NGI FORWARD

A VISION FOR THE FUTURE INTERNET

WORKING PAPER

September 2020

NEXT GENERATION INTERNET
INTERNET OF HUMANS

AUTHORS

Katja Bego,
contributions by **Markus Droemann**

Original illustrations by: **Isabel Sousa**
https://isabelsousa.com/
Report design by: **Emma Charleston**
https://www.emmacharleston.co.uk/

ABOUT NGI

NGI Forward is the strategy and policy arm of the Next Generation Internet (NGI), a flagship initiative by the European Commission, which seeks to build a more democratic, resilient and inclusive future internet. The project is tasked with setting out an ambitious vision for what we want the future internet to look like, and identifying the concrete building blocks - from new technologies to policy interventions - that might help bring us closer towards that vision.

NGI Forward is made up of an international consortium of seven partners: **Nesta** in the United Kingdom, which leads the project, **DELab** at the University of Warsaw in Poland, **Edgeryders** in Estonia, the **City of Amsterdam** in the Netherlands, **Nesta Italia** in Italy, **Aarhus University** in Denmark and **Resonance Design** in Belgium. The NGI Forward project commenced in January 2019 and will run for three years. To learn more or get involved, visit **http://research.ngi.eu**.

A VISION FOR 2030

The European Commission's ambitious Next Generation EU recovery plan[1] aims to not just kickstart economic growth and boost employment, but also use this moment as an opportunity to catalyse the digital and green twin transition. The internet and its supporting technologies will be instrumental in making these efforts a success, but we cannot harness its full power unless we solve the underlying, systemic issues currently holding it back. **This paper sets out an ambitious vision and mission framework to create a more democratic, resilient, sustainable, trustworthy and inclusive internet by 2030.**

There is no single silver bullet solution that can help resolve all the challenges presented by connected technologies and the digital economy. We instead need a wide variety of interventions to reach our objectives, targeting issues across all layers of the internet's stack – from its underlying physical infrastructures to the ways in which information flows through the system and impacts our societies. We propose unifying the ambitious objectives of the Next Generation Internet initiative into one single mission, to sit alongside the ambitious missions previously defined by the European Commission.[2]

Taking such a mission-based approach will empower policymakers and the public sector to take a holistic view, articulate a compelling European story, and mobilise the right actors in Europe's diverse technology ecosystem to bring about the changes we want to see.

We focus our efforts on five key pillars:

1. **Democracy:** Power over the internet is concentrated in too few hands. Citizens should have more ownership over their own personal data and identity, and a real voice in the development of new innovation. Building a more democratic internet also means levelling the playing field in the digital economy, allowing more actors to meaningfully compete, and initiatives that serve the public interest to thrive.
2. **Resilience:** A human-centric internet also needs to be resilient in order to ensure the continued reliability and sustainability of its networks and social infrastructures. Mounting cyberthreats and governance breakdown, climate shocks and rising demand impact different layers of the system, and require renovation and more secure processes to remain robust.
3. **Sustainability:** If we want the internet and related digital technologies to play a role in solving the climate emergency and further the objectives of the European Green Deal, we need to ensure we minimise their own environmental footprint and advance the circular economy for digital devices.
4. **Trust:** From reading an article on social media to making an online payment – trust in and on the internet is vital if we want to make most of its promise. Europe needs more trustworthy models for online interactions, reliable information, data-sharing and identity management, to both help strengthen social cohesion and ease growing distrust in the geopolitical arena.
5. **Inclusion:** The internet needs to be accessible to all. This means removing social, economic and infrastructural barriers to access, but also the development of a flourishing multilingual internet, where services are available and safe to use for underrepresented communities.

Challenges: We have to address complicated and interconnected challenges across all layers of our power stack model.

[1] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1658
[2] https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme/missions-horizon-europe_en

	Democracy	Resilience	Sustainability	Trust	Inclusion
Physical infrastructure and hardware layer	Privatisation of infrastructure. Loss of the Right to Tinker and restrictive ownership models. Market concentration in supply chains	Vulnerability of infrastructures to cyberattacks and climate shocks Arms race over resources Weak governance of cyberspace	Environmental footprint hardware Lack of recyclability and right to repair Path dependency and lock in.	Geopolitical tensions Supply chain dependencies Eavesdropping and tapping of communications	Lack of Affordable broadband access Urban / rural digital divide Socio-economic barriers to access
Standards, protocols and internet governance layer	Internet governance dominated by a small number of actors. Increased complexity and opacity of governance processes	Limited governance of (cyber)security issues. Take-up of critical patches and improvements	Lack of focus on sustainability objectives in standard setting process	Fragmentation and emerging splinternet. Breakdown of governance processes	High barriers to entry for participating in governance processes Lack of representation of diverse voices
Data & transport layer	Concentration of power over data Surveillance capitalism and surveillance states	Data breaches and single points of failure Weaponisation of large data lakes	Environmental footprint of storing and processing data Data minimisation	Data collection processes are opaque, not consent-based and infringe on citizens' privacy.	Biases in algorithmic decision making Right to Opt Out and Representation
Technology and software development layer	Unequal access to talent Power balances means tech for good does not come to fruition	Democratisation leading to development of harmful solutions	Proliferation of energy-intensive smart devices Energy use of Blockchain and ML	Lack of robustness in development processes Government surveillance creep	Lack of diversity in tech industry Groups under-represented in tech development
Applications layer	Walled gardens siloing off the internet, and setting the rules User lock-in and network effects	Fragmentation in rule-setting approaches due to walled gardens Fragility adtech business models	Growth of more energy-intensive uses of the internet, such as video streaming	Identity problem and lack of trust in online interactions Lack of transparency about workings of apps	Lack of accessibility and linguistic diversity in applications and services Service shutdowns
Information layer	Power of platform gatekeepers and other intermediaries Online censorship	Fragility of the online media ecosystem	Information overload Inefficient design and SEO practices	Disinformation and fake news Emergence of deepfakes	Online harassment and abuse Multilingual internet and access to info
Societal impact layer	Power of digital economy over physical businesses Augmented neutrality	Fragility of the barely-holding-on economy Untethering from physical space	Incentivising unsustainable consumerism Not making use of full opportunities	Meaningful consent and encroachment on public space Smart city accountability	Growing digital divide Inequalities perpetuated by lack of access

