer protection;
- Supplier limitations: while not in the EECC itself but in other pieces of regulation, regulated entities are imposed limitations on which suppliers they may use for national security reasons.

In addition to what is currently in the EECC, the White Paper implies the addition of the following obligations:

- Universal Service Funding: the White Paper implies the potential expansion of contributions to national universal service funds, making reference to the "European Declaration on Digital Rights and Principles for the Digital Decade"
- IP interconnection arbitration: the possible introduction of an arbitration mechanism for IP interconnect would effectively bring peering and transit under regulatory scrutiny.

These obligations may be enacted as a result of bringing other digital services into scope of EECC for the first time.

Figure 4.1: Matrix of regulatory scope and burden expansion in White Paper proposals

	Digital Infrastrusture Provider				Network or service provider			
	Cloud and Hosting Providers	Content Delivery Networks	Internet Exchange Points		Using a digital or network service	Providing a digital service	Operating a private network	Operating a public network
Obligations								
Notification requirements	●	●	●			●	●	●
Reporting obligations	●	●	●			●	●	●
Interconnection obligations	●	●	●			●	●	●
Network security	●	●	●			●	●	●
Lawful intercept	●	●	●			●	●	●
Data protection	●	●	●			●	●	●
Consumer protection						●	●	●
Supplier limitations	●	●	●			●	●	●
Universal Service Funding	●	●	●			●	●	●
IP interconnection arbitration	●	●	●			●	●	●
Further impacts								
Additional costs for delivery of traffic demanded by users	●	●			●	●	●	●
Additional costs for use of Cloud Services	●	●	●		●	●	●	●
Potential conflict with existing sector-specific EU legislation						●	●	
Potential conflict with existing EU horizontal digital legislation	●	●	●			●	●	

●: Currently the focus of EECC
●: New obligations and impacts as a results of proposals in White Paper

In addition to the direct impacts for digital service and infrastructure providers as the result of the changes proposed in the White Paper, there will be a range of further impacts that will fall on both industry and end-users, harming progress towards the Commission's Digital Decade targets. These include:

- **Additional costs for delivery of traffic demanded by users**: the interconnection dispute resolution regime may lead to "network usage fees", as telecom operators leverage their termination monopoly and seek dispute resolution to extract payments from CAPs for delivery of traffic demanded by users. This will apply not only to the largest CAPs but also Cloud providers hosting content for third parties, and IP transit providers attempting to deliver traffic from the rest of the Internet - ultimately the vast majority of the Internet ecosystem will be affected.

- **Additional costs for use of Cloud services**: in addition to additional costs for delivery of traffic from Cloud providers, the additional and potentially conflicting regulatory obligations on Cloud providers who operate their own networks will be passed back to Cloud customers. This will harm competitiveness for European firms using Cloud services, compared to those using Cloud services elsewhere. European firms may even seek to offshore their Cloud and hosting requirements outside Europe to avoid such additional costs, resulting in worse quality of experience for users accessing these services, and depressing demand for Cloud services hosted in Europe, contrary to Digital Decade Cloud adoption targets. Such impact has been documented in the case of South Korea, the only country to have implemented similar policies to those proposed by the EC[6].

- **Potential conflict with existing sector-specific EU legislation**: an increasing number of industries have seen significant new European legislation in the past few years regarding digital operations and services – for example the Digital Online Resilience Act for financial services. These acts may have provisions that conflict with those in EECC.

- **Potential conflict with existing EU horizontal digital legislation**: a raft of horizontal digital legislation has also been developed in the EC including GDPR, NIS2, AI Act, Cybersecurity Act, and so on, and imposing telecoms-specific regulation on top could conflict with these horizontal requirements. For

[6] https://ccianet.org/research/reports/myths-surrounding-network-usage-fees-south-korea/

example, security incident reporting was part of EECC and has subsequently been moved to NIS2 – untangling further conflicts and duplication is likely to be required if the Commission's proposals proceed.

The cumulative impact of these other issues may even result in new services deciding not to launch in Europe, and existing content and application providers deciding to exit the European market altogether, denying users the benefit of the latest innovative Internet services, leading to a fragmented Internet experience between regions, and depressing demand for next-generation broadband services contrary to the Commission's Digital Decade connectivity targets.

5 The EC's justifications for the proposals are debatable

As discussed above, the Commission lists many arguments in its White Paper to justify its proposed changes in regulation. Unfortunately, many of these arguments are, at best, not evidenced or justified, and in some cases are in contradiction of known market trends or documented facts. In this section we will explore these arguments in turn and assess their validity.

5.1 Supposed convergence of telecom and cloud

The White Paper discusses the cloudification of communication networks, without clearly defining this concept and what cloudification entails in this context.

The European Commission defines cloud computing as a key component of its IT strategy[7], emphasizing a "cloud-first" approach. The NIS2 Directive states that "*'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations*". [8] According to the EC cloud strategy, "*cloud computing" is an IT paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level IT services that can be dynamically provisioned with minimal management effort, usually over the Internet. Cloud computing relies on the sharing of resources to achieve coherence and economies of scale, similar to a public utility.*"[9] Another definition says that "'*Cloud computing' in simplified terms can be understood as the storing, processing and use of data on remotely located computers accessed over the Internet. This means that users can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can get to their data from anywhere with an Internet connection.*"[10]In a nutshell, cloudification represents the broad adoption of cloud services across various industries, a process integral to the ongoing digital transformation of the global economy. By moving data and applications to the cloud, businesses can reduce costs and increase operational efficiency, opening new opportunities. Recognized as a 'General Purpose Technology,' cloudification benefits all sectors, not just telecoms (where it enhances network management and service delivery). The cloud industry itself serves as a foundational layer, supplying its versatile services to vertical industries. A few examples include:

- In **finance services,** the use of cloud technology facilitates innovation and agility within the financial sector. It supports the deployment of modern IT architectures like microservices, AI, and blockchain, enabling institutions to quickly adapt to changes and roll out new services at reduced costs[11]. Cloud is especially useful for computationally intensive operations like risk management and liquidity simulations.[12]

