February 2024

Helping Europe's digital economy take off

An agenda for the next Commission

By Zach Meyers

CENTRE FOR EUROPEAN REFORM
LONDON ★ BRUSSELS ★ BERLIN

Helping Europe's digital economy take off:

An agenda for the next Commission

By Zach Meyers

★ The EU has huge potential to unlock a thriving digital economy. Since the pandemic, the number of successful European start-ups has grown rapidly, European businesses are increasingly adopting new technologies, and Europe is catching up with the US in deploying digital infrastructure.

★ But there remain significant weaknesses that need to be urgently addressed to capitalise on these promising signs. European start-ups are growing in number – but they still struggle to scale up in Europe. Smaller businesses are falling behind in digitalisation. The EU's efforts to build a data economy are not yet delivering results. And there remain large gaps in Europe's digital infrastructure.

★ As the EU heads to the polls in June, the next European Commission must tackle these challenges to help Europe's digital economy take off. Some of the solutions, like building digital skills in Europe and developing an EU-wide capital market, will take time to achieve results. But the Commission should take several steps to accelerate digital growth.

★ First, after the recent swathe of digital laws addressing everything from artificial intelligence to digital competition to chips manufacturing, the next Commission's focus should be on ensuring these laws are properly implemented and enforced. To ensure that regulation does not overwhelm firms' and regulators' resources and detract from business efforts to adapt to and incorporate new technologies, the Commission should ensure recent digital laws form a predictable, coherent rulebook which is applied consistently across the EU, and which is future-proofed, principles-based and proportionate. The Commission should ensure tech laws build on the EU's strengths: its single market and open trading links with the rest of the world.

★ Second, the current Commission has understood that European firms have a huge, and mostly untapped, opportunity to exploit data in a privacy-friendly way. But the Commission's many efforts to help firms exploit non-personal data have not yet delivered results. A significant problem is that firms often cannot easily isolate non-personal data from personal data. Regulators have not done enough to help firms understand how to commercialise data without harming individuals' fundamental rights. The Commission should also pursue targeted improvements to the EU's General Data Protection Regulation (GDPR) to ensure it is applied consistently and proportionately across the EU.

★ Third, the EU needs to boost investment in connectivity and digital infrastructure. Without sufficient resilient infrastructure, European customers will not be able to take advantage of new innovations, and European tech firms will not see local demand for their services. Member-states must do a better job of removing regulatory barriers to infrastructure deployment across Europe and support a true single market for telecoms.

Despite its current lack of tech giants, the EU has huge potential to unlock a thriving digital economy. Contrary to frequent complaints that Europe is insufficiently entrepreneurial, the number of EU-based start-ups is growing significantly – even outpacing the US by some measures.

For example, the number of founders starting new tech start-ups in Europe exceeds the number in the US,[1] and Europe's total number of 'unicorns', or start-ups valued above $1 billion, has grown 88 per cent since 2014 – larger than the US' growth of 56 per cent over the same time period.[2] The EU's low-cost education and social welfare policies are potentially significant advantages. They provide European workers with good opportunities to build digital skills and mean entrepreneurs can rely on a social 'safety net' – which should allow them to take more risks. Europe also has some leading researchers in a number of emerging technologies. It has introduced regulatory tools to help businesses get access to more public and private sector data – which is essential for new technologies like AI and machine-learning. And despite the common complaint that European industries and consumers are slow to adopt new technologies, some figures tell a different story. Since the Covid pandemic, EU firms have begun rapidly integrating more technologies into their business practices.[3]

"The number of EU-based start-ups is growing significantly. But this has not yet translated into many successful tech firms on the global level, or even EU-wide."

The challenge for the next European Commission is how to capitalise on these promising signs. They have not yet translated into Europe creating many successful tech firms on the global level, or even EU-wide. Start-ups with promising ideas struggle to implement, commercialise and scale up their ideas in Europe. Too many European start-ups move to the US or face little choice but to be acquired by US firms when their ideas take off. US start-ups remain far more likely to grow and succeed than European ones. According to the Commission, the EU's share of the global ICT market has fallen from 21.8 per cent in 2013 to 11.3 per cent in 2022.[4] And there are still huge gaps in the EU's digital infrastructure, particularly in rural parts of the EU which have the most to gain from being better connected.

Similarly, while EU firms might be adopting new technologies to improve their productivity, much of this digitalisation is occurring in larger firms.

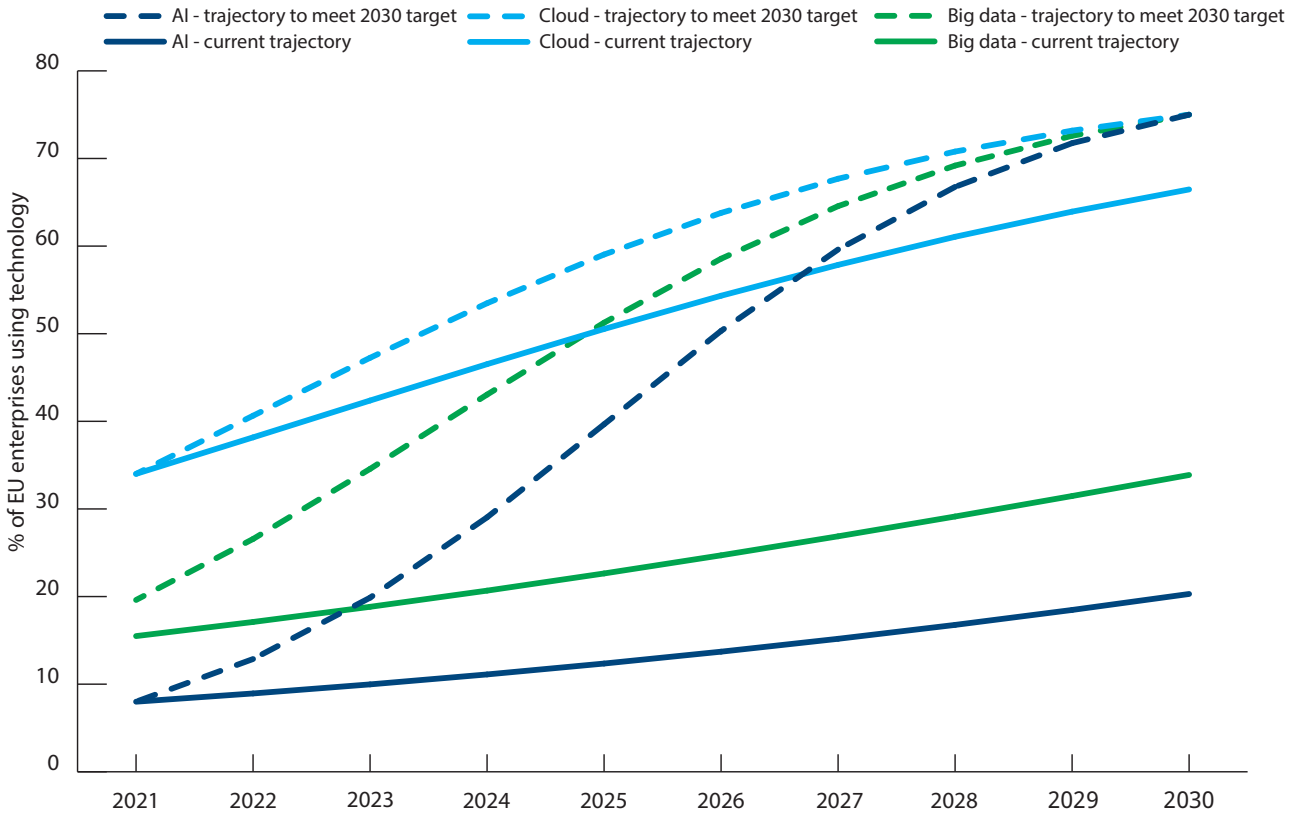
Smaller businesses – which can often offer more productivity-enhancing disruption – are much less likely to adopt digital technologies.[5] And although the EU is approaching US levels of digitalisation, in some technologies EU firms still have significant room to improve. As Chart 1 (on the next page) shows, based on their historic trajectory, EU enterprises should come close to reaching the EU's 2030 targets for the use of cloud computing, which is fast becoming a mature technology. But EU firms need to vastly increase their use of cutting-edge technologies like AI and make far better use of data.

While the EU's productivity growth – as measured by GDP per hour worked – is keeping pace with the US,[6] indicating good use of technology, the EU cannot take much comfort from this fact. For one thing, much of the EU's productivity growth is from 'catch-up performance' in poorer member-states: but that is low-hanging fruit which will eventually become exhausted. The EU also faces much larger economic headwinds than the US because of its aging population, which means the EU needs to do much better on productivity growth if it is to maintain its current share of the global economy. Unfortunately, however, the trend is going in the wrong direction: productivity growth has been slowing over time. Europe's economic growth is poor and consistently trails that of the US.

Many of the steps to boost the digital economy, and therefore productivity and economic growth, are politically complex or will take time to deliver meaningful results. For example, one reason for the EU's lack of large tech firms is that Europe does not have deep and well-integrated capital markets. Too few investors are ready to back high-risk, high-potential ideas for a long enough period to allow those firms to scale up significantly. The EU is partly compensating with a range of funds and programmes to promote EU innovation – but real progress on the capital markets union project has been slow and painful. Another long-term constraint is that many EU firms find it difficult to hire people with digital skills. While the Commission has set targets to increase the digital skills of the EU's labour force, there has also been little progress on this front and faster solutions like increased immigration remain politically challenging.

1: Atomico, 'State of European Tech', 2023.
2: Creandum and Dealroom, 'European tech ascendancy: Unlocking a continent's innovation potential', July 2023.
3: European Central Bank, 'Digitalisation in Europe 2022–2023: Evidence from the EIB Investment Survey', 2023.
4: European Commission, 'Long-term competitiveness of the EU: Looking beyond 2030', March 16th 2023.
5: European Central Bank, 'Digitalisation in Europe 2022–2023: Evidence from the EIB Investment Survey', 2023.
6: Aslak Berg, 'Why Europe should not worry about US out-performance', CER insight, December 13th 2023.