A Mission and a Vision: We define a specific mission for each of our five pillars, setting tangible goals to move us closer towards our vision.

DEMOCRACY:

- We democratise the internet by giving citizens control over their data and future trajectory of innovation, and create a single market for ethical data use and technology worth 1 trillion Euros by 2030.
- Every European gets access to their own secure digital identity and personal data store (data wallet) by 2025.
- We level the playing field in the digital economy by opening up access to data through the creation of commons-driven decentralised data spaces for personal data as well as strengthening interoperability and data portability rules.
- We democratise the technology innovation process by supporting open innovation and knowledge, and harnessing the wisdom of the crowd through collective intelligence.
- We rejuvenate democratic processes across all layers of governance, from the local level all the way up to the European institutions, by proactively implementing digital deliberation tools, and protect freedom of speech and the Right to Whisper around the world.

SUSTAINABILITY:

- We move to a fully circular and carbon-neutral economy for digital technology by 2030, strengthening the joint objectives of Europe's twin green and digital transition.
- We move to a fully circular economy for digital devices by 2030, by improving production processes, ensuring longevity and repairability of individual devices and expanding our e-waste recycling capacity.
- We reduce the energy use of the data economy by raising awareness among the public about the impact of their use, extending data minimisation practices to include sustainability measures, and developing less energy-intensive technologies and data analysis methodologies.
- Europe becomes a global frontrunner in the market for green digital devices, software and technologies, the backbone of a market for trustworthy technology worth 1 trillion Euros by 2030.
- Seizing on the twin digital and green transition, we invest in digital technologies that can meaningfully help address the climate crisis, a central tenet of the European Green Deal.

RESILIENCE:

- We build internet infrastructure and systems that can withstand environmental, economic and cyber shocks, and strengthen our role as a global champion of good governance and the open internet.
- We transition to a model of open-source technology and open standards first across all layers of European governance, from the local to the supranational.
- We play an active role in strengthening global governance of the internet, by opening up internet governance processes to a wider community, reviving the multi-stakeholder model and protecting global digital rights.
- We roll out an ambitious infrastructure renewal plan as part of Europe's Green New Deal plans, protecting critical infrastructures and building in more flexibility to leave us agile to adapt to changing threat horizons.
- We build up Europe's cybersecurity capacity through an ambitious retraining programme, building skills within organisations and among the general public, and strengthening the rules for secure design and deployment.

TRUST:

- We establish a globally-recognised "Made in Europe" brand for trustworthy and privacy-enhancing technology, and play a leadership role in ensuring citizens around the world have access to trustworthy technology, data and information flows.
- We launch an auditing body that scrutinises the security, trustworthiness and privacy-awareness of hardware, software and digital services, and administers European Commission-endorsed trustmarks to those solutions that pass the test.
- We build a healthy ecosystem around trustworthy, high-quality journalism and information flows, ensuring reputable media outlets can find sustainable business models without undue levels of market concentration. We do this through the creation of a dedicated News Innovation fund.
- We relocate and diversify aspects of the internet technology supply chain, bringing more development of devices and solutions back to Europe.
- We find new modes for citizens to give meaningful consent to being tracked or subjected to data-driven decision-making tools and systems, bringing reciprocity to our relationship with smart city solutions.

INCLUSION:

- By 2030, all Europeans can meaningfully access and participate in shaping the internet.
- We ensure all European have the opportunity to get affordable, high-speed internet access by 2030, and have the skills to safely and effectively use the internet.
- We broaden access of more marginalised groups across all layers of the internet, with a particular emphasis on making the internet governance and technology development layers more inclusive and diverse.
- We build a multilingual internet, where minority languages are equally well-represented and all services accessible.
- We reduce barriers to access, by improving the accessibility of services for people with disabilities, and address the cultural and socio-economic dynamics that mean marginalised groups are less likely to participate.

TABLE OF CONTENTS

1. INTRODUCTION

1. INTRODUCTION

The internet has changed. While early internet pioneers dreamed of an open, free and decentralised internet, the story of the internet today is mostly a story of loss of control. Just a handful of companies determine what we read, see and buy, where we work and where we live, who we vote for, who we love, and who we are. Many of us feel increasingly uneasy about these developments. We live in a world where new technologies happen to us, rather than for us; a world in which citizens have very little agency to change the rules.