- In the **energy sector**, cloud can be used to support energy generation, distribution as well as administration. Cloud enables predictive maintenance: using cloud-based asset management systems and machine learning algorithms, energy companies can monitor the health of equipment in real time. This helps predict when maintenance is needed, reducing downtime, and extending the lifespan of critical infrastructure.[13] Cloud platforms also facilitate the integration of various operational processes, allowing

[7] https://commission.europa.eu/publications/european-commission-cloud-strategy_en
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1714054562658#tocId82
[9] https://commission.europa.eu/document/download/3bb440ec-f777-484c-8802-baf08ebb87c0_en?filename=ec_cloud_strategy.pdf
[10] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
[11] https://www.globalbankingandfinance.com/why-2023-will-see-more-cloud-adoption-in-financial-services-not-less/
[12] https://kpmg.com/de/en/home/insights/2023/10/cloud-monitor-financial-services-2023.html
[13] https://www.contino.io/insights/cloud-energy-sector

for better data management and analytics. This helps energy companies optimises everything from resource allocation to energy production and distribution, ensuring they can quickly adapt to changes in demand or operational conditions.[14] Renewable energy integration[15] and regulatory compliance and sustainability[16] are other cloud services use cases of the energy sector.

- The **gaming industry** is another example of a cloud-services using sector. Services provided by cloud gaming platforms (e.g. Microsoft's xCloud, Sony's Playstation Plus) allow gamers to stream games directly from the cloud without needing high-end hardware. This has democratised access to high-quality gaming experiences, enabling users to play advanced games on less powerful devices such as smartphones and low-spec PCs. Gamers can access a broad library of games instantly and on multiple devices, which significantly enhances convenience and accessibility. This also benefits users who prefer not to invest in expensive gaming hardware.[17] Cloud gaming platforms often operate under a subscription model, much like how Netflix operates for movies. Gamers save on hardware and software expenses, while developers can cut down on distribution and production costs.[18] Also, with the advancement of 5G technology, cloud gaming is set to become even more seamless, reducing latency issues which are critical for a good gaming experience, and allowing high-quality graphics.[19]

The cloud technology shift started a few years ago[20]. As per the examples described above, it has fostered different industries to evolve and contributed to an unprecedented transformation of how data and content are delivered to the final user, whether in telecommunications or in energy, finance, and gaming for instance.

The White Paper proposes some significant regulatory changes by including cloud services in the ECN/S existing regulations. Nevertheless, when assessing whether ex ante regulatory obligations are justified within the EECC, the regulatory approach normally follows a specific process that includes the definition of a relevant market[21] and the assessment of significant market power on that market[22] (including the identification and assessment of market failure.). Thus identifying the market in which the issue may reside and defining the issue in clear and documented terms are key components of the philosophy of any regulatory approach. The White Paper does not explain how cloud services are part of the same relevant market as ECN/S.

The cloud market is a very diversified market, with a large variety of offers supplied by a large variety of suppliers and vendors.[23]

Besides new entrants, existing players are entering markets they didn't previously address, contributing to create a new paradigm of power relations between them: The EC claims there is "convergence" between telecom and cloud services, but in reality the overlap of one industry operating in the other is limited, and any such operations are not in themselves "convergence":

- On one side, traditional telecom operators providing network access have tried to expand their service offerings into cloud, building their own small-scale Cloud footprint, and offering cloud services, such as hosting, data storage, and computing power, to businesses and consumers. Orange Business

[14] https://www.accenture.com/us-en/insights/energy/cloud-imperative-energy
[15] https://ratedpower.com/blog/cloud-computing-renewable/
[16] https://ratedpower.com/blog/cloud-computing-renewable/
[17] https://www.datamation.com/cloud/cloud-gaming-market/
[18] https://www.datamation.com/cloud/cloud-gaming-market/
[19] https://yourstory.com/2022/09/cloud-technologies-revolutionising-indias-gaming-future
[20] https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications
[21] The European Electronic Communications Code framework was rightly constructed from robust identification of markets (e.g., SSNIP test).
[22] The European Commission has published guidelines on market analysis. Those subject to potential regulatory measures must be identified based on their market power in the European market.
[23] https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications

Services[24] offers public and private cloud, cloud hybrid and multi-cloud; and Virtual Data Centre, storage, back up, and monitoring are part of Telefonica cloud offer.[25] These have met with limited success, resulting in telecom operators increasingly partnering with pure-play Cloud operators in order to provide a full suite of services – see below.

- On the other side, a few online service providers (those with a sufficient investment capacity and appetite for entering entirely new lines of business) have attempted entering the telecommunications access network market, with limited success so far: Project *Loon*[26] by Google was discontinued and Meta closed its connectivity division last year.[27] Project Kuiper by Amazon is one of the only ongoing Internet access projects led by a Content and Application Provider branching out into the access market, awaiting commercial launch.[28] Projects have often taken the form of "test beds" or limited deployments, either in the provider's home US market (e.g. Google Fiber) or in developing countries (e.g. Google Station[29], also sunset). In particular, there is no scaled cloud provider active in consumer broadband services in Europe today.

Partnerships and joint ventures have been signed between telecommunication operators and cloud providers, with the objective to combine connectivity from telcos with cloud capabilities from cloud providers. These partnerships typically take one of two forms – firstly, partnering to move parts of a telecom operator's operations or network management to the cloud, secondly partnering for the telecom operator to offer cloud services from the cloud provider to the operator's enterprise customer base.

Examples of the first type of partnership include Deutsche Telekom with Google Cloud[30]and AWS[31], Orange with Google Cloud[32] Vodafone with Google Cloud[33] and Microsoft Azure[34], Telefonica with Google Cloud[35] and AWS[36]. Examples of the second type of partnership include Deutsche Telekom with Microsoft Azure[37], Orange with AWS[38] and Microsoft Azure[39], Vodafone with AWS[40], Telefonica with Microsoft Azure[41], and Telecom Italia with Google Cloud[42].