Chart 1: To reach the EU's 2030 targets, enterprises must speed up adoption of cutting-edge technologies



Source: EC, DESI 2023 indicators.
Note: Enterprises include firms employing at least 10 employees. AI figures exclude financial sector.

While the EU must solve these problems to accelerate the digital economy in the long run, this policy brief focuses on three priorities to give Europe's digital economy a more immediate boost:

★ Simplifying the EU's tech regulation by ensuring it is well implemented, consistently enforced – and provides a predictable and proportionate approach which builds on the EU's economic strengths. Good regulation can boost innovation and growth – as when the EU's early action on climate change helped the Union become a leader in green technologies. But the Commission needs to address the reasons why the EU's rules have not yet helped Europe lead in cutting-edge tech markets.

★ Unlocking Europe's data economy and creating new data-driven business opportunities. There are significant opportunities for Europe to lead on privacy-friendly data innovation – but the current rulebook needs to facilitate this.

★ Building more resilient digital infrastructure. Without sufficient, robust and secure infrastructure, European firms will not be able to use new technologies, and promising tech firms will seek more opportunities outside, rather than within, Europe.

Fostering a digital economy matters greatly for Europe's future economic growth. Europe faces huge demographic headwinds, such as an aging population, and political opposition to higher migration. It will therefore be increasingly difficult for Europe to increase the economic pie by working more. Europeans must work smarter, not harder. This can only be achieved by helping all European firms go digital, and ensuring innovative European firms can scale up. Success should be measured by whether European firms adopt the best technologies from Europe and around the world – and whether European tech firms can innovate, test, commercialise and scale their innovations in Europe and globally.

Improving the EU's tech regulation

As a 'regulatory superpower', which has limited ability to co-ordinate an EU-wide fiscal policy or industrial policy, the EU's main policy lever is passing laws governing its single market. The speed, volume and detail of EU regulation in the technology sector over the last few years has been unprecedented. The think-tank Bruegel has identified 116 EU laws relevant to digitalisation which have been, or might be, enacted over the period 2019–2024.[7] Some of these have only incidental impacts on the overall digital environment. However, as Box 1 shows, there have been many major pieces of digital legislation over the period since 2019 which impact the whole digital economy.

Box 1: Examples of major digital laws passed since 2019 or proposed by the current Commission

Name	Status	Objective
Platform to Business Regulation	Enacted (Regulation 2019/1150)	Improve transparency and fairness for businesses who deal with online platforms
Digital Markets Act	Enacted (Regulation 2022/1925)	Ensure large digital platforms act fairly and make digital markets more contestable
Digital Services Act	Enacted (Regulation 2022/2065)	Create a safer digital environment protecting the fundamental rights of users
Data Act	Enacted (Regulation 2023/2854)	Improve use of data across the EU, including requiring providers of internet-connected products to share data with others
Artificial Intelligence Act	Politically agreed but not yet enacted	Introduce a risk-based regulatory framework for artificial intelligence systems
Chips Act	Enacted (Regulation 2023/1781)	Bolster Europe's competitiveness and resilience in semiconductor technologies
Cyber Resilience Act	Provisionally agreed but not yet enacted	Impose new cybersecurity requirements for products with digital elements
Network Information and Security Directive (NIS2)	Enacted (Directive 2022/2555)	Provide a high level of cybersecurity across the EU including in sectors vital to the economy
Gigabit Infrastructure Act	Politically agreed but not yet enacted	Speed up the deployment of high-capacity networks across the EU

EU digital rules can deliver important benefits. They may give consumers and businesses more trust in digital services, knowing services are safe and their data will be protected. They may help increase competition and unlock innovation by a wider range of players – making technologies cheaper and more accessible for European firms, and boosting productivity by helping more efficient firms displace less efficient ones. At its best, EU law-making can deliver a clear set of rules for tech firms. That can help European tech entrepreneurs, and foreign tech firms, establish and grow their tech businesses across all of Europe – equivalent to how entrepreneurs can easily access the US market of 330 million residents.

Ensuring laws are effectively and proportionately implemented and enforced

The volume of new laws creates a risk that the Commission and national enforcers will lack the resources to implement them properly. EU law-makers are vastly underestimating the challenge of implementing and enforcing the recent swathe of digital laws. Take the Digital Markets Act. The Commission is tasked with a complex set of responsibilities, including the following:

★ On 6 September 2023, it identified and defined 22 'core platform services' from six companies which will be regulated.

7: J Scott Marcus, Kamil Sekut and Kai Zenner, 'A dataset on EU legislation for the digital world', Bruegel dataset, November 16th 2023.

★ By 6 February 2024, it was supposed to have completed investigations into Microsoft's Bing, Edge and advertising services, and Apple's iMessage service, to decide whether Microsoft and Apple have presented sufficient arguments to avoid regulation for those services. (In fact, it appears the Commission was not able to complete any of these investigations in its target timeframe.)

★ By 6 March 2024, the regulated companies will have to comply with the Act's rules. By this date, the Commission should have determined how each regulated company needs to comply with the Act's rules.

★ By 6 September 2024, the Commission must have completed an investigation into Apple's iPad operating system to decide whether it will also be regulated.

★ The Commission must also spend significant resources monitoring how the six companies are complying with the rules, drafting more detailed requirements, and bringing enforcement action if companies are not compliant.

★ In the meantime, the Commission will also have to defend litigation brought by various companies which want to avoid regulation.

"If the Commission does not have the resources to properly implement and enforce laws, then it will not be in a good position to judge later whether those laws have been a success."

Each of these tasks is complex. The Commission must consider in each case how to enforce the rules properly while minimising unnecessary negative consequences for consumers. For example, the Commission will need to be deeply involved in understanding how regulated companies present choices to users to balance competing factors like the need for fair competition, the ability for consumers to protect their security, and to avoid 'choice fatigue'. Yet the Commission has only tasked a team of 150 staff to accomplish these goals. In comparison, the competition regulator in the UK is expected to have a team of 200 staff implementing its digital competition regime.[8] Moreover, the UK regime is far less mechanistic than the EU's – which means the 200 UK staff will be allowed to prioritise certain markets and services and they will not immediately need to impose rules for all regulated companies at the same time.

Without proper guidance and enforcement, large technology companies may face insufficient pressure to deliver the Digital Market Act's objectives. Or a resource-constrained Commission might implement the Act in ways that have unintended consequences – such as unnecessarily reducing the quality of digital services.

Implementation is not just a problem for regulators: industry faces similar resourcing problems. Take the Cyber Resilience Act, which aims to set cybersecurity standards for internet-connected devices – everything from industrial sensors to smart vacuum cleaners. The Act envisages the development of technology standards for a huge number of devices for which no standards currently exist. This will require a monumental effort from industry and other stakeholders over several years before there is certainty about how compliance with the Act can be achieved. Equivalent laws in the UK and the US are far more modest in scope.

If the Commission does not have the patience and resources to ensure laws are properly implemented and enforced, then it will not be in a good position to judge later whether those laws have been a success. The Commission may mistakenly conclude that more regulation – rather than better implementation and enforcement – is the answer, rendering implementation and enforcement capacity even more inadequate.

The next Commission should be more realistic about the resources required from regulators and from industry to make sure existing laws are implemented and enforced properly.

Reducing complexity

Another problem with the EU's tech regulation is that the EU's digital rules each tend to focus on individual problems. Law-makers have spent insufficient time considering how the many different laws work together to create a single rulebook. At best, this means the regulatory framework in Europe is unnecessarily complex. In the worst cases, the EU's approach fails to consider comprehensively how competing policy priorities should fit together – leading to inconsistencies, unintended regulatory gaps and an overall lack of coherence.

Take the following examples:

★ Two digital policy priorities are to increase the bloc's cybersecurity standards and to increase competition by making it easier for smaller firms to challenge incumbents. Yet the Digital Markets Act creates conflicts between the two objectives. For example, to limit the largest firms' advantages, those firms will not be able to use data as freely – even if their only reason for doing so is to spot and tackle cybersecurity threats.

★ The Data Act aims to give consumers the right to access data generated from their internet-connected products. The GDPR is supposed to take precedence

8: Sarah Cardell, evidence to the House of Commons Digital Markets, Competition and Consumers Bill Committee, June 13th 2023.

over the Data Act, which should mean that the Data Act only gives consumers the right to access their own personal data. Yet one device can collect data from many individuals (such as when different people in a household or business share the use of a device). Neither Act clarifies what to do in this context.

★ Problems like the use of 'dark patterns' – where services are designed to manipulate users' choices – may be regulated under each of the GDPR, the Digital Services Act, the Digital Markets Act and the Artificial Intelligence Act. Yet the rules, terminology and requirements of each law are all different, creating the risk of confusion or outright inconsistency.

★ While artificial intelligence is regulated by the Artificial Intelligence Act, numerous other laws also impose their own overlapping rules. These include the GDPR, the Digital Services Act, the Digital Markets Act and the Platform to Business Regulation. Moreover, the terms used across these laws are inconsistent – such as algorithms, recommender systems, profiling and automated decision-making – and these terms do not have the same definitions. This makes it very difficult for businesses that want to develop or use artificial intelligence to understand which obligations they have to comply with.

This situation means that entrepreneurs may prefer to take their ideas to the US, where the digital regulatory framework is easier to understand and comply with, and means that innovative EU firms may hold back commercialising new ideas out of a fear of non-compliance with EU laws. It also risks creating unnecessary barriers to competition – because large firms, with well-resourced legal and regulatory teams, are far better able to manage regulatory complexity and uncertainty than smaller ones. This is self-defeating, given the EU's intention to deliver a digital policy framework that provides more opportunity for European businesses.

The next Commission needs to undertake a rationalisation exercise. The exercise would involve an overarching study of the current digital regulatory landscape in Europe in order to identify and propose ways to address tensions, ambiguities and inconsistencies.

Recommendation 1

The next Commission should focus on ensuring the existing digital rulebook is properly implemented and enforced, before considering significant new regulatory obligations. It should also undertake a simplification and rationalisation exercise. This exercise should assess and address gaps, overlaps and inconsistencies in the EU's many recent digital laws.