As the internet and digital economy now permeate more and more layers of our societies and economies, it is no surprise that vested interests have increasingly used them as channels through which to spread their own influence, and conversely also have used their influence to take charge of shaping the internet itself. The internet has become one of the main theatres of geopolitical conflict, with governments and increasingly powerful private-sector actors embroiled in an accelerating tech arms race, vying for control. At time of writing, the emergence of the long-feared splinternet appears closer than ever before.

This ongoing battle for domination has led to an extreme centralisation of power across virtually all layers of the internet, with a small number of players now calling the shots in shaping its underlying systems, such as physical infrastructures, standard-setting processes and data flows, and using this power to rewire our societies and economies. The business models and governance systems enabling this current incarnation of the internet have a natural tendency to lead to ever greater accumulation and centralisation. This winner-takes-all dynamic makes it increasingly difficult for new actors to meaningfully compete, especially those who want to address some of the internet's structural inequalities and power imbalances.

This tendency towards accumulation and ever greater scale has repercussions for the resilience and environmental sustainability of the systems and services we increasingly rely on, excludes large swathes of the population from meaningfully contributing to – or benefiting from – innovation, and exacerbates existing social, economic and political divides.

Despite the growing clamour of voices who wish we could just pull the plug, we believe that the internet is still a force for good. But now more than ever, we must work hard and take decisive action to harness its full potential. The COVID-19 crisis has revealed the many inequities and vulnerabilities in the system, and risks cementing them even further, but it has also shown us once again how powerful a tool the internet can be. It allowed us to connect, share knowledge and come together when the physical world temporarily prevented us from doing so. As Europe sets out on its path towards recovery, to rebuild communities and economies ravaged by the pandemic, we now have a vital opportunity to make the internet a healthier part of a more sustainable shared future.

This renewed sense of urgency to rebuild and right some of the pervasive wrongs in our societies also gives us the momentum to address the underlying dynamics that underpin so many of the internet's current problems. To do that, we need to become better not just at diagnosing the issues, but coming up with remedies. We know what we do not want. But what kind of internet do we want to see instead? This paper is an attempt to make our ambitions more concrete, by setting out a **coherent vision for a more democratic, resilient, sustainable, trustworthy and inclusive future internet by 2030**, and by outlining a roadmap of tangible actions and interventions that could help get us there. This vision serves as a call to arms to move away from our role as passive bystanders to proactively shape a better future; from defining principles to taking tangible action.

This working paper was developed by Nesta as part of the Horizon-2020-funded NGI Forward project. NGI Forward acts as the policy and strategy arm of the European Commission's flagship Next Generation Internet (NGI) initiative[3], which sets out to build a more human-centric internet by the end of the decade. While the paper does not necessarily reflect the opinions of the Commission, it forms part of our project's overarching recommendations for the NGI and future European internet policy.

1.1 EUROPE'S ROLE IN SHAPING THE POST-COVID-19 INTERNET

Europe has often been presented as one of the lone powerful voices still championing digital rights and the open internet in an increasingly fragmented digital sphere, a third way between Silicon Valley and Beijing. While this has proven a helpful heuristic to articulate an alternative and strike the right balance

[3] https://www.ngi.eu/

between unbridled private sector-led innovation and government oversight, the reality is a lot more complex. Much like the world around us, the internet is becoming increasingly chaotic and multipolar, with a multitude of actors, private and public, trying to transpose their own visions for the future onto it.[4]

Amidst these duelling narratives and objectives, the European Union needs to more proactively chart its own path. We must become better at articulating what we want, rather than diagnosing (and regulating) what we do not want to see. As global tensions rise, globalisation stagnates, and existing economic and political paradigms are challenged as a result of the impacts of the pandemic and the longer-term threats of climate change and inequality, Europe finds itself at an important crossroads. It is perhaps no wonder that this is to be the first 'geopolitical' Commission, as President Ursula von der Leyen has described it.[5] Indeed, this is not a time to stand idly by.

Driven by fears of falling behind, a growing number of voices in Europe are promoting rash approaches to bolster the bloc's own industrial strategy: rapidly creating national champions ("picking winners") and diverting large amounts of funding to support the most hyped technologies, such as artificial intelligence, with ethics an afterthought. While it is indeed important that Europe boldly invests in taking the lead in shaping newly emerging industries, **this rush to compete should not come at the expense of championing European values, one of our unique strengths.** Conversely, our value-led approach should also not lead to inaction, where the development of ethics frameworks and principles can sometimes get in the way of taking tangible steps forward and building alternatives. We instead advocate for a long-term approach geared towards setting the right conditions for new public-interest innovation to thrive; an approach that aims to embed the values we hold dear into our infrastructure and the next generation of technologies that will form the future backbone of the internet.

As the European Commission's launches its ambitious Next Generation Europe programme, aimed at ensuring the post-pandemic recovery is both digitally-focused and sustainable, while also pursuing greater sovereignty in the technology space ("open strategic autonomy")[6], we are offered a critical opportunity for Europe to look beyond the value of individual technologies and explore how the internet, as a whole, could be reconfigured to generate greater economic and societal value and facilitate long-term growth within planetary bounds.

1.2 A COHESIVE EUROPEAN APPROACH

The European Union's strengths in the digital arena are well known, from our regulatory power – the sheer size of the Single Market and strict standards mean the bloc gets to set global rules, harnessing the so-called Brussels effect[7] – to our reputation as a trustworthy, value-led actor, to the dynamism of our bottom-up innovation ecosystem.