These limited attempts of telcos to enter the cloud market and of cloud providers to enter the access network market - whether they are successful or not – do not mean there is a convergence between both markets. If we may be allowed a slightly tongue in cheek comparison, the fact that Deutsche Telekom endeavoured to manage a set of German night clubs does not mean there is convergence between the telecom market and night club services[43]. The connectivity and Internet access markets and the cloud market remain different ones, with their

[24] https://cloud.orange-business.com/en/
[25] https://cybersecuritycloud.telefonicatech.com/en/solutions/cloud-telefonica
[26] Alphabet Inc. subsidiary working on providing *Internet* access to rural and remote areas through high-altitude balloons.
[27] https://techcrunch.com/2022/12/12/meta-unplugs-connectivity-division-home-of-satellite-and-drone-Internet-experiments/
[28] https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper
[29] https://en.wikipedia.org/wiki/Google_Station
[30] https://www.telekom.com/en/media/media-information/archive/telekom-and-google-expand-partnership-1010150
[31] https://aws.amazon.com/fr/blogs/industries/cloud-technology-empowers-deutsche-telekoms-fiber-optic-network/
[32] https://5glab.orange.com/en/orange-5g-lab-opens-its-doors-to-edge-computing-in-partnership-with-google-cloud/
[33] https://www.vodafone.com/news/technology/vodafone-cardinality-io-google-cloud-smarter-pan-european-network-performance-platform
[34] https://www.vodafone.com/news/corporate-and-financial/vodafone-microsoft-sign-10-year-strategic-partnership-generative-ai-digital-services-cloud
[35] https://telecomtalk.info/telefonica-partners-google-ericsson-move-5gcore-cloud/633559/
[36] https://www.telefonica.com/en/communication-room/press-room/telefonica-expands-its-strategic-collaboration-with-amazon-for-cloud-development-and-the-digital-home/
[37] https://news.microsoft.com/de-de/microsoft-deutsche-telekom-partnerschaft/
[38] https://www.orange-business.com/fr/partenaires/amazon-web-services-est-plateforme-cloud-plus-complete-et-adoptee-monde
[39] https://cloud.orange-business.com/nos-partenaires/partenaires-technologiques/microsoft/
[40] https://www.vodafone.co.uk/business/cloud-solutions/cloud-partners/aws
[41] https://www.telefonica.com/en/communication-room/press-room/telefonica-tech-partners-with-microsoft-to-provide-the-industrial-sector-with-private-5g-connectivity-and-on-premises-edge-computing/
[42] https://www.gruppotim.it/en/press-archive/corporate/2020/CS-TIM-Google-04-03-2020.html
[43] https://www.telekom.com/en/media/media-information/archive/electronic-beats-480654

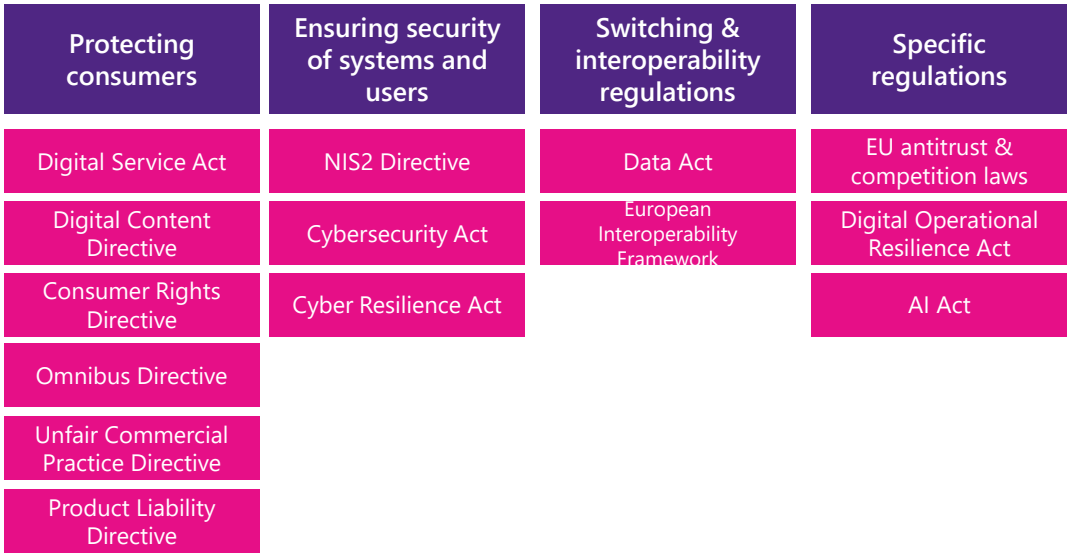
respective applicable regulations, and there is no so called "convergence" between these markets. While telecom operators' core business is to mainly provide connectivity services, the offering of cloud providers is that of computing resources for various sectors, providing multiple functionalities to their customers, such as computing, storage, machine learning and security services. Connectivity services and cloud services are not substitutes and answer different customer needs.

The activity of any existing or future access and electronic communication service is regulated by the provisions of the EECC, whether it is provided by an existing telecom operator or by an online service provider. In the same way, the activity of any existing or future cloud service is regulated by cloud regulations (see below), whether it is done by an online service provider or a telecom operator.

5.2 Supposed absence of regulation of cloud services

According to the White Paper, "*the existing EU regulatory framework for electronic communications networks and services does not establish obligations related to the activities of cloud providers*", which makes sense since, as demonstrated above, the cloud market is a market different from ECN/S. Nevertheless, a number of EU regulations do apply to cloud providers and include the following ones in the sub-section below, classified by regulation objective.