Future-proofed, principles-based regulation

In its efforts to respond quickly to technological developments, the EU also risks being overly prescriptive or taking disproportionate action. Regulation which is too specific, or is targeted at particular technologies or immediate problems, rarely creates a clear and enduring set of rules. These types of regulations will become out-of-date as technologies and markets evolve, creating further uncertainty. And such rules may lock in suboptimal market structures, technologies and ways of doing business – hindering competition, take-up of new technologies, and productivity growth.

To list a number of recent examples:

★ The Digital Markets Act – which sets rules to address the 'gatekeeping' position of large technology firms and promote more competition. The law seems to be inspired mostly by a desire to settle existing antitrust cases or investigations against large technology companies, rather than setting future-looking principles. Consequently, the Act seems to both omit some pressing competition problems, while hindering large firms when they try to enter new markets as 'challengers' to improve competition.

★ The Commission's proposal for an Artificial Intelligence Act was targeted at cases where artificial intelligence posed risks, rather than regulating the technology itself. However, when numerous generative artificial intelligence services like ChatGPT launched midway through the legislative process, MEPs added rules which applied to general purpose models – such as those used to analyse and process language, which underpin services like ChatGPT – regardless of how much risk they pose in practice. In regulating providers of particular technologies, instead of the ways those technologies are applied, these changes may risk making it harder for small, disruptive firms to provide certain types of artificial intelligence – or making it harder for European businesses to adopt and integrate artificial intelligence systems in their businesses.[9]

9: DigitalEurope, 'Joint statement: Let's give AI in Europe a fighting chance', November 23rd 2023.

★ The Data Act proposal also imposes unnecessary rules on firms that want to use technologies. The Act would force firms who produce connected, data-generating devices (from smart fridges to industrial robots) to share that data with other firms. The Act may help in cases where dominant firms are 'hoarding' data: in which case, the refusal to share that data might hinder innovation. But most connected devices are sold in highly competitive markets: there are countless manufacturers of connected fridges, vacuum cleaners, and smart speakers, for example. By applying the same rules to all manufacturers – even where there is no competition problem – the Data Act risks reducing firms' incentives to collect valuable data in the first place. The proposal was widely opposed by industry.[10] A more future-proofed and principles-based approach would have allowed regulators to identify specific markets where a lack of data sharing is hindering competition, and give the Commission flexibility to make targeted interventions tailored to the particular markets in question. This model has worked well in areas such as banking, payments and communications. In those markets, regulated data-sharing has promoted innovation and helped consumers switch services easily, boosting competition.

In all these cases, the weakness of EU digital laws is their focus on addressing immediate problems rather than stepping back to identify overall objectives and principles that should govern the digital sector. More effective tech regulation should be future-proofed and principles-based – it should tell regulated firms the outcomes they need to achieve, but give them the flexibility to work out how to deliver that outcome, and should avoid rules that are too focused on particular technologies. Good tech laws therefore give an appropriate amount of space for at least some degree of self-regulation (where firms decide themselves how to deliver a law's objectives) or co-regulation (where firms and regulators co-operate to decide how a law's objectives should be achieved).

This type of regulation would do a better job of unlocking Europe's digital economy. It would reduce regulatory complexity, making life easier for smaller firms, and making it easier for EU regulators to enforce the law properly. It would give a more certain environment for investment: because laws would not need to be updated and supplemented each time technologies or market structures change. It would promote innovation in Europe, because it would allow firms to use cutting-edge technologies and services from around the world, so long as they were consistent with a law's overall objective. It would help firms stay competitive globally, because they would be allowed to find the most cost-effective ways to achieve a law's objectives. Finally, principles-based regulation can help keep European markets open. It would minimise the risk of conflict between European rules and those of other countries – giving European tech firms confidence that they could take their business model and apply it across Europe and beyond. It would also make it less challenging for global firms to do business in Europe – improving competition and making it easier for European firms to adopt technologies from elsewhere in the world.

The EU has good examples of what this type of regulation might look like in practice:

★ The Cyber Resilience Act borrows heavily from the EU's existing and highly successful approach to product safety. The Act's goal is to promote the development of cybersecurity standards. Although the scope of the Act is very broad, which as noted above will impose significant costs on industry, the design of the law at least helps to give industry opportunities to find the most efficient way to comply. The Commission estimates that for 90 per cent of devices, the manufacturer will be able to self-assess whether the device complies with the Act's cybersecurity requirements.[11] This type of approach trusts individual firms to act responsibly in low-risk cases, and in higher-risk cases empowers industry to work collaboratively to set standards. Only in cases where industry fails to prepare proper standards will the Commission step in and set its own requirements.

★ Another example is the way in which the Digital Services Act requires the largest online platforms to identify and mitigate certain systemic risks caused by their services. But it does so without prescribing what those large platforms must do. This is a sensible approach, since tackling problems like disinformation is complex, context-specific, and needs to evolve to make use of new technologies like artificial intelligence. In assessing whether online platforms comply with the Act, the Commission can focus on whether platforms have dedicated resources and have put systems in place to tackle risks, avoiding a more resource-intensive approach of delving into more technical detail.

Recommendation 2

The Commission should consider whether existing digital laws could be recast to deliver more future-proofed and principles-based regulation, including an appropriate role for self-regulation and co-regulation.

10: Clément Perarnaud and Rosanna Fanni, 'The EU Data Act: Towards a new European data revolution?', CEPS Policy Insight, March 2022.

11: European Parliament, 'EU Cyber-resilience Act: Briefing', May 2023.

Deepening the digital single market

Law-makers intended recent EU digital laws to promote regulatory harmonisation across Europe and therefore foster an EU-wide marketplace for accessing and using online services. In 2015, the Commission estimated a true digital single market could contribute more than 2 per cent to future GDP growth.[12] It would give businesses access to a market of 448 million people, making Europe a more attractive destination for foreign technology firms to invest in. Digital services typically benefit from huge economies of scale. So completing the digital single market also offers large opportunities for European tech firms – if European firms could achieve a similar scale 'at home' to that which American firms currently enjoy in the US market, then European firms would have more incentives and resources to invest in technology to achieve this scale. By reducing barriers to cross-border growth, more productive firms in one part of the EU will be able to earn market share across the Union, forcing all firms to become more efficient, lower their prices, or find new ways to innovate. That would improve Europe's productivity, which consistently lags that of the US.

"By reducing barriers to cross-border growth, more productive firms in one part of the EU will be able to earn market share across the Union, forcing all firms to become more efficient, lower their prices, or find new ways to innovate."

In some respects, the Commission is making good progress at delivering this vision. It is shifting away from the use of directives, which member-states often fail to transpose into domestic law quickly, and which member-states may 'gold-plate' with additional requirements. It is increasingly replacing them with regulations – the Data Protection Directive was replaced by the GDPR, and the E-Commerce Directive was replaced by the Digital Services Act, for example. Regulations apply directly in EU member-states' legal systems. Enforcement of digital laws, such as the Digital Markets Act and the Digital Services Act, is also taking place at EU-level (at least in the most important cases).[13] This is helping to ensure digital laws are implemented and applied consistently across the whole of the EU – promoting harmonisation and thus market integration and scale.

But EU laws still allow too much fragmentation, and overlapping or inconsistent national approaches. For example, law-makers passed the Digital Markets Act in 2022. The legal basis for the Act was Article 114 of the Treaty on the Functioning of the European Union (TFEU), which gives the EU powers to make laws to harmonise regulation across the Union. The Commission's impact assessment emphasised that this harmonisation would lead to economic benefits of €92.8 billion.[14] Yet the Act specifically allows member-states to supplement the rules by toughening their own competition legislation in the digital sector. In January 2021, as the law was being considered, Germany introduced such reforms – which allow the German competition authority to adopt different solutions to competition problems caused by big tech firms. While the German law is in some respects an improvement on the Digital Markets Act, it means that large tech firms may have to follow more onerous rules in Germany – and smaller firms who need to do business with big tech may have to follow different processes in different EU countries. This introduces unnecessary complexity. Some legal scholars have even questioned whether the Act has a sound legal basis, given its contribution to regulatory fragmentation.[15] Similar problems exist in other areas of digital regulation. For example, the EU's Digital Services Act aims to increase the accountability of online platforms. Yet France continued to press ahead with its own laws regulating similar topics such as online influencers and other online content.[16]

It is not just the existence of individual member-states' laws that detracts from the digital single market – but also their inconsistent enforcement across EU member-states. Cybersecurity laws are a particular culprit. Cybersecurity laws tend to be directives rather than regulations and so must be transposed by member-states.[17] Many of the EU's cybersecurity laws are also enforced largely by member-states' own national agencies, rather than EU agencies like the European Union Agency for Cybersecurity (ENISA).[18] This provides significant scope for national divergence on issues like the reporting of cyber incidents. The proposed certification scheme for the security of cloud

12: European Commission, Staff Working Document, 'A Digital Single Market Strategy for Europe - Analysis and Evidence', June 5th 2015. Estimates of 0.6 – 1.7 per cent of GDP are cited in European Parliamentary Research Service, 'Mapping the Cost of Non-Europe, 2019-24', April 2019.

13: The Digital Markets Act also prevents member-state regulators or courts taking a different approach to the Commission: Digital Markets Act article 39(5).

14: European Commission, 'Impact assessment of the Digital Markets Act', SWD (2020) 363, December 15th 2020.

15: Alfonso Lamadrid, 'Why the Proposed DMA Might be Illegal under Article 114 TFEU, and How to Fix It', *Chillin' Competition* blog, April 12th 2021.

16: Loi 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux.

17: For example, the NIS2 Directive and the Resilience of Critical Industries Directive.