The European Union's role as the global technology watchdog and champion of openness in an increasingly fragmented system, while powerful, ultimately risks being a reactive one. Regulatory interventions such as the GDPR are vital, but are there to right existing wrongs in the system. In their current incarnation, they are predominantly a lever to get outside actors to adapt to the rules of the European Single Market, rather than to successfully incentivise innovation of our own.

But internet sovereignty, both on the individual and continental level, can only be achieved through taking charge of the future trajectory of technological development and building our own alternatives. Our rule-setting power, from the European Commission down to the city-level, is not being optimally used to support the creation of a market for solutions that could help correct some of the excesses and fundamental inequalities currently present in the digital economy.

Building the systems for public-interest innovation to thrive

Many of our existing efforts have focused on either using regulation to push technology giants in a direction we consider more favourable, or to try to build – so far fruitlessly – similarly centralised alternatives to these large incumbents. But our ambition should not be to create our own European Google. Instead, we need to focus on setting the conditions that prevent the next Google.

In this paper, we set out a new model for an EU-

[4] *Four Internets by Kieron O'Hara, Wendy Hall - Communications of the ACM, March 2020, Vol. 63 No. 3, Pages 28-30 https://m-cacm.acm.org/magazines/2020/3/243022-four-internets/fulltext*

[5] *https://www.politico.eu/article/meet-ursula-von-der-leyen-geopolitical-commission/*

[6] *https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940*

[7] *Bradford, Anu, The Brussels Effect (2012). Northwestern University Law Review, Vol. 107, No. 1, 2012, Columbia Law and Economics Working Paper No. 533, Available at SSRN: https://ssrn.com/abstract=2770634*

funded and maintained standards-based framework (A European Democratic Data Space Framework) for data-sharing and online identity, which will help democratise access to data while preserving citizens' privacy, enabling smaller companies to gain a foothold in the market and operate sustainable, ethical business models. Building such a new, decentralised but robust infrastructure is but one example of how Europe could break through the vicious circle towards ever more power accumulation by allowing all of us to participate on our own terms.

Government as a market-creator

Public procurement – the process of public authorities, such as national ministries, municipal governments or indeed the European Commission itself purchasing goods or services from companies – makes up about 14 per cent of European GDP.[8] From smart transport systems to digital education solutions or online ticket payment systems: spending on technological innovation and digital services makes up a significant share of this total. Government spending and investment of this kind means that the public sector is a crucial player in the market for innovation – we must get better at using this power to our advantage.

By combining proactive procurement with forward-facing, bold regulation, governments can set standards for the technology and innovation they want to see. Think for example of conditions for interoperability and data portability, fairness or privacy protection. Steering the development of new solutions in this way also helps governments themselves to become a market for responsible alternatives which would otherwise find it difficult to find a sustainable path to profitability.

Empowering policymakers from the local level up

Europe's ambitious new digital agenda must not solely be a top-down exercise driven forward by the European Commission alone. Instead, we need to involve Europe's rich and diverse ecosystem of actors shaping and reflecting on the future of the internet – from large industry players to civil society; academia to startups. We do that by setting out an ambitious mission, focused on mobilising key stakeholders all over the continent. Policy actions need to be spearheaded by actors across all levels of governance: from experimentation within cities and local communities, to bold, shared regulatory action in Brussels.

In Europe, many of the most interesting developments happen from the bottom-up. From cities taking back control, to grassroots initiatives building ethical tools. We need to bring coherence to these many disparate activities, champion collaboration and put communities and the creation of an inclusive, open innovation ecosystem at the heart of our approach.

Bringing this type of cohesion is no lofty task. Because while Europe's digital innovation ecosystem is stronger than it is sometimes presented, it is also incredibly fragmented. It remains difficult for businesses to find a market beyond their own national borders as they are forced to adapt to differing regulatory and cultural contexts, and a lack of coordination between the various actors in the ecosystem means we often end up reinventing the wheel. This is not only wasteful, but also means that it is hard for any one solution to truly gain traction. Through knowledge sharing, more coordination and shared action (what if we could harmonise procurement rules to make it easier for networks of cities and towns to purchase a new, ethical solution together?), we can amplify the impact of our proposed interventions.

Institutional innovation and new governance models

The unprecedented scale and complexity of the digital economy has meant not all of our existing regulatory and competition frameworks are still fit-for-purpose to respond to the challenges it has brought to the fore. We need to move to anticipatory regulatory models[9], where we remain more agile and responsive to the rapidly-changing nature and context around emerging technologies, and need to experiment with new forms of government oversight and collaboration with our stakeholder community.

In this paper, we propose the establishment of a number of fully independent but government-funded governance bodies, tasked with, for example, issuing trustmarks, auditing technology solutions and maintaining new trust and identity infrastructures. We believe these kinds of models could bring a new dynamism and robustness to an otherwise increasingly fraught and fragmenting internet governance arena.

From the local and city-level up to the institutions of the European Union, governments have more power than we often think to shape the future trajectory of technology and the internet. In this paper, we set out several ways in which policymakers can become market-creators rather than reactive regulators by

[8] https://ec.europa.eu/growth/single-market/public-procurement/innovative_en

[9] https://www.nesta.org.uk/project/anticipatory-regulation/

setting standards and shaping the parameters in which new technology is deployed.