Figure 5.1: Existing regulations applying to cloud services



5.2.1 Protecting consumers

The following Regulations and directives collectively aim to protect European consumers, ensuring they have rights and remedies when engaging with products and services across the EU market, and apply to cloud providers:

- The **Digital Services Act (DSA)**[44] regulates, amongst other markets, that of cloud services by imposing obligations to ensure higher levels of transparency, accountability, and safety for users. Specifically, cloud service providers are required to implement robust systems to manage risks and prevent the

[44] Digital Services Act: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en; https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

dissemination of illegal content. They must also provide clear terms of service, mechanisms for users to report illegal content, and processes to appeal content moderation decisions. This regulatory framework aims to enhance user trust and safety in the digital space, aligning cloud services with broader EU standards for digital service providers.

- The **Digital Content Directive**[45] regulates transactions involving digital content and digital services to protect consumers. It governs digital content and services, including cloud-based software and storage. Cloud service providers must ensure their services meet the contract standards promised to consumers, such as uptime reliability, data integrity, and security. If the service fails to meet these standards, consumers are entitled to remedies such as repair, replacement, or even a refund.

- The **Consumer Rights Directive**[46] enhances consumer protections in relation to transparency and rights in sales contracts, particularly for online purchases. Cloud service providers must adhere to this directive by providing clear and comprehensible information about the terms of service, including pricing, cancellation rights, and the functionality of the services offered. This is particularly important for subscription-based cloud services, where consumers must understand what they are agreeing to and how they can cancel or switch services.

- The **Omnibus Directive** updates existing consumer protection laws to improve enforcement and modernize rules in line with digital market developments. Under this directive, cloud service providers are required to be more transparent about the algorithms used to determine what content or ads users see, especially if these influence transactions. They must also clearly state whether an online review is verified or if it could be manipulated. This is part of the broader requirement for transparency in online marketplaces, which can apply to cloud platforms that host third-party services.

Other consumer protection laws like the **Unfair Commercial Practice Directive**[47] and the **Product Liability Directive**[48] would apply to cloud services providers.

5.2.2 Ensuring security of systems and users

Other EU Regulations and directives contribute to protect the security of systems and users of cloud services, focusing on risk management, incident reporting, and ensuring that cybersecurity measures are an integral part of the service delivery and operational strategy. This unified approach is intended to bolster trust and security in cloud computing within the EU and benefit both providers and consumers.

- The **NIS2 Directive**[49] (Directive on measures for a high common level of cybersecurity across the Union) is an update of the original Network and Information Systems (NIS) Directive. It significantly broadens the scope of the original directive to include more sectors and types of companies, including medium and large companies in essential and important sectors. For cloud services, NIS2 requires providers to implement specific security measures and incident response strategies. Providers must also report significant cybersecurity incidents to national authorities, ensuring a higher level of cybersecurity preparedness and resilience.

- The **Cybersecurity Act**[50] establishes a comprehensive framework for cybersecurity certification of ICT products, services, and processes. For cloud technologies, it provides a mechanism through which cloud services can be certified for security compliance across the EU. This helps in standardizing the level of

[45] Digital Content Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770
[46] Consumer Rights Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083
[47] This directive prohibits misleading consumers about the features, capabilities, or benefits of a cloud service.
[48] If a cloud service integrates with or delivers physical products that are defective and cause harm, the directive could apply.
[49] NIS2: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[50] Cybersecurity Act: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

cybersecurity among providers and gives consumers a clear metric for assessing the security of cloud services. As part of the broader Cybersecurity Act, the European Cybersecurity Certification Framework for Cloud Services[51] (EUCS) aims to establish a unified certification framework for cloud services across the EU. This certification helps in verifying that cloud service providers meet EU-wide cybersecurity standards, offering assurances on data integrity, availability, and confidentiality. For cloud providers, achieving EUCS certification is an important feature to demonstrate compliance with stringent security requirements and to facilitate trust among users and within the market.

- The **Cyber Resilience Act** aims to ensure that products with digital elements, including cloud services, have built-in cybersecurity features from the design phase. For cloud providers, this means adhering to minimum cybersecurity requirements throughout the lifecycle of their service, from development to deployment and maintenance. The act will likely require cloud services to maintain systematic updates and patches, manage vulnerabilities effectively, and ensure robust defence mechanisms against cyber threats.

5.2.3 Switching and interoperability regulations

Interoperability and vendor switching has been tackled by the following regulations which apply to cloud providers:

- The **Data Act**[52] is designed to govern the use and accessibility of data across the EU. For cloud service providers, this act has significant implications, particularly in terms of data sharing and data portability. Providers are required to ensure that customers can easily switch between different cloud services and retrieve their data efficiently and securely. This may necessitate changes to the infrastructure and services to accommodate the seamless movement and integration of data across platforms. Additionally, the Data Act mandates transparency regarding data usage and gives users more control over their data, which cloud providers will need to ensure through clear policies and technical measures.

- The **European Interoperability Framework (EIF)** is designed to support digital cooperation among EU public administrations, ensuring that their digital services can interact with each other and with users across the EU. While it primarily targets public sector bodies, the principles of the EIF can indirectly affect cloud service providers, especially those working with public sector clients. The framework encourages the use of open standards and interoperable systems, which can influence how cloud services are designed and offered, to ensure they can seamlessly integrate with various public services. For cloud providers, adapting to these interoperability standards is crucial when aiming to provide services that need to interface with government digital systems efficiently. Although the EIF doesn't impose direct obligations on cloud service providers like other regulations might, its principles can guide how cloud services should be structured to facilitate better interaction with public services, aligning with broader EU goals of digital cohesion and efficiency.

5.2.4 Specific regulations

On top of the previously listed regulations and directives, some specific regulations place distinct demands on cloud service providers, ranging from maintaining competitive practices and operational resilience to ensuring that the deployment of AI systems complies with new EU standards.