18: See European Court of Auditors, 'Challenges to effective EU cybersecurity policy', briefing paper, 2019.

services could further fragment the single market. While the scheme is being designed at EU level, member-states will be free to decide for themselves how to use the certifications, such as to restrict some contracts to cloud companies who achieve the highest security accreditation.[19]

Finally, a number of key laws critical to EU digitalisation remain directives and have therefore suffered from slow and inconsistent implementation across the EU. The European Electronic Communication Code – which regulates electronic communications networks and services, and is therefore central to the EU's digitalisation efforts – is an important example. Twenty-four of the 27 member-states failed to transpose the Code into domestic law by the deadline of 21 December 2020, and in September 2021 the Commission had to take further action against 18 member-states, which still had not implemented the Code in full. The delays deprived consumers of new rights, prevented telecoms operators from enjoying more harmonised EU-wide rules, and delayed a regulatory regime that was intended to boost rollout of digital infrastructure.

Continued allowances for divergence between EU member-states undermine the EU's ambitions for a digital single market – making Europe a less attractive market and making it harder for European businesses to scale. To address this problem, the Commission should continue to prioritise regulations over directives, and allow fewer opportunities for EU member-states to supplement or diverge from EU-wide rules.

Recommendation 3

The Commission should consider ways to promote more centralised implementation and enforcement of the EU's digital laws, and limit the scope for member-states to supplement or diverge from EU-wide rules.

Building on the EU's economic strengths

A fourth and final problem is that hasty digital regulation does not always protect and promote an important driver of Europe's economic growth – its position as an open trading bloc.

Most of the EU's productivity growth is currently concentrated in smaller and poorer member-states, who can benefit from adopting mature technologies. This 'catch-up growth' relies heavily on being able to take advantage of technologies and services from anywhere around the world – and therefore maintaining economies which are open to international trade. Most European research and development is focused in areas like auto manufacturing and pharmaceuticals rather than digital services. As Chart 2 on the next page shows, the EU lags far behind the US and China in investing in research and development in the ICT sector.[20]

The EU has ambitions to lead in cloud computing and AI. But its lack of research and development funding means it cannot afford to discourage or limit take-up of foreign technologies in the meantime. In any event, to deliver economic growth, adoption of technology by firms is far more important than being the source of innovation. American cloud computing firms may earn high profits, for example – but those services have also brought undeniable and significant productivity improvements to European businesses. To maximise these benefits, European companies should not face artificial barriers to using foreign services where these are the best or cheapest options.

Besides, if the EU limits access to its market, other countries will retaliate – or the EU will lose the moral high ground, blunting its own efforts to persuade other countries to open their markets to European firms. Maintaining the EU's openness – at least to countries that have a similar commitment to openness – is therefore critical both to firms' technology adoption and to EU tech firms who have ambitions to be global leaders.

While the EU repeatedly commits to keeping markets open, in practice a number of digital laws have shifted away from open markets and towards a more 'sovereignty-first' approach to technology. The two areas where this is most prominent are cloud computing and data transfers.

In cloud computing, the EU's cloud cybersecurity certification is still under negotiation, but it seems likely to include a number of 'sovereignty' requirements. These requirements might, for example, reserve the highest security accreditations for cloud services which are either operated by EU-based companies with no non-European entity exerting effective control, or those that have measures in place to stop non-EU companies having

19: Zach Meyers, 'Can the EU afford to drive out American cloud services?', CER insight, March 2nd 2023.

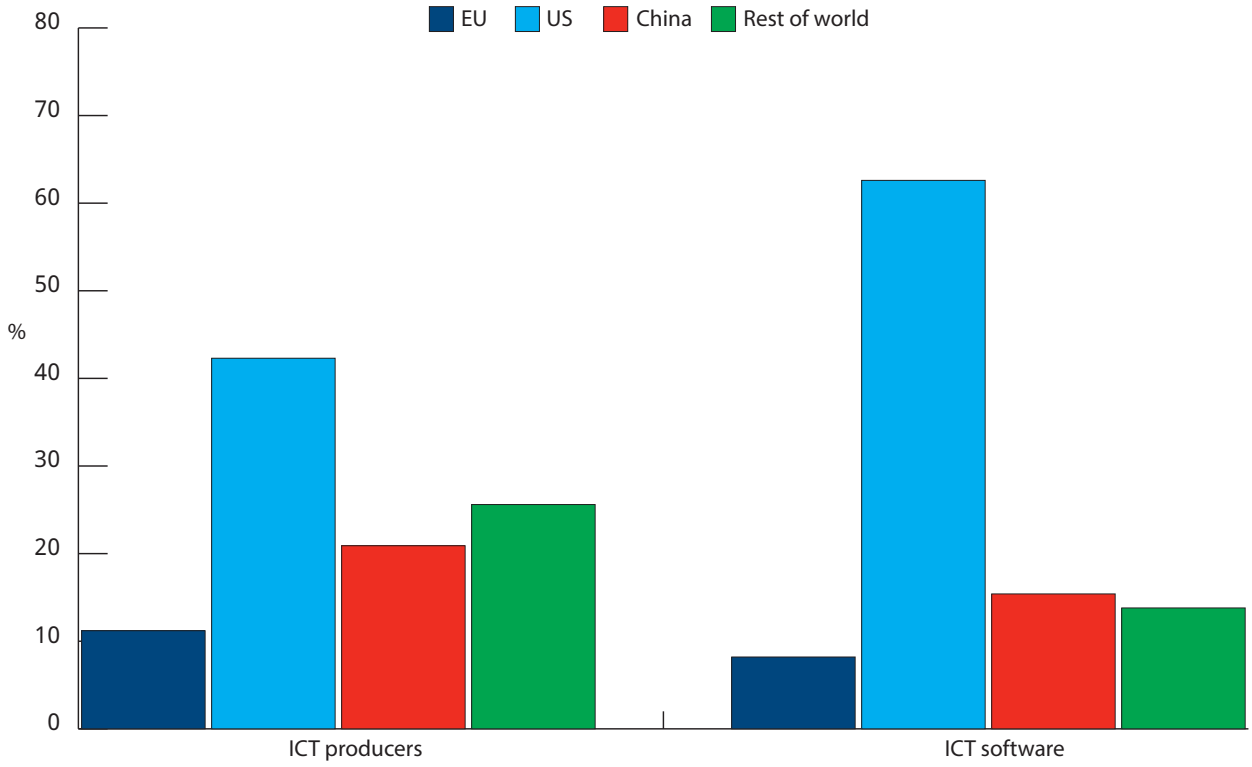
20: European Commission, 'EU industrial R&D investment scoreboard', 2023.

decisive influence over certain activities. There may also be requirements that data is located only in Europe.[21] These requirements risk leaving important European firms with fewer cloud services to choose from – limiting their access to cheap and world-leading technologies.

The EU has also started to shift away from championing free dataflows, towards a more restricted approach to transferring data out of the EU more generally. Two recent EU laws – the Data Act and the Data Governance Act – impose new requirements on companies that want to transfer even non-personal data outside the EU. These restrictions are intended to protect EU trade secrets and intellectual property from foreign governments who might try to access them. But the restrictions introduced seem excessive. They do not require companies to analyse whether intellectual property theft is a real issue. And EU companies already have incentives to protect their own intellectual property, so law-makers had no real evidence that regulatory intervention was necessary. If smaller firms are unaware of the risks of sending their trade secrets and intellectual property overseas, then a more proportionate approach might be for the Commission to provide resources to help educate firms about those risks and how to mitigate them.

There may be justifications to limit data transfers in specific cases: such as to protect personal data. But limitations on data transfers come at a significant economic cost, so those limitations should be as narrow as possible and used only as a last resort. The EU could focus on developing bilateral or multilateral solutions to address its concerns about non-personal data rather than imposing unilateral restrictions on dataflows – such as reaching an agreement with the US about access to European industrial data by American law enforcement officials.

Chart 2: The EU's share of global R&D in ICT, 2022



Source: European Commission, EU industrial R&D investment scoreboard.

Recommendation 4

The EU's digital regulations should focus on maintaining open markets – encouraging European firms to adopt the best technologies available, and helping ensure that European tech companies have access to a global marketplace.

21: Luca Bertuzzi, 'EU cloud scheme slightly tones down sovereignty requirements', Euractiv, November 22nd 2023.

Facilitating the use of data

The overall tech regulatory landscape would therefore benefit from simplification and a renewed focus on EU-wide harmonisation and market openness. That is especially true in the case of the EU's data regulations, which deserve particular attention.

The current Commission understands the immense potential that could be unlocked if European businesses made better use of big datasets. Advances in artificial intelligence offer the opportunity for firms to analyse vast quantities of data – generated by everything from consumer devices to industrial sensors. The insights can be used to optimise processes, and to create innovative new products and services. But only 14.2 per cent of European firms currently take advantage of big datasets.[22] And firms say that they have insufficient access to data to use technologies like AI.[23]

Laws like the GDPR should not inherently prevent innovation. Many global technology firms have voluntarily chosen to adopt parts of the GDPR all over the world[24] and the GDPR is widely accepted by data-intensive businesses like digital marketers.[25] However, when the EU finalised the GDPR in 2016, law-makers hoped it might unleash a wave of privacy-focussed European tech successes. These hopes have so far proved unfounded.[26] As other countries move closer towards the GDPR in their own data protection regimes,[27] however, the EU still has opportunities to achieve leadership in privacy-enhancing technologies. These could unlock ways for European firms to extract value out of personal data without compromising individuals' fundamental rights.

Helping firms exploit non-personal data

To help firms exploit data, firms must have legal avenues to collect and use them. Numerous recent EU initiatives are helping firms get more access to usable data:[28]

★ The 2019 Copyright Directive allows copyrighted material to be reproduced and extracted for data-mining purposes, unless the rights-holder opts out.[29] This provides a legal basis for European firms to use data to train artificial intelligence models.

★ The EU has forced member-states to publish more of their datasets, making them available for businesses to use in innovative ways.[30]

★ The recent Data Governance Act takes steps to enable and promote more voluntary data sharing in the private sector.[31]

★ A 2018 regulation promotes the free flow of non-personal data throughout the EU, stopping member-states from insisting non-personal data is processed in their own country.[32]

★ The Data Act will force firms to share more data, which the EU hopes will unlock value in the 80 per cent of non-personal data which firms are collecting but not using.[33]

★ The Commission has championed 14 'common European data spaces' in strategic economic sectors.[34] Building on the above initiatives, the common data spaces aim to create secure tools, infrastructure, standards and governance frameworks to help firms co-operate in pooling and sharing data.