1.3 FIVE PILLARS FOR THE FUTURE

Europe prides itself in its values-led approach when it comes to governing and shaping the internet: we champion digital rights, strive for inclusion and accessibility, and promote technology that can help solve real societal problems.[10] But we must also recognise that the values and ideals we hold dear can at times be in tension with each other. We champion online freedom, but not at the expense of users' privacy and safety. We want to expand access to the internet and reduce the digital divide, but are also cognizant about the environmental strain this increased connectivity would bring. These are difficult choices, and we must strike the right balance between these trade-offs, and take a consistent, coherent approach to articulate what we prioritise and value most.

Many of the most important issues we face today in our societies – climate change, inequality, political polarisation, threats to the resilience of our democracies, geopolitical tensions[11] – closely map onto the key problems we grapple with on the internet, as we found confirmed through NGI Forward's own data-driven analysis.[12] As we grapple with addressing these vital societal challenges on- and offline, we thus let the evidence inform us about which key areas to focus on. Synthesising this complexity led to the selection of five key principles that we believe a future internet must embody and embrace: democracy, resilience, sustainability, trust and inclusion. These five values, or pillars, will form a leitmotif throughout this paper, as we surface the key challenges ahead of us, and articulate a concrete vision and mission for each.

Throughout this paper, we focus on the following five pillars:

Democracy:

Power over the internet is concentrated in too few hands. Citizens should have more ownership over their own personal data and identity, and a real voice in the development of new innovation. Building a more democratic internet also means levelling the playing field in the digital economy, allowing more actors to meaningfully compete, and initiatives that serve the public interest to thrive.

Resilience:

A human-centric internet also needs to be resilient in order to ensure the continued reliability and sustainability of its networks and social infrastructures. Mounting cyberthreats and governance breakdown, climate shocks and rising demand impact different layers of the system, and require renovation and more secure processes to remain robust.

Sustainability:

If we want the internet and related digital technologies to play a role in solving the climate emergency and further the objectives of the European Green Deal, we need to ensure we minimise their own environmental footprint and advance the circular economy for digital devices.

Trust:

From reading an article on social media to making an online payment – trust in and on the internet is vital if we want to make most of its promise. Europe needs more trustworthy models for online interactions, reliable information, data-sharing and identity management, to both help strengthen social cohesion and ease growing distrust in the geopolitical arena.

Inclusion:

The internet needs to be accessible to all. This means removing social, economic and infrastructural barriers to access, but also the development of a flourishing multilingual internet, where services are available and safe to use for underrepresented communities.

1.4 THE STRUCTURE OF THIS PAPER

The purpose of this paper is to set out an ambitious vision for the European Commission towards building a more democratic, resilient, sustainable, trustworthy and inclusive internet by 2030, a vision in which Europe charts its own future and strengthens the global open internet. Realising this vision requires a radical rewiring of the internet's underlying systems, business models and infrastructures. To target these efforts well, we need to understand the full complexity of the challenges we face on the internet today. What's more, we need to make this vision tangible and empower policymakers, by setting out the concrete building blocks – from policy interventions to technological and institutional innovation – that can help get us there.

[10] https://europa.eu/european-union/about-eu/eu-in-brief_en

[11] https://carnegieeurope.eu/2019/05/07/what-are-europe-s-top-three-challenges-not-brexit-not-migration-not-populism-pub-79070

[12] https://ngi.delabapps.eu/; https://research.ngi.eu/data-lab/overview/ These two websites show data visualisations created by NGI Forward Partner DElab, detailed reports and papers available on request.

The remaining chapters of this paper are thus divided in **three parts:**

1. Where are we now:

In this section, we take a holistic view of the challenges we face today. To help us make sense of a space as interconnected, rapidly-evolving and complex as the internet, we introduce the **power stack model**, which reconceptualises the traditional technology stack to focus on the **key actors and issues** defining each layer of the system – from the physical infrastructure underpinning the internet up to its impact on our societies. We discuss the complex web of problems we need to address one layer at a time.

2. Where do we want to go:

In this section, we set out our vision for 2030 for each of our five key pillars: **democracy, resilience, sustainability, trust and inclusion**, focusing on tangible, realistic action that could be taken by Europe's innovation ecosystem.

3. How do we get there:

In this final part, we elaborate on some of the specific interventions, policy instruments and technological solutions we need to move us closer towards our vision. We do this by setting out a **Mission** for building a more human-centric internet, following the mission-based innovation model championed by the European Commission, to ensure we mobilise and optimally harness the full strength of Europe's internet ecosystem and innovative potential.

2.

WHERE ARE WE NOW

2. WHERE ARE WE NOW?

The fragmentation and eventual possible splintering of the global internet, monopoly power of a kind not seen before, the growing peril of the digital divide, lack of resilience of underlying infrastructures, unaffordable cities, unaccountable algorithmic decision-making, deliberate misinformation campaigns and cyber attacks, emerging surveillance states...

The problems we face on the internet are overwhelmingly diverse, making it hard to determine where interventions are needed.