[51] EUCS: https://ec.europa.eu/newsroom/cipr/items/713799/en
[52] Data Act: https://digital-strategy.ec.europa.eu/en/policies/data-act; https://www.datacenterdynamics.com/en/news/eu-cloud-companies-required-to-facilitate-provider-switching-by-data-act/

- The **EU traditional antitrust and competition laws**[53] aim to prevent anti-competitive practices and ensure fair competition within the internal market. For cloud providers, antitrust laws are particularly relevant in cases of dominant market positions or anti-competitive behaviour such as price fixing, restrictive practices, or unfair exclusionary tactics. The European Commission scrutinizes mergers, acquisitions, and partnerships involving major cloud providers to avoid excessive market concentration that could harm consumers. Additionally, antitrust laws regulate how cloud providers interact with competitors and clients, ensuring that no company unfairly restricts the market to prevent new entrants or innovation.

- The **Digital Operational Resilience Act (DORA)** specifically targets the financial sector but has implications for cloud service providers that offer services to financial institutions. This act requires providers to ensure a high level of security and operational resilience, focusing on the ability to withstand, respond to, and recover from ICT-related disruptions and threats. Cloud providers must meet rigorous standards for incident reporting, testing, and information sharing. They need to demonstrate that their infrastructures can handle threats and that they can maintain continuity of services under adverse conditions. For cloud services used by financial entities, compliance with DORA is crucial as it directly affects their ability to operate within the EU's regulatory framework for financial services.

- As AI technologies increasingly rely on cloud-based platforms for deployment and operation, the **AI Act**[54] will also impact cloud providers by setting standards for AI systems used within the EU, including those deployed on cloud platforms. It categorizes AI systems based on their risk level and imposes stricter requirements for high-risk applications, such as those involving biometric identification, critical infrastructure, or employment. Cloud providers must ensure that their platforms can support compliance with these regulations, including data governance, transparency, and ensuring that AI systems do not result in discriminatory outcomes. This might involve implementing specific controls, providing detailed documentation, or ensuring that AI systems running on their infrastructure are capable of being audited for compliance.

5.3 Supposed imbalance in cloud vs. telecom regulation

In a section named "convergence and level playing field", the White Paper implies that there is a different treatment between "electronic communications networks and services" and the "activities of cloud providers": "*Even if cloud providers run large (backbone) electronic communications networks, these networks are exempt from parts of the electronic communications regulatory framework, notably in the area of access regulation and dispute resolution.*"

The Commission does not identify examples of such regulatory imbalance. The most common examples used by operators making these same arguments revolve around perceived differences in treatment between Number Based Interpersonal Communication Services (NBICS) and Number Independent Interpersonal Communications Services (NIICS). And indeed there are obligations associated with the numbering system that weigh specifically on services that rely on or interact with the numbering system. But this is not a difference in treatment between functionally identical services: it is because the services are not functionally identical that they are regulated differently. In addition, the 2020 edition of the EC Recommendation on Relevant Markets Susceptible to Ex-Ante Regulation does not identify any retail or wholesale interpersonal communications services as meriting specific attention in terms of risks to competition. In fact, those markets were removed many years ago, on account of markets having trended towards effective competition. The 2020 edition of the Recommendation identifies only 2 markets: wholesale local access provided at a fixed location, and wholesale high quality access. These are 'hard access network markets, on which telecom operators are active, and from which cloud providers are absent, as is

[53] Antitrust and competition laws: https://competition-policy.ec.europa.eu/antitrust-and-cartels_en

[54] The EU Artificial Intelligence Act was proposed by the European Commission on 21 April 2021, itw as adopted by the European Parliament on March 13, 2024 ; it was voted by the Council of Europe on 21 May 2024.

evidenced by the market analysis decisions taken by National Regulatory Authorities throughout the EU, and validated by the European Commission's decisional practice in assessing notifications by National Regulatory Authorities made in application of Article 32 of the EECC. It should be noted that these are not old decisions, but ones that have only very recently been introduced in the latest iteration of the EECC. These arguments in the White Paper seem to contradict these recent decisions by the EC, at a time when some European countries still haven't had time to fully implement the EECC.

Plum Consulting has not found other documented cases of functionally identical services that would carry a different regulatory burden depending on whether a market participant is regulated by the EECC framework or not. Furthermore, should there be circumstances where such imbalance existed, the Commission in its White Paper seems to take the position that such regulation should be aligned on the basis of the most regulated service rather than the least regulated. This position does not seem to be consistent with the Commission's stated goal to reduce the regulatory burden.

It is worth noting also that a large part of the burden of regulation is tied to the lack of harmonised implementation in Europe: on many regulatory obligations, the rules for the same family of obligations are different in each European country, such as on the processes for lawful intercept, the obligations and durations for data retention, etc.

In summary, not only is it difficult to pinpoint the mentioned regulatory imbalance, but should there be imbalances, they should be addressed by lessening regulation rather than increasing them for all.

5.4 Expected increase in interconnection dispute frequency

The EC White Paper points out that "in contrast to voice traffic (which is billed according to the "calling party's network pays" principle), IP interconnection currently appears to rely on transit and peering agreements". It acknowledges that this is guided by a "very direct and cooperative interaction between CAPs and ISPs as they have to agree on technical and commercial conditions for transit and peering bilaterally". In this context, the White Paper acknowledges that interconnection "generally functions well", but speculates disputes are likely to become more frequent, hence the need for implementation of an arbitration mechanism.

This speculation is not backed by any analysis that would suggest such a development is likely, and the proposal of a dispute resolution mechanisms for interconnection is simply repeating what large European incumbent telecom operators asked for in the Commission's 2023 "Exploratory Consultation", for example from Telefonica[55]. In fact, as was pointed out by the vast majority of other stakeholders who responded to that consultation, there is no market failure or issues with the way IP interconnection is happening that would justify such intervention. This feedback came from stakeholders as broad as BEREC[56], governments[57], consumers associations[58], Internet infrastructure operators[59], mobile virtual network operators[60], broadcasters[61], Internet infrastructure experts[62], civil society[63], the gaming industry[64], and more.