However, the focus of these initiatives is mostly on exploiting non-personal data. This is understandable: there is little appetite to make substantive changes to the EU's flagship data protection rules, the GDPR, and protection of personal data is in any event embedded in the Charter of Fundamental Rights of the European Union. However, the Commission's emphasis on non-personal data is very limiting, because the distinction between personal and non-personal data can be extremely difficult to determine in practice[35] – and because personal and non-personal data are often tightly linked together.[36] Take, for example, the data generated by connected cars, or consumer goods like smart vacuum cleaners. These data usually qualify as personal data, since they can be attributed to an identifiable person – even if firms only need the data to understand overall

22: European Commission, 'Long-term competitiveness of the EU: Looking beyond 2030', COM(2023) 168, March 16th 2023.
23: Mia Hoffmann and Laura Nurski, 'What is holding back artificial intelligence adoption in Europe?', Bruegel, November 2021.
24: Jeff Bullwinkel, 'The GDPR can foster, rather than hinder, innovation in Artificial Intelligence', LinkedIn, December 2nd 2018.
25: Jack Apollo George, 'Red tape, innovation and the future of GDPR', *Raconteur*, September 17th 2021.
26: Giorgio Presidente and Carl Benedikt Frey, 'The GDPR effect: How data privacy regulation shaped firm performance globally', VoxEU, March 10th 2022.
27: See, for example, Australian Government, Attorney-General's Department, 'Privacy Act Review Report', 2022.
28: European Commission, 'A European strategy for data', COM(2020) 66, February 19th 2020.
29: Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market.
30: Directive (EU) 2019/1024 on open data and the reuse of public-sector information.
31: Regulation (EU) 2022/868 on European data governance.
32: Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.
33: Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act) COM/2022/68.
34: European Commission, 'Commission staff working document on common European data spaces', SWD (2022) 45, February 23rd 2022.
35: Michèle Finck and Frank Pallas, 'They who must not be identified-distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law*, Volume 10, Issue 1, February 2020.
36: Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, article 2.2.

usage patterns. But it is unclear how to remove the personal elements of data so it is anonymous. That often means businesses must assume entire datasets fall under the scope of the GDPR – vastly constraining the benefits of the EU's recent data initiatives.

The opportunities of the EU's recent data reforms cannot be unlocked without providing a clearer boundary between personal and non-personal information. Firms need to better understand, for example, how they can sufficiently anonymise data so that it is no longer governed by the GDPR.

"The opportunities of the EU's recent data reforms cannot be unlocked without providing a clearer boundary between personal and non-personal information."

Anonymised data holds enormous economic potential for Europe. It offers a way to reconcile the EU's ambitions for data-driven economic growth and innovation, on the one hand, with protection for fundamental rights on the other hand:[37]

★ It could help more firms find innovative uses of their data. For example, unlike personal data, firms can freely use anonymous data to experiment and test new products.

★ Anonymous data can help firms comply with the Artificial Intelligence Act rules, which require certain AI systems to avoid bias.[38] Although regulators have not clarified how these rules will work, using anonymised datasets to train AI models could help ensure data is properly representative.

★ Anonymisation may help firms reduce their costs of using global services based in other parts of the world. Anonymisation may, for example, assist European tech firms to transfer data across borders (even in countries that have inadequate protection of personal data) while complying with the GDPR.

★ Anonymous data may help unleash new privacy-protective business models and technologies in Europe which could be exported around the world. One example is the production of 'synthetic data'. Synthetic data is generated using personal datasets, but it aims to replace the personal data with artificially generated data, while preserving relevant structures, patterns and correlations in the personal data. The synthetic data can therefore remain useful for particular purposes, like training an artificial intelligence model. In the context of digital advertising, for example, synthetic data can be used to project a user's likely interests (and therefore the ads that are likely to be relevant to them) without requiring the explicit collection of personal data – providing a much more privacy-friendly alternative to today's targeted advertising.

Many of these activities would not be practical if the data was governed by the GDPR: for example, because it would be infeasible for firms to obtain consent or even to notify every person from whom the data derives.

The GDPR recognises that data protection principles do not apply to anonymous data. Under the GDPR, data is anonymous where an individual cannot be re-identified and the anonymisation process is irreversible. To treat data as anonymous, a firm must consider the means "reasonably likely to be used" to try to identify an individual,[39] taking into account factors such as the costs and time required to do so. In determining whether data is anonymous, the GDPR therefore takes a proportionate, risk-based approach. This is practical. Whether data can be reverse-engineered to identify individuals is not always easy to answer – for example, in very large datasets, there can sometimes be a theoretical risk that some individuals might be identifiable based on statistical analysis, even if the practical risk is very low, for example because it would require combining data which is held by different parties, or require immense computing power. In some areas, like production of synthetic data, firms need to carefully balance the risk of re-identification against having data which more closely tracks the patterns in the original dataset.[40] Regulators therefore need to provide sensible, clear guidance on exactly when and how data can qualify as 'anonymous'.

Clear, proportionate and tech-savvy guidance from regulators is essential. However, when it comes to anonymity, in practice some national data protection authorities have taken an unduly rigid approach, different member-states have been inconsistent, and many questions are still unanswered. For example:

★ Authorities have provided little guidance so far on the role of emerging technologies like artificial intelligence, which might make it easier for bad actors to use anonymous or synthetic data to re-identify individuals, but can also be used to obtain more protections against re-identification.

★ Whether an individual can be re-identified is often context-specific. Some EU authorities have implied that it must be impossible to infer or identify an individual.[41] This poses an unrealistic hurdle, especially when it comes to large datasets, where it can be very difficult to entirely eliminate any theoretical possibility of reidentification, but where the practical risks can sometimes be negligible.

37: See Andrew Burt et al, 'A guide to the EU's unclear anonymization standards', IAPP, June 15th 2021.
38: For example, high-risk systems must use representative, complete and error-free training data.
39: GDPR recital 26.
40: Deloitte, 'Preserving Privacy in Artificial Intelligence Applications through Anonymization of Sensitive Data', 2022.
41: Article 29 Working Party (Opinion 05/14).

★ Data protection agencies have taken very cautious and inconsistent approaches to synthetic data and the circumstances in which it can be treated as anonymous. For example, some stakeholders in the UK seem to believe the use of synthetic data should still comply with the principle of data minimisation, which implies synthetic data is still governed by the GDPR.[42]

The GDPR set up a European Data Protection Board, comprising the head of each member-state data protection authority, and tasked with ensuring the consistent application of the GDPR. The European Data Protection Board is currently preparing new guidelines on data anonymisation – and this offers an opportunity to provide a more consistent and workable approach. The Commission should engage with the Board, for example by requesting that the Board ensures the new guidelines are comprehensive and proportionate. Industry has called for 'codes of conduct' or 'certification schemes' to help give firms certainty about the appropriate standards and techniques to anonymise data, which would be a practical way forward.[43] Consistent, practical and proportionate regulatory guidance on anonymisation could help unlock the benefits of the Commission's reforms to non-personal data.

Recommendation 5

The Commission should engage with the European Data Protection Board to encourage the Board's new data anonymisation guidelines to be comprehensive, proportionate and risk-based.

Consistency and a single rulebook for data

While anonymisation and synthetic data offer big opportunities, the Commission should also recognise that some data cannot be de-personalised without losing its value. So the GDPR needs to provide a realistic basis for privacy-friendly innovation in these cases. Currently, however, the GDPR reflects a number of the general problems with EU tech regulation identified in the previous section of this paper – such as a lack of clarity, EU-wide consistency and flexibility. Germany's digital industry association Bitkom, for example, has found that nearly three quarters of businesses surveyed thought their biggest challenge was uncertainty about the GDPR's requirements.[44]

The GDPR was a step-change in EU-wide harmonisation on data protection. However, it still has not delivered a single rulebook in practice.[45] The Commission recently proposed some reforms to harmonise processes and improve co-ordination between authorities in cross-border cases.[46] These reforms are helpful but they do not address most of the ways in which the GDPR has failed to deliver a digital single market. Three primary problems remain:

★ First, the GDPR allows different member-states to adopt different positions on certain points – such as, for example, the age at which a person can consent to the use of their data.[47] This directly undermines the single market, by requiring digital services to operate differently in different member-states – unnecessarily driving up the costs of rolling out services in Europe. Member-states are also allowed to supplement certain parts of the GDPR in their own national laws, for example on the protection of health and biometric data, the use of data for research purposes or in employment law, and the use of data about criminal convictions.

★ Second, the GDPR is supposed to operate via a 'one-stop-shop': meaning that companies which operate in different member-states generally only need to deal with a single data protection authority (the authority in their country of establishment). However, the 'one stop shop' does not apply to all activities under the GDPR,[48] meaning that businesses that operate in more than one member-state still risk having to deal with different authorities on the same issue.

★ Third, and most importantly, different member-states' authorities have applied divergent interpretations of the GDPR. The Irish data protection authority, for example, has become infamous for its different approach to enforcement and interpretation of the law. In some cases, this has led to fierce disagreements between different countries' authorities on fundamental aspects of the

42: Financial Conduct Authority, the Information Commissioner's Office and the Alan Turing Institute, 'Research Paper: Exploring Synthetic Data Validation – Privacy, Utility and Fidelity', 2023.
43: DigitalEurope, 'Two years of GDPR: A report from the digital industry', June 10th 2020.
44: Andreas Streim, 'Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen', BitKom, September 29th 2020.
45: Bitkom, for example, found that nearly half of surveyed German companies considered the GDPR to be implemented differently across EU member-states.
46: Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679.
47: GDPR article 8.
48: Namely, where processing takes place pursuant to a legal obligation or where necessary for the performance of a task carried out in the public interest or in the exercise of an official authority: see GDPR article 55.