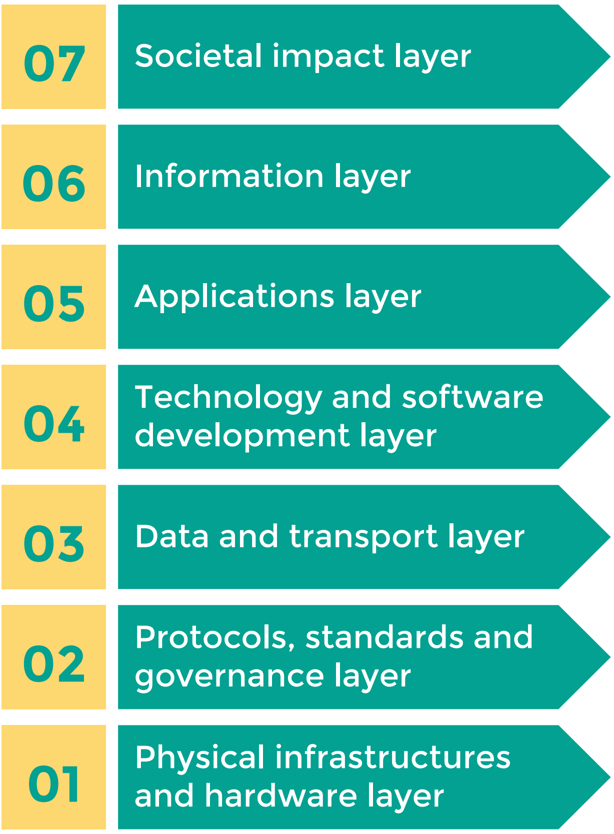
To set out a tangible vision for the future requires us to understand where we are now, and what levers of change we have available to us. What are the key hurdles we need to surmount on the road to achieving our objectives? In this section, we provide an overarching structure to consider these challenges, and identify where there are important commonalities and shared root causes we should seek to address first.

Introducing the stack model of power:

The multilayered, intertwined nature of the global internet means we need a clear picture of how the various slices and layers of the system interact, and understand who the key actors driving development are.

Many traditional models for visualising the internet, such as the well-known Internet Protocol Stack[13], looks at slices of the system solely from a technological point of view: from the physical layer and routing protocols, up to the various operating systems making the internet actually function. While this approach to visualising the various elements of the system is useful, we need to also look at the social, economic and political aspects shaping the system if we want to take a truly holistic approach to remaking the internet.

To help us better understand the complicated issues that our vision seeks to address, we therefore propose **reimagining the traditional stack as a layered system of both social and technological infrastructures.** In this model, these layers are not defined by their importance to making the internet work from a technical point of view, but by the powerful forces driving them. As we seek to build an internet that is more democratic, resilient, sustainable, trustworthy, and inclusive, we need to ensure we address these questions of power for each of these layers individually, and understand how certain dynamics and challenges flow through them and reinforce each other.



07 Societal impact layer

06 Information layer

05 Applications layer

04 Technology and software development layer

03 Data and transport layer

02 Protocols, standards and governance layer

01 Physical infrastructures and hardware layer

Figure: The layers of the power stack model for the internet

[13] https://www.w3.org/People/Frystyk/thesis/TcpIp.html

We will now go through each of the layers of the power stack model one by one, highlighting key challenges that stand in the way of achieving our mission. It is important to note the recurring themes we see emerge again and again throughout this analysis: **the self-reinforcing nature of extreme centralisation of power and resources, lack of transparent and effective governance processes, and challenges that come with increased scale and demand.**

The actors that are dominant in one layer, especially those in the applications and data layers, are becoming increasingly powerful in other slices of the system too. Large technology companies are beginning to deploy their own proprietary cables and integrated hardware solutions, flexing their muscles in the internet governance sphere, and spreading their reach outside the confines of the internet. With their influence growing both horizontally within layers and vertically across layers, the large incumbents have proven themselves particularly adept at solidifying their own positions – effectively pulling up the drawbridge to prevent smaller players from following in their footsteps and challenging their dominance. As we think about solutions to combat some of these dynamics, we need to understand the common underlying complexities fuelling them, and think about ways we can break this vicious circle towards ever-greater centralisation.

2.1 PHYSICAL INFRASTRUCTURES AND HARDWARE LAYER

We often think of the internet as immaterial; technology that just exists on our phones or in the cloud. But the internet's underpinning physical infrastructures and hardware are very much real, bound by geographical jurisdictions and finite physical resources. With the climate emergency looming over us and geopolitical tensions rising globally, questions about the system's physical resilience are now more pertinent than ever.

Democracy:

A democratic internet is an internet that offers a level playing field, where all of us can compete in a fair manner, and consumers have agency to shape their own interactions with the technologies they rely on. Unfortunately, even the physical infrastructures of the internet have developed in ways that centralise power and limit the freedom of end users to determine their digital lives and meaningfully participate or compete online.

Image credit: Ricardo Gomez Angel via Unsplash

Users have lost agency when it comes to owning their devices. The early ethos of the internet community was one of tinkering,[14] of building your own computer or server. New designs and rigid terms and conditions have made that difficult, now often preventing us from doing something even as simple as opening up our laptop to replace its battery. New ownership models have similarly changed our relationship with our hardware. Devices are increasingly vessels for software and services we rent rather than items we truly own. Once the software updates stop, smartphones and other tech rapidly decrease in utility and soon become unusable altogether even though the hardware itself is still in fine order.