[55] https://www.telefonica.com/en/wp-content/uploads/sites/4/2023/05/Contribution-to-Exploratory-Consultation-Telefonica.pdf
[56] https://www.berec.europa.eu/en/document-categories/berec/others/berec-input-to-the-ecs-exploratory-consultation-on-the-future-of-the-electronics-communications-sector-and-its-infrastructure
[57] https://www.tweedekamer.nl/downloads/document?id=2023D26941
[58] https://www.euroconsumers.org/wp-content/uploads/2023/09/The_Future_of_Connectivity_-_euroconsumers.pdf
[59] https://www.euro-ix.net/media/filer_public/c7/72/c772acf6-b286-4edb-a3c5-042090e513df/spnp_impact_on_ixps_-_signed.pdf
[60] http://mvnoeurope.eu/mvno-europe-position-paper-on-network-investment-contributions/
[61] https://www.acte.be/publication/tv-vod-statement-on-network-fees/
[62] https://datatracker.ietf.org/doc/statement-iab-response-to-the-european-commissions-exploratory-consultation-on-the-future-of-the-electronic-communications-sector-and-its-infrastructure/00/pdf/
[63] https://epicenter.works/sites/default/files/2022_06-nn-open_letter_cso_0.pdf
[64] https://www.egdf.eu/egdf-opposes-network-fees/

Furthermore, by proposing the introduction of an arbitration mechanism, the Commission seems to assume that despite the fact that peering interconnection, for the most part, is free of charge[65], that should not be the norm. It should be noted that paid peering between operators and content and application providers happens nearly exclusively in the case of incumbent telecommunications operators and always to the benefit of said incumbents. This occurs as a result of the access operator limiting alternative routes to reach their customers who are demanding content, such that a CAP has no option other than to negotiate directly with the access provider or users will suffer with a poor quality of experience for that CAP's services.

While there may be exceptional circumstances in which paid peering is a suitable mutually beneficial solution that may be the optimal outcome of a commercial negotiation, in the most part, the norm is rather for free peering[66], and that paid peering is a form of abuse of dominant position by some of said incumbents who operate their networks in this way. In which case, again, introducing an arbitration mechanism for peering would result in normalising an abuse of dominant position.

5.5 Funding sources for universal service funds

The EC White Paper advocates that since broadband benefits every participant in the digital market, its universal service should consequently be funded by all these participants. This approach promotes a shared responsibility, reflecting the widespread advantages conferred by broadband access.

While seemingly rational on paper, this position omits two important elements of the way the Universal Service Directive and the EECC which replaced it set out Universal Service mechanisms:

- Firstly, universal service funds in Europe are not mandatory for Member States in application of the EECC (in fact, findings that there is no need for funding, or that small scale state funding is more appropriate than instituting a complex industry funding arrangement, is, prevalent in EU Member States). The EECC states that "a fundamental requirement of universal service is to ensure that all consumers have access at an affordable price to an available adequate broadband Internet access and voice communications services, at a fixed location. Member States should also have the possibility to ensure affordability of adequate broadband Internet access and voice communications services other than at a fixed location to citizens on the move, where they consider that this is necessary to ensure consumers' full social and economic participation in society. "Where Member States decide to designate a Universal Service Provider (USP), the EECC requires assessment on whether providing Universal Service represents an unfair burden on the designated provider. In several Member States, this test has not been passed (a hotly disputed matter, including in the courts). Where Universal Service funding is done by actually compensating operators designated with a universal service mandate, the amounts are minor, and an industry funding mechanism can apply (qualification for payment and the amounts of payment are a hotly disputed matter, including in the courts).

- Secondly, while universal service has an availability component to it, that does not mean that very high-capacity networks are deployed through universal service contributions. These may in some cases pay for the cost to install a broadband solution to a particular eligible home, but do not pay for the deployment of an entire network in a white area. There are other, much larger, national and European funds to do this.

There is a logic to these purposes of universal service being funded, where applicable, by the telecom industry since the designated providers are required to offer discounted tariffs to disenfranchised populations, and they are being compensated for taking on that responsibility. Similarly, financing the individual connection of eligible

[65] https://www.ripe.net/participate/forms/uploads/fobi_plugins/file/menog-22/LT-PCH-Peering_Survey-Sara%20_793f532a-148a-47fe-97cd-411ee94c43d0.pdf
[66] BEREC Report on IP-Interconnection practices in the Context of Net Neutrality, 2017

homes will generate revenues for the universal service operator at the retail or wholesale level, and it makes sense that those operating in the telecoms field should fund that (they will benefit from that wholesale connection also).

If universal service for broadband is funded as proposed in the White Paper, telecom operators designated as USPs would directly benefit through compensated revenue losses, generated revenues and asset accrual, whereas other digital market participants would see only indirect financial benefits, if any, through expected increased digital participation. This disparity highlights the varying impact of such funding on different stakeholders within the ecosystem.

Changing the universal service regime would likely be a complex legislative endeavour which, considering the different views amongst member states may well take years, by which time the digital target goals will have been met and the availability angle of universal service would largely have become moot. It is certainly very unlikely to be a tool to deliver these targets.

Finally, it should be noted that several European countries are transitioning away from universal service entirely. This shift raises questions about its continued effectiveness in the rapidly evolving EU market. Nations like France, Sweden, and Denmark no longer have a universal service fund. The affordability and availability missions previously under universal service are now handled either through dedicated mechanisms such the Cohésion Numérique des Territoires[67] scheme in France or through social security, as in Sweden. Subsidised broadband deployment is funded through state funds dedicated for this purpose.

[67] https://www.economie.gouv.fr/particuliers/cohesion-numerique-territoires-aide-linstallation-haut-debit#

6 Significant impact of proposed regulatory changes

The changes proposed in the EC's White Paper could have massive impacts on consumers, innovation, and the broader Internet ecosystem. In this section we outline the key impacts of these proposals.

6.1 Cost of regulation

The costs of regulation are both direct and indirect. The European Commission commissioned a study related to this "Assessing the Costs and Benefits of Regulation" (2013) which details the categories of costs that derive from new regulation. These proposals will result in both direct and indirect costs.