GDPR, such as the legal ways in which firms can conduct targeted advertising (which forms the business model for countless digital firms). On several related questions, the Irish authority has been overruled by other data protection authorities, creating significant uncertainty.[49]

Lack of harmonisation imposes costs on all firms – in the worst case, forcing them to fragment their services in different countries, and undermining the digital single market. But it has particular consequences for European firms trying to grow across Europe. They are likely to be less able to cope with inconsistent guidance, practice and requirements than American behemoths that already have a footprint across the EU.

Removing member-states ability to set their own rules in some areas, and reducing national authorities' ability to supervise certain activities, would require changes to the GDPR itself. While some of these changes would be politically contentious, the Commission is due to evaluate the application of the GDPR by May 2024. The Commission should use this evaluation to highlight the need for a genuine single rulebook and its potential to unlock more privacy-friendly innovation in Europe. Targeted improvements to create a consistent application of the GDPR across Europe would help the law deliver its initial innovative promise – without compromising its important role in protecting EU citizens' fundamental rights.

Recommendation 6

In its evaluation of the GDPR, the Commission should consider amendments to help ensure the law is interpreted and applied consistently across the EU.

Proportionate and risk-based rules

A second focus should be whether the GDPR delivers the initial promise of imposing proportionate regulatory burdens. Law-makers intended the GDPR to create a risk-based approach to protecting personal data. For example, the fundamental requirement of the GDPR is that businesses protect EU citizens' data by implementing "appropriate" measures that take into account "risks of varying likelihood and severity".[50] That implies that proportionality is a key principle of the GDPR. In other words, firms must do more to protect against high-likelihood, high-severity risks, and might not need to take exactly the same steps to protect against more remote or theoretical risks.

Yet in certain areas, EU courts and national data protection authorities have shifted away from a risk-based approach. Cross-border dataflows are one example. The GDPR allows firms to send personal data to countries that do not have an equivalent law to the GDPR, so long as the firms take additional steps to keep that data safe – such as getting contractual guarantees from the overseas firm that receives the data. However, courts and national data protection authorities have increasingly decided that these additional steps will often be insufficient to allow transfers to take place – even if the possibility of a data protection breach is only theoretical.[51] The Commission recently negotiated a new set of safeguards for Europeans' data in the US to try to protect free dataflows. However, if the European Court of Justice (ECJ) invalidates that arrangement – which is a distinct possibility, since the ECJ overturned the last two attempts at such a deal[52] – EU-US personal data transfers could end up being banned entirely. This would make Europe a far less desirable destination for US tech firms to roll out services, and would have significant consequences for the countless European businesses that rely on US technologies and services. DigitalEurope estimated in 2021 that Europe would be €2 trillion better off if international data transfers were facilitated, compared to a baseline (which looks increasingly plausible) where the GDPR makes cross-border dataflows largely infeasible.[53] The Commission should consider ways to ensure that the GDPR, and in particular its rules for cross-border dataflows, is applied in a proportionate and risk-based way.

49: European Data Protection Board, 'Facebook and Instagram decisions: "Important impact on use of personal data for behavioural advertising"', January 12th 2023.

50: GDPR article 24.

51: The Italian and Austrian data protection agencies, for example, recently prohibited the use of Google Analytics, a service used by countless European websites. And a decision by the Irish data protection authority decided Meta must end its data transfers to the US. Garante per la Protezione dei Datai Personali, 'Google: Garante privacy stop all'uso degli Analytics. Dati trasferiti negli Usa senza adeguate garanzie', June 23rd, 2022; Datenschutz Behörde, Decision 020, Zl. D155.027, 2020-0.527.385, October 2nd 2020; Data Protection Commission, 'Data Protection Commission announces conclusion of inquiry into Meta Ireland', May 22nd 2023.

52: Maximillian Schrems v Data Protection Commissioner (Judgment), C-362/14, October 6th 2015; Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Judgment), C-311/18, July 16th 2020.

53: DigitalEurope, 'The EU can be €2 trillion better off by 2030 if we secure cross-border data transfers', June 17th 2021.

Recommendation 7

In the Commission's evaluation of the GDPR, it should consider whether the original intention to create a proportionate and risk-based approach to data protection is being maintained – and, if not, propose amendments to re-emphasise this principle.

Expanding Europe's digital infrastructure

Good regulation can help reduce barriers to European tech firms' growth in Europe and around the world. But digital infrastructure will also be essential to ensure European businesses can adopt new technologies like artificial intelligence and cloud computing – and so that European tech firms can build demand for their services in Europe. Infrastructure is essential for Europe's industrial ambitions. Firms need it to access and process the data collected by everything from connected consumer devices to smart industrial machinery, and to adopt new remote or automated manufacturing processes like 3D printing and advanced robotics. Digital infrastructure is also an essential part of Europe's ambition to be a leader in green technologies – for example, smart energy grids can help make reliance on green energy cheaper and more secure, and they rely on reliable and ubiquitous telecommunications networks.

"The low price of digital connectivity in Europe remains a strength - but low prices need to be matched with high-quality, resilient and ubiquitous infrastructure."

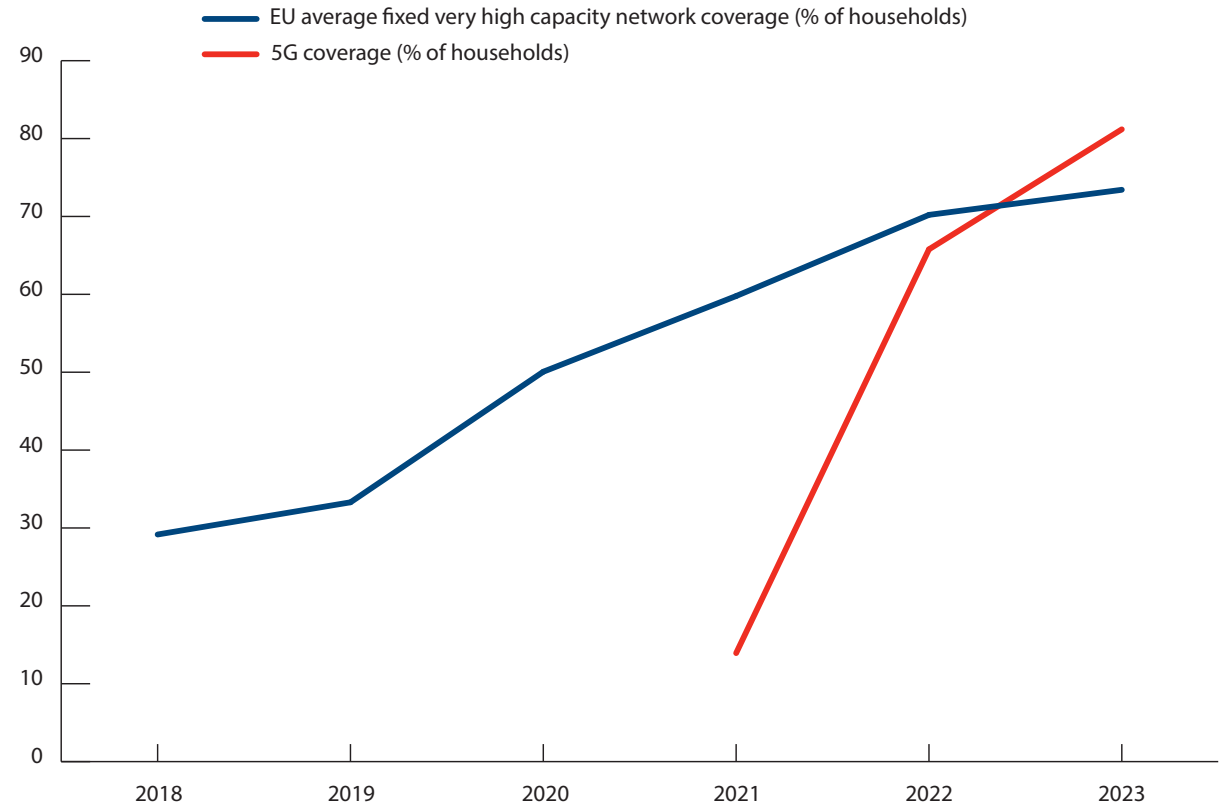
Numerous studies illustrate a correlation between greater rollout of telecommunications networks, on the one hand, and productivity and GDP growth, on the other.[54] This is unsurprising. The replacement of copper cable networks, and newer generations of mobile networks, have revolutionised how people connect and businesses operate. They let businesses hire employees from all over Europe and beyond; enable people in poorer or less urban locations to participate more easily in the economy; and allow businesses to reach customers all over Europe and globally. Regions with faster internet speeds tend to have firms which are more digitally-enabled, more innovative and more resilient.[55] In 2014, the Commission estimated that a full rollout of high-speed fixed and wireless networks across Europe would directly contribute €106 billion to the European economy per year.[56] More recent estimates suggest the benefits could be substantially higher.[57]

The low price of digital connectivity in Europe remains a strength – connectivity is overall significantly cheaper and more competitive than in the US – but low prices need to be matched with high-quality, resilient and ubiquitous infrastructure.

By 2030, the EU intends that all European households should have access to a communications network capable of achieving gigabit speeds and all populated areas should have 5G (or equivalent) mobile coverage.[58] The EU's roll-out statistics look satisfactory on the face of it. As Chart 3 (on the next page) shows, after a slow start, the EU has significantly increased the coverage of high-quality digital networks in recent years and is making good progress towards its targets. The EU is currently ahead of the US in terms of the number of 5G base stations per capita[59] although the US has significantly greater population coverage of 5G, with 96 per cent compared to 81 per cent in the EU.[60]

54: OECD, 'National Broadband Plans', OECD Digital Economy Papers, No. 181, 2011.
55: European Central Bank, 'Digitalisation in Europe 2022–2023: Evidence from the EIB Investment Survey', 2023.
56: European Commission, 'The Economic Impact of Digital Structural Reforms', September 2014.
57: Accenture, 'The impact of 5G on the European Economy', February 2021.
58: Digital Decade Policy Programme article 4(2)(a).
59: European 5G observatory, 2022.
60: European Commission, 'Report on the state of the Digital Decade', 2023.

Chart 3: Digital connectivity in the EU is picking up



Source: EC, DESI 2023 indicators.
Note: Very high capacity networks comprise full-fibre, fibre-to-the-building, or DOCSIS3.1 and higher cable networks.