A particularly notorious example of this trend is the case of American agro-tech giant John Deere, which prevents farmers from repairing their own tractors, as this would mean tampering with the proprietary software in the machine , which the company contractually still owns.[15] Cases such as this have become the subject of ongoing, complicated lawsuits about the nature of ownership, engendering a global movement in support of the 'Right to Repair'. In response, the European Commission recently announced that it would press forward with a Right to Repair for digital devices – an important first step if we want to return control over physical hardware back to users.[16]

As is the case across virtually all layers of our stack model, the physical backbone of the internet is subject to a decreasing number of actors that are dominating and rewriting the rules of the market. A notable trend in recent years sees tech giants, particularly those that rely on fast broadband for the delivery of products and services, deploying their own undersea cables and other such systems.[17] Proprietary infrastructure ensures more constant and reliable access and helps these companies create their own private networks, which increasingly bypass the internet altogether. By some estimates, private networks now use up to 60 per cent of the total capacity offered by trans-Atlantic cables, surpassing internet traffic routed through traditional means.[18] This provides a large advantage to the well-funded incumbents who can afford these more reliable proprietary systems, and also poses a challenge to net neutrality, which posits that all internet traffic, regardless of its source of origin, should be treated equally.

Market concentration has also left us with a less diversified supply of both consumer and non-consumer hardware. While globally we see more competition as more and more low-cost Chinese device producers gain traction particularly in the Global South, in Europe, the picture looks very different. Just three companies, Apple, Samsung and Huawei, cumulatively control nearly eighty per cent of the smartphone market.[19] In the race to deploy 5G, only three key producers, Huawei, Ericsson and Nokia, lead the charge,[20] together able to set the global standards for communications technology and solidify their own positions. This centralisation reflects how difficult it can be for new competitors to enter the market, particularly those hoping to compete on sustainable and ethical business models rather than cost.

The European Commission already plays an important role in challenging some of these dynamics, but can do more, for example as part of upcoming Right to Repair legislation, and through proactively opening up the market for smaller device producers.

Resilience:

As we become more reliant on the internet, with more and more of our key infrastructures now connected, the associated risk that comes with a challenge to these systems increases. Cyber-security experts warn about the lacklustre defence of everything from air traffic control towers[21] and voting machines[22] to nuclear plants.[23] The internet itself is also a target[24]. As countries around the world are building up their cyber arsenals, debilitating attacks, by both state or non-state actors, will increase in frequency and intensity.[25] A global race to control access to resources needed to build devices adds to the geopolitical tension surrounding the internet's physical systems. Risks to the system do not always have to be the product of malicious intent: more frequent extreme weather events and climate-change-induced shocks also require us to urgently

[14] https://www.eff.org/deeplinks/2016/01/why-owning-your-stuff-means-owning-your-digital-freedom
[15] https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor
[16] https://ec.europa.eu/ireland/news/New-Circular-Economy-Action-plan-shows-the-way-to-a-climate-neutral-competitive-economy_en
[17] https://www.economist.com/graphic-detail/2017/10/09/tech-companies-are-laying-their-own-undersea-cables
[18] https://www.wired.com/2016/06/google-turns-giant-internet-cable/
[19] https://gs.statcounter.com/vendor-market-share/mobile/europe
[20] https://uk.reuters.com/article/us-telecoms-5g-orders-factbox/factbox-deals-by-major-suppliers-in-the-race-for-5g-idUKKBN23O2G4
[21] https://www.govinfosecurity.com/air-traffic-control-system-vulnerable-a-1449
[22] https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/
[23] https://www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry-protected-from-cyber-threats/
[24] https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html
[25] https://www.brookings.edu/research/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/

reconsider the robustness of our infrastructures.[26]

When it comes to cyber warfare, we are still in the early days, but that should not lull us into a false sense of security. The lack of visibility over the respective capabilities of other actors makes it hard to predict how a larger attack might play out. According to some experts, a well-placed cyberstrike on critical systems could potentially do as much damage as conventional military campaigns, at a fraction of the cost.[27] The 2018 NotPetya attack gave us a taste of what this future might look like. NotPetya, thought to be the most impactful cyber attack we have seen so far, shut down critical systems across the world, crippling industries like health, banking and logistics in dozens of countries, amounting to a conservative estimate of over a total of 10 billion in damages.[28]

Weaponisation of connectivity to attack critical systems is a worryingly effective tool in the new hybrid warfare toolbox, but we also see growing concerns about the internet's own systems falling victim. Increased submarine activity around hard-to-reach undersea cables have left many countries worried about the impact of the deliberate destruction of such key infrastructures,[29] which could hamper cross-border communication systems for prolonged periods of time.

The worrying lack of governance and international agreement about what constitutes acceptable state behaviour in cyberspace further complicates the situation, as do the difficulties around attribution: many, if not most, malicious actors have been allowed to get away without consequences, increasing the risk of further escalation. The European Union, multilateral organisations and leading countries in the cyber arena urgently need to move towards deescalation and establish a clearer set of rules.