Direct costs in the context of these proposals by the Commission include:

- Compliance costs, including:
  - Charges – payments to regulators for universal service funding, forced interconnection payments from CAPs to telecom operators
  - Substantive compliance costs – filing returns, training staff to understand and comply with the regulations, capex and opex related to e.g. new legal intercept systems,
- "Hassle" or "irritation" costs – these include slower pace of innovation, the opportunity cost of waiting time when dealing with administrative or litigation issues, and so on.

Indirect costs include changes in the prices of goods or services in the regulated sector. Changes in these prices then ripple through the rest of the economy, causing other prices to rise or fall and ultimately affecting the welfare of consumers. In the case of the proposed regulation, this will result in higher prices for Cloud services for European industry, higher prices for delivery of Internet traffic demanded by users more broadly (passed on in higher subscription fees for digital services, or higher digital advertising costs for European businesses), lower take-up of Cloud services, and lower take-up of next-generation broadband services.

Other indirect costs, also known as "secondary costs", include

- Substitution effects – customers may choose Cloud platforms located outside of Europe to avoid the regulatory costs of operating within the region
- Transaction costs – the significantly increased cost of negotiating interconnection agreements with forced dispute resolution will introduce significant inefficiencies in the Internet ecosystem, making it more fragile and brittle
- Reduced competition and inefficient resource allocation – raising barriers to entry, making it harder for startups and innovative new services to compete with those who are established within the regulatory system
- Reduced market access – with CAPs potentially withdrawing from Europe to avoid regulation

- Uncertainty and investment – a challenging regulatory regime will discourage new digital investment in Europe, harming progress towards the digitization of the European economy.

6.2 Further fragmentation of the Internet ecosystem

Europe already has issues with fragmentation of the global Internet, or creation of a "splinternet," due to regulatory costs and barriers that discourage content providers from providing services to European users. For example, a number of American press outlets geo-blocked service to European users in 2018 as a result of the GDPR legislation, and even those that later were able to comply with GDPR and restored access, suffered a long-term loss in European visitors[68]. There remain a number of US press outlets who do not offer their content to European Internet users.

The Commission's significant expansion of telecoms regulation to a much wider range of digital services could have a similarly broad detrimental effect. Furthermore, if similarly to GDPR, the Commission deems any digital service accessed by a user in Europe to be in scope of the expanded EECC (regardless of where that service is located) then there is likely to be a similar set of geographic restrictions imposed again restricting access for European users, this time potentially on a much wider range of digital services than were affected by GDPR.

In addition, the specific proposal around forced interconnection dispute resolution may result in CAPs withdrawing from serving users on specific ISPs, rather than pay a mandated "network fee". It is unclear how the Commission or regulators can "force" a CAP to make payments to a counterparty for interconnection, if that CAP does not want to interconnect due to the terms that are being proposed by the counterparty. Examples from the news industry, where media firms have successfully lobbied for forced remuneration from Internet companies, shows harm to users and ultimately loss of revenue to the media companies concerned as digital services withdraw from the countries concerned[69].

6.3 Impact on startups and innovation

There has been no impact assessment for the proposed regulatory measures outlined in the White Paper. One thing that an impact assessment would undoubtedly highlight is that while the increased burden of regulation would have an impact for large established businesses, they could likely bear that burden or afford to exit the European market entirely. Not so with smaller European companies and start-ups: they would have neither the financial means nor the knowledge, time and skills to be able to comply with a high burden of new regulation.

This would have a deleterious effect on European innovation on several levels:

- European start-ups would struggle to meet with their regulatory obligations from their inception, especially those whose business models depend on operator across the whole of the EU from day one;

- Non-European start-ups would de-prioritise Europe as a core launch market due to the cost of handling regulatory constraints;

- Investors would exercise extra-caution when considering investing in European start-ups as the regulatory burden and associated risks might tarnish the perspectives of the companies they were looking to invest in. As a consequence funding of European innovation would become more complicated;

- Technology companies offering foundational "building block" type technologies would potentially shy away from serving the European market, causing cost increases for startups and others seeking to access

[68] https://reutersinstitute.politics.ox.ac.uk/news/many-eu-visitors-shut-out-us-sites-response-gdpr-never-came-back
[69] https://www.techdirt.com/2024/05/09/link-taxes-backfire-canadian-news-outlets-lose-out-meta-unscathed/

these new technologies, (due to lower competition) or even a gradual lag in adoption of new technology adoption as the most dynamic of these innovators turn away from Europe to avoid compliance of what they might perceive as excessive regulation.

These are only a few of the potentially negative impacts on start-ups and innovation in Europe. It would be ironic that proposals included in a White Paper that professes to promote European innovation would have the opposite effect.

6.4 Capability of EU to regulate and harmonisation issues

The existing EECC already has resulted in significant differences across Europe in terms of transposition into national law, implementation and enforcement by national regulatory authorities. Unless these differences are addressed, expanding the scope of EECC significantly will magnify these issues further, creating an unworkable patchwork of regulation across Europe for anyone operating a digital service. Far from creating the "digital single market" that the Commission would like, it will create a highly fragmented regulatory landscape across different countries of the EU.

In the case of forced dispute resolution, the Commission suggests that NRAs or BEREC could be the arbitration authority for IP interconnection disputes. Given that BEREC and NRAs have been clear that they do not consider IP interconnection to be a market that requires regulatory intervention, and that indeed such a measure is counterproductive to the good functioning of the Internet ecosystem, it is unclear how such arbitration will proceed. Furthermore, introducing national arbitration in interconnection would undoubtedly lead to "forum shopping", as favourable rulings in one country would encourage networks to interconnect where it is most favourable to them rather than where it makes technical sense in order to most efficiently deliver traffic.

Finally, it should be noted that EU Telecom ministers themselves have stressed as recently as May 2024 in the conclusions their "Future of EU Digital Policy Council" that they need time to absorb the series of recent new piece of digital economy policies. Ministers from the 27 countries noted the significant number of EU legislative acts that have been adopted in recent years, and stressed the "need to prioritise in the coming years their effective and efficient implementation." Error! Reference source not found. lists the breadth of regulatory measures targeting the digital sector.