However, these encouraging headline figures hide many underlying problems. For one thing, as Chart 4 (on the next page) shows, many countries are still lagging. For example, Greece has by far the smallest proportion of premises with access to high-speed fixed broadband.

The pace of infrastructure rollout is slowing and rural areas, which are the most expensive and difficult to reach, still lack good connectivity.[61] This risks holding back EU economic growth, since a major economic benefit of digital connectivity is to help integrate and unlock the potential of many of the poorest and least well connected parts of the EU – areas which have big potential to deliver 'catch up' growth. Illustrating these problems, a significant number of European firms still see limited access to digital infrastructure as a major obstacle to investment in digitalisation.[62]

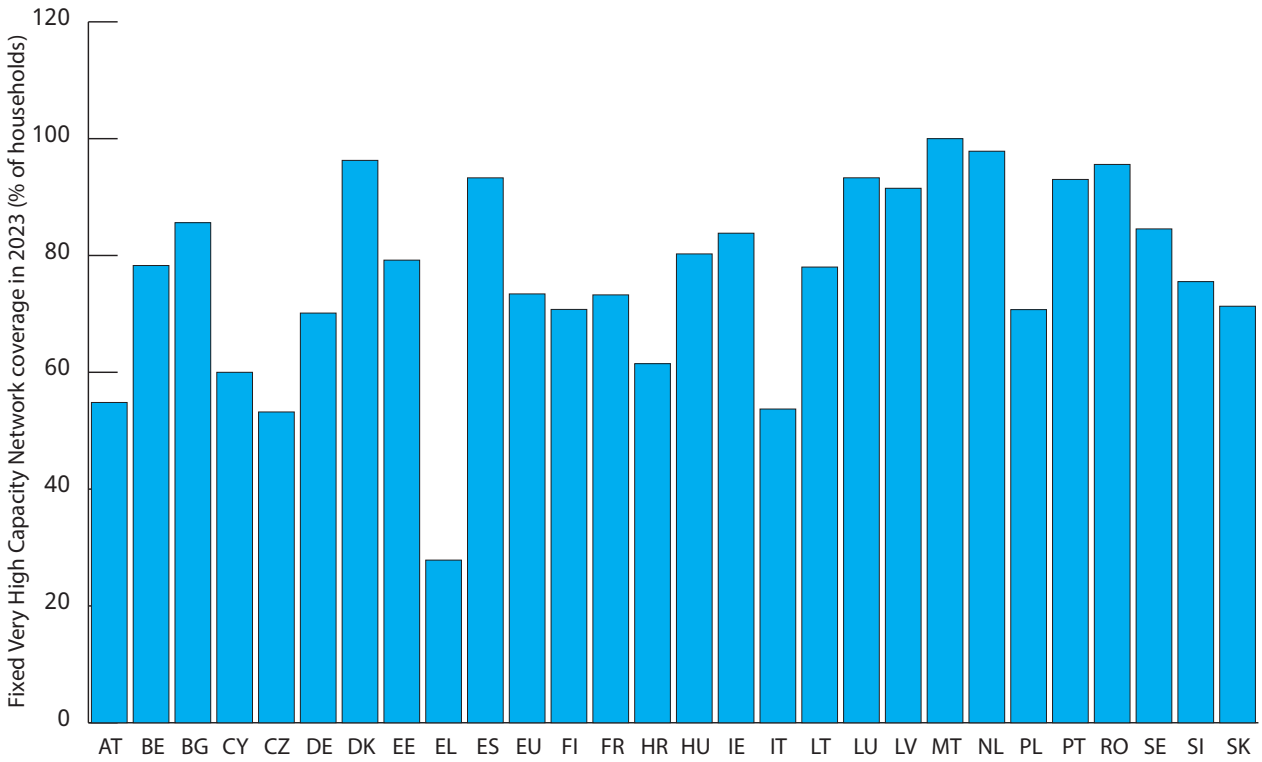
Coverage is only one issue – network quality is another. For example, while 73 per cent of households have access to so-called fixed very high capacity networks (as defined in Chart 3 above) only 56 per cent of that represents access to full-fibre networks. Only full-fibre networks are future-proofed: they use optical fibre all the way to the customer's home, and are theoretically capable of delivering nearly unlimited internet speeds. In countries like Germany only 19 per cent of the population currently has access to a full-fibre network.

On the mobile side, there remain many concerns about the quality of 5G coverage. The Commission has focused its targets solely on securing network coverage rather than also assessing quality issues like network reliability and download speeds. This has encouraged mobile operators to focus on upgrading 4G base stations, instead of installing 5G standalone.[63] The '4G upgrade' approach means that the 5G network merely piggy-backs off the 4G network and uses much of the same infrastructure. The consequence is that the '4G upgrade' approach delivers less reliability and security. It does not as easily support large numbers of devices, contributes to battery drain in end-user equipment, has less network responsiveness, provides less ability to provide dedicated capacity and services for particular customers, and limits coverage, when compared to installing 5G standalone. It is also less sustainable, since 5G standalone can significantly reduce networks' energy consumption. Simply put, upgrading 4G base stations will not, by

61: European Commission, 'Report on the state of the Digital Decade', 2023.
62: European Central Bank, 'Digitalisation in Europe 2022–2023: Evidence from the EIB Investment Survey', 2023.
63: In August 2023, only 10 out of 114 operational 5G networks in Europe were '5G SA': Telefonica, 'Competitiveness and the state of digital communications in Europe in 2024', February 6th 2024.

itself, deliver 5G's full economic potential.[64] Take device numbers. Standalone 5G networks can support 1 million devices per square kilometre, compared to only 2,000 with advanced 4G networks. So only 5G standalone will be able to support widespread use of internet-connected consumer devices, or the mass deployment of industrial sensors to enhance manufacturing productivity. 5G standalone is a platform for innovation. European mobile operators will have to install 5G standalone infrastructure or they will quickly see European networks be significantly less useful for innovators than networks in China and the US.

Chart 4: Many EU countries are falling behind in rollout of fast broadband



Source: EC, DESI 2023 indicators.

The Commission has taken practical steps to help boost investment in connectivity. These include:

★ The 2014 Broadband Cost Reduction Directive,[65] which aimed to improve rollout of new networks by allowing telecoms companies to use utility and transport infrastructure (such as pipes and towers) to deploy new digital networks. The Directive will soon be replaced by the Gigabit Infrastructure Act: a regulation which the Commission intended to further boost rollout, for example by allowing mobile operators to install new infrastructure without permission if authorities take too long to issue permits.

★ The 2018 European Electronic Communications Code.[66] Among other things, the Code adjusted the previous rules requiring telecoms operators to share assets, in order to encourage operators to build more of their own infrastructure.

★ A 2022 Commission decision establishing its Digital Decade Policy Programme. The policy sets targets for digital connectivity such as 5G and fixed broadband access, to be achieved by 2030. The Commission periodically reports on progress towards these targets.

★ Making significant public funds available for connectivity, for example through the European Regional Development Fund, the European Agricultural Fund for Rural Development, the InvestEU programme which aims to unlock investment in the EU's top policy priorities, European Investment Bank loans, the Connecting Europe Facility which provides funding for growth and competitiveness, and through member-state funds.

64: See WIK Consult, 'Investment and funding needs for the Digital Decade connectivity targets', 2023 and, 5G Observatory, 'Biannual Report', October 2023.

65: Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks.

66: Directive 2018/1972 establishing the European Electronic Communications Code.

The Commission recently updated its guidelines on how member-states can use public funds to support the rollout of broadband networks.

Yet these initiatives from the Commission have not always been matched by similar political determination by member-states. Take the Gigabit Infrastructure Act. The proposal was announced by the Commission after a review concluded that many member-states failed to implement its predecessor, the Broadband Cost Reduction Directive, properly. But member-states have watered down the Commission's proposal. For example, they softened the proposed rules that would have allowed operators to install network equipment without permission if local authorities took too long to decide whether to grant a permit.[67] Such changes will undermine the Act's effectiveness, causing continued unnecessary administrative delays and costs for telecoms firms trying to expand their networks – and allowing member-states to take different approaches. Similarly, the Commission has used 'toolboxes' – sets of policy and legal tools – as soft law measures to cajole member-states into taking steps to improve network rollout. However, member-states have done a poor job of implementing them consistently, often because permits are granted by municipal authorities, making even national consistency difficult to achieve.

Finally, even less impressive results have been achieved in deploying other types of necessary infrastructure like data centres, supercomputers and cloud computing infrastructure. For example, the Commission's aim is that in 2030 Europe will have 10,000 'edge nodes'. Edge nodes offer a compromise between traditional computing (where users have data storage and processing power on-site) and cloud computing (where these functions are centralised in global data centres). Edge nodes provide storage and processing close to where it is needed in order to improve security (since not all data needs to be sent to a central cloud or data centre) while increasing data processing speeds. For example, sensors in factories could send data to a central node which can monitor, analyse and adjust the facility's energy use, without needing to send it to a distant data centre. Yet the EU is yet to see any wide-scale deployment of this infrastructure.

There is an opportunity to revisit these problems in 2024: Commissioner Thierry Breton is about to launch a white paper to shake up the sector and adopt "a more comprehensive approach" to ensuring infrastructure can be deployed quickly.[68] The ideas could then be taken forward by the next Commission in a mooted 'Digital Networks Act'. The next Commission should ensure the white paper and the Digital Networks Act put more pressure on member-states to accept measures that would make infrastructure rollout cheaper and faster. The Commission should take inspiration from the recent Net Zero Industry Act, which speeds up and simplifies permitting for technologies necessary for the green transition – and should aim for a similar level of action to push forward the digital transition. Measures should not merely facilitate more telecoms networks, but also help reduce regulatory barriers for other types of digital infrastructure like data centres and edge nodes.

Recommendation 8

The next Commission should continue to push member-states to remove regulatory barriers to the deployment of digital infrastructure across Europe – including both connectivity and newer types of digital infrastructure like data centres and edge nodes.

Does Europe's telecoms market structure support investment?

Telecoms companies are also asking broader questions about whether market structures and commercial arrangements in Europe limit investment in digital infrastructure. They complain, for example, that competition in Europe is ineffective, with an excessive emphasis on the short-term and too little on long-term investment as a competitive differentiator. These companies argue that allowing more in-country mergers would make their networks better utilised, boosting efficiency and therefore promoting more investment. The companies also point out that large digital content providers – like Amazon, Apple and Netflix – are deriving huge profits by piggy-backing off the investments of far-less-profitable telecoms companies. In the telecoms companies' view, large content providers should help pay telecommunications players for infrastructure. These two debates – which might be explored in the Commission's upcoming telecoms white paper – have been polarising and raise complex questions. These include how policy-makers would in practice ensure that the costs of less competition were outweighed by benefits to infrastructure investment. Policy-makers should also be wary that lack of demand appears to be a factor driving slow rollout of some infrastructure.[69] In-country mergers

67: Théophane Hartmann, 'EU policymakers clinch toward agreement on broadband law', Euractiv, February 1st 2024

68: Thierry Breton, 'A 'Digital Networks Act' to redefine the DNA of our telecoms regulation', LinkedIn, October 10th 2023.

which might increase prices are therefore a double-edged sword: they might boost the business case for better rollout in some cases, but higher prices could also dampen demand for services, which would have negative impacts for investment. Getting the balance right will be tricky. Rather than adopt a new standing policy, the Commission will in any event continue to examine impacts of mergers on a case-by-case basis, by looking at the evidence.

As a policy stance, the Commission should instead focus on encouraging consumers and businesses to take up new digital technologies, so that telecoms companies will see a better business case for investing in infrastructure to support those technologies. The Commission should also review telecoms regulations to ensure they are technologically-neutral and do not impose disproportionate costs on telecoms firms. For example, when telecoms firms offer services like voice calls and SMS, they should not face more burdensome regulatory compliance obligations than tech firms which offer similar services like internet-based instant messaging.

"While the telecoms sector has been governed by EU-wide rules for many years, there are still areas where telecoms operators must negotiate individual member-state laws and regulations."

The next Commission should also explore how to encourage more pan-European operators. Pan-European operators could make the European telecoms markets vastly more efficient, by giving operators access to more scale, compared to the current situation where most operators only provide services in relatively small national markets. Pan-European integration deserves broad support and has the potential to help unlock significantly more investment.[70]

One reason why few pan-European operators have emerged is that, while the sector has been governed by EU-wide rules for many years, there are still many areas where telecoms operators must negotiate individual member-state laws and regulations. This drives up costs and complexity and prevents operators enjoying EU-wide economies of scale – and operators, and potentially other players, providing connectivity services across the EU. Examples include:

★ Authorisation and access – despite increasing efforts to create EU-wide consistency, it is still up to national telecoms regulators to set local conditions for operating (in areas like consumer protection) and to determine how smaller telecoms firms can use the services and infrastructure of dominant players. The rules for operating and obtaining access to other firms' infrastructure should be made more consistent across the EU. Revised telecoms laws could also go further in promoting shared use of passive infrastructure like phone towers – which can drastically reduce the cost of rolling out competing networks, without undue negative impacts on innovation and competition.

★ Roaming and intra-EU surcharges – while the EU has mostly eliminated inter-EU roaming charges for consumers, operators in the EU still pay roaming rates to each other, and users can get slugged with surcharges for calling or texting someone in another EU country. Pricing reforms might, at least in some cases, promote a more integrated EU-wide market. However, any proposal to revisit these rates and fees needs to be evidence-driven, consider carefully the impacts on operators' revenues, and needs to be part of a broader package of reforms to the regulatory framework to make it easier for companies to operate across the EU. Recent moves in the Gigabit Infrastructure Act do not appear to be evidence-driven and risk driving down telecoms firms' revenues without commensurate steps to make pan-European operations easier.

★ Radiocommunications – currently member-states retain control over when and how to reallocate spectrum, including when to take spectrum bands away from lower-value users (such as wireless microphones and television broadcasting) so they can be used for 5G and future mobile networks. Many member-states have, however, delayed making reallocation decisions. In an effort to mitigate this problem, the 2018 European Electronic Communications Code obliged member-states to reassign certain spectrum bands to 5G in 2020. However, some member-states missed this deadline, and many had not assigned all the required spectrum even by October 2023.[71] There are good reasons for the EU to take more responsibility for spectrum policy – or at least to require member-states to better align spectrum bands across the EU. The Commission may be less politically beholden than national regulators to incumbent radiocommunication users who need to be shifted to other spectrum bands in order to allow more 5G, for example. The Commission should also discourage the use of spectrum auctions as a revenue-raising exercise for national governments, and instead auctions could be used to allocate spectrum to telecoms companies that promise to deliver the fastest and widest network rollout. Member-states could give operators longer-term spectrum licences, so they have more certainty and more time to earn a return on their investments. Given most

69: European Court of Auditors, 'Special Report: 5G roll-out in the EU', 2022.

70: Théophane Hartmann, 'Telecoms: Commission mulls market deregulation, infrastructure resilience, spectrum governance', Euractiv, December 20th 2023.

71: 5G Observatory, 'Biannual Report', October 2023.

countries already have a good degree of competition between mobile operators, the Commission should also encourage spectrum auctions to be non-discriminatory and give all firms the same opportunities to bid – rather than seeking to shape the market, by ensuring a minimum number of winners.

★ Cybersecurity and lawful intercept – the Commission and member-states launched a 'toolbox on 5G cybersecurity' setting out measures to address cybersecurity risks with 5G, such as a framework that could be used to assess the risk profile of equipment vendors like Huawei. However, different member-states have adopted widely different approaches to managing high-risk vendors, and over different timescales. Uncertainty about how high-risk vendors would be treated has made firms in some countries unwilling to invest in rollout – fearful that they may later be exposed to costs for having to replace their equipment. Furthermore, in areas like authorities' ability to access telecoms firms' records for law enforcement purposes, member-states' practices and procedures vary dramatically. If the Commission could take more of a leadership role, telecoms companies would get more clarity, certainty and consistency across the EU.

These issues all limit a true single market for digital connectivity in the EU. The differences in member-states' approaches mean that operators – and potentially new players who will rely on operators' infrastructure – cannot coordinate rollouts, their product offerings, or business practices across the EU. This helps explain why few telecoms firms provide services across multiple EU countries. Harmonising policies may be technically and commercially complex and politically sensitive. But it is an essential step to supporting Europe's digital ambitions – enabling telecoms firms to scale, find efficiencies and boost their investment.

Recommendation 9

The Commission should prioritise delivering a true single market in telecommunications, for example through better harmonisation of regulations in technically or politically difficult areas like radiocommunications. The proposed 'Digital Networks Act' should be a priority for the next Commission, focused on cutting red tape, deepening the EU telecoms market, improving the environment for investment and ensuring competition drives operators to deploy new technologies.

Conclusion

Given its aging population and the increasing industrial challenges posed by China and the US, Europe must accelerate efforts to foster its digital economy. These efforts should centre on helping European firms adopt technology and giving innovative European tech firms the best chance of success. This is a long-term project. The current Commission has laid out helpful targets – covering areas like business use of new technologies, digital skills and infrastructure deployment – and has made good progress in many areas.

But the next Commission still faces an enormous challenge in helping the EU unlock its digital potential. One is a lack of digital skills. Regions with digitally skilled workers are better at adopting new technologies – but the EU's aging population means that this will remain a problem. Another is lack of capital: a significant reason for US success in the tech sector is its pool of investors willing to make long-term and high-risk investments to push innovation forward. Addressing these problems comprehensively will require long-term reforms over successive Commissions.

This policy brief focused on three key planks of the EU's digital vision where some improvements could be achieved relatively quickly: improving tech regulation to increase commercialisation and uptake of technologies; unlocking the data economy; and ensuring European firms are not held back by inadequate digital infrastructure. In all these areas, the next Commission's best chance of success is to build on the EU's strengths. These include its values-driven approach to building trust in technology; its single market which helps build opportunities for European businesses; and its open approach to trade, which helps European firms thrive by improving their access to global markets and allowing them to grow by using the best technologies available.

Zach Meyers
Assistant director, CER

February 2024

This policy brief was written thanks to generous support from Europe Unlocked. The views are those of the author alone.

Annex: List of recommendations

Tech regulation

1. The next Commission should focus on ensuring the existing digital rulebook is properly implemented and enforced, before considering significant new regulatory obligations. It should also undertake a simplification and rationalisation exercise. This exercise should assess and address gaps, overlaps and inconsistencies in the EU's many recent digital laws.

2. The Commission should consider whether existing digital laws could be recast to deliver more future-proofed and principles-based regulation, including an appropriate role for self-regulation and co-regulation.

3. The Commission should consider ways to promote more centralised implementation and enforcement of the EU's digital laws, and limit the scope for member-states to supplement or diverge from EU-wide rules.

4. The EU's digital regulations should focus on maintaining open markets – encouraging European firms to adopt the best technologies available, and helping ensure that European tech companies have access to a global marketplace.

Data economy

5. The Commission should engage with the European Data Protection Board to encourage the Board's new data anonymisation guidelines to be comprehensive, proportionate and risk-based.

6. In its evaluation of the GDPR, the Commission should consider amendments to help ensure the law is interpreted and applied consistently across the EU.

7. In the Commission's evaluation of the GDPR, it should consider whether the original intention to create a proportionate and risk-based approach to data protection is being maintained – and, if not, propose amendments to re-emphasise this principle.

Boosting connectivity

8. The next Commission should continue to push member-states to remove regulatory barriers to the deployment of digital infrastructure across Europe – including both connectivity and newer types of digital infrastructure like data centres and edge nodes.

9. The Commission should prioritise delivering a true single market in telecommunications, for example through better harmonisation of regulations in technically or politically difficult areas like radiocommunications. The proposed 'Digital Networks Act' should be a priority for the next Commission, focused on cutting red tape, deepening the EU telecoms market, improving the environment for investment and ensuring competition drives operators to deploy new technologies.