Even putting aside the above, there is a very real question about the ability of regulators to suddenly absorb and handle a much-increased scope of regulation. Most European regulators currently focus their activities on a number of market participants in the hundreds, low thousands at most. For the sake of comparison, there are around 207,000 e-commerce websites[70] in France alone, and that is before considering non-ecommerce sites, and non-French websites that may be accessed inside France. It is unclear how a telecom regulator could manage such a large increase in regulated entities.

[70] https://www.statista.com/statistics/382964/number-of-active-e-commerce-websites-in-france/

7 Conclusions

The EC would likely argue (and has publicly done so) that the contents of the White Paper are only proposals, or even just 'scenarios', and that it is open to feedback from industry to assess the relevance and feasibility of its suggestions. However, its publication coincided with a context of European elections and appointments in the fall for an incoming new commission.

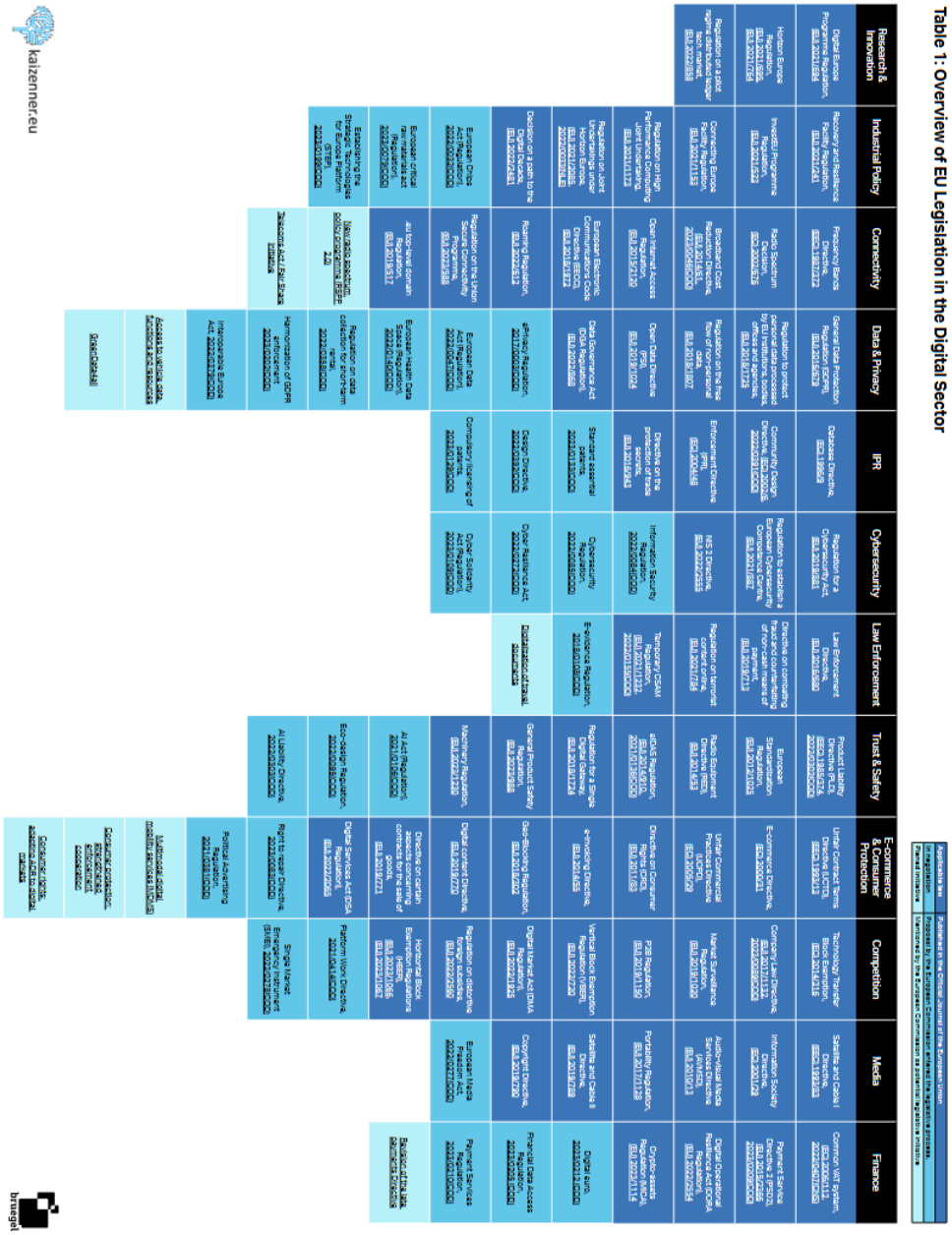
The White Paper is not simply a collection of regulatory scenarios, it attempts to outline a vision for the future of the digital economy in Europe. Its regulatory proposals are very much a tool to make that vision into a reality. It is, in many ways, an exercise in industrial policy rather than regulation. It is very important for participants in the digital economy to recognise it as such, because its very nature makes it broad both in its proposed measures and in its likely impact, should these be implemented.

If the White Paper is, as it seems to be, a blueprint from the current Commission to the future Commission, then it will be incumbent upon the future Commission to assess not just its proposals, but its premises and its impacts. There are at least three questions which the White Paper does not assess that the incoming commission should focus on before even considering the proposals it contains:

- Is the industrial vision that the White Paper outlines the right one for Europe?
- Is regulation the way to shape that industrial vision?
- How can the balance of costs and benefits of regulatory intervention be maintained to avoid harm to all or part of the ecosystem?

In this complicated and uncertain context, it is crucial that the various parties impacted by these proposals make their voice heard to highlight the significant risks and potentially damaging impacts that many of these proposals represent for consumers, businesses, digital start-ups, content providers, digital infrastructure providers, operators and more.

Appendix A Overview of EU legislation in the digital sector[71]



[71] Source: https://www.bruegel.org/sites/default/files/2023-07/Tables_Scott_Kai.pdf