But cyber-resilience is not just the purview of states and multilateral organisations. It also requires action by businesses and individual users to ensure they protect systems where they can, and not inadvertently allow devices to lend a hand in facilitating botnet and other types of cyber-attacks.[30] A lack of awareness and public debate has left us ill-prepared, and many businesses in critical industries remain vulnerable to data breaches, espionage or DDoS attacks. According to some estimates, the cost of worldwide data breaches alone could exceed $5 trillion by 2024.[31]

Geopolitically-driven resilience risks also come into play further upstream: the global technology arms race has fuelled a scramble for resources such as rare earth minerals and lithium, all vital ingredients in the production of internet-enabled devices, from smartphones to connected cars, as well as many technologies vital to the green revolution. Critical minerals like cobalt are often mined in politically volatile countries such as the Democratic Republic of the Congo,[32] further inciting local conflict and causing risky dependencies in a vital supply chain. Today, the DRC accounts for roughly 60 per cent[33] of the world's cobalt output, but over 99 per cent of it is exported to China.[34]

This worrisome dependency affects a range of elements. China now controls 97 per cent of the global supplies of some materials, such as tungsten and molybdenum[35], (important in electrodes and steel production respectively) and has already demonstrated its willingness to weaponise this advantage. In 2010, for example, Beijing informally restricted access to rare earths to Japanese businesses over a territorial dispute, temporarily paralysing elements of their industry.[36] While this episode incentivised countries to diversify their supply chains and increase production elsewhere, we see signs of similar bottlenecks reemerging once again – with both the private sector and governments looking to secure access.[37] Our continued over-reliance on insecure supplies opens up important questions about sovereignty and autonomy: could we diversify supply chains, or improve recovery of critical materials from discarded devices? Reframing the debate in this light, achieving a more circular economy becomes not just an environmental but also a geopolitical objective.

Indeed, sustainability and resilience are closely linked. The adoption of environmentally friendlier practices will not only serve to reduce supply chain risks, they will become increasingly vital if we want to protect our internet infrastructure overall. As the impacts of

[26] *Durairajan, Ramakrishnan & Barford, Carol & Barford, Paul. (2018). Lights Out: Climate Change Risk to Internet Infrastructure. 9-15. http://pages.cs.wisc.edu/~pb/anrw18_final.pdf*

[27] *Finkelstein, Claire Oakes and Govern, Kevin H., "Introduction: Cyber and the Changing Face of War" (2015). Faculty Scholarship at Penn Law. https://scholarship.law.upenn.edu/faculty_scholarship/1566*

[28] *"Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers", Andy Greenberg, New York, Doubleday, 2019*

[29] *https://www.maritime-executive.com/editorials/the-challenge-of-defending-subsea-cables*

[30] *https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html*

[31] *https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches*

[32] *https://www.ft.com/content/c6909812-9ce4-11e9-9c06-a4640c9feebb*

[33] *https://www.statista.com/statistics/339834/mine-production-of-cobalt-in-dr-congo/*

[34] *https://oec.world/en/profile/country/cod*

[35] *https://www.wsj.com/articles/china-ends-rare-earth-minerals-export-quotas-1420441285*

[36] *https://www.nytimes.com/2010/09/23/business/global/23rare.html*

[37] *https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/lithium-cobalt-may-be-next-in-strategic-metals-struggle-between-us-china-52545818*

the climate crisis begin to manifest themselves more prominently, extreme weather events and climate-change-induced shocks will become more frequent, threatening to do great damage to fragile internet systems.[38] We must begin to more actively plan for such eventualities. Protecting internet infrastructures should thus be a key objective of the Next Generation recovery plan and the European Green Deal.

The European Union is well-placed to play a global leadership role in strengthening the governance of cyberspace, as an effective "third way" buffer between the dominant American and Chinese paradigms, and should aim to spearhead the push for cyber arms control and further explore non-proliferation treaties. To do this credibly, European countries have to work together to improve the resilience, security and sovereignty of our own key infrastructures.

Sustainability:

While we often tout digital transformation as one of the key solutions to addressing the climate emergency, we must also recognise that the internet itself is a growing source of pollution and emissions. Across the value chain, from the production processes, to the storing of data in the cloud and the energy required to power them, the average internet device's carbon footprint is substantial, especially if we consider the short lifespan of many of these products.

By far the largest share of this footprint is generated in the mining and manufacturing process. Across the lifecycle of an average smartphone, for example, from the input materials to how we use it and then finally dispose of it again, production processes account for a staggering 95 per cent of the total greenhouse emissions produced.[39] The alarming rate at which we replace our laptops and smartphones, and the parallel explosion in cheap new smart devices compound this issue, with some estimates suggesting we will reach 25 billion connected 'things' by 2021.[40]

Mapping out the footprint of a device across the full supply chain is difficult because of the extreme complexity of the production process. Over 200 suppliers are involved in the production of a single iPhone.[41] While there are many fairly straightforward interventions that could make these processes more sustainable, identifying and targeting specific actors is difficult. While there are existing efforts to clean up supply chains, there are few incentives for producers to fundamentally change their manufacturing pipelines as long as consumer awareness, industry standards and regulatory pressure remain limited.

The high rate of device replacement is in part fuelled by deliberate design choices on the side of the producer. Smartphones, laptops and other pieces of hardware are notoriously hard to repair. Company policies sometimes even actively discourage repair, since tinkering with devices is often considered a breach of warranty. Replacement is usually cheaper than repair. Inflexible, non-modular design means that users who want the latest camera in their smartphone have to replace the complete device, rather than just upgrade a specific part. While there is a growing legislative push both inside and outside of Europe to strengthen Right to Repair principles, these initiatives are being met by strong pushback from the large actors in this space.

Pointing to even more nefarious business practices are accusations of manufactured obsolescence, the idea that devices are designed to break or slow down as they get older and newer product lines are released. While hard to prove, we see rising calls for more forceful regulatory action to curb these practices where they exist.[42] The smartification of other appliances and technologies will likely lead to another source of premature device disposal: a smart fridge, for example, might be expected to last at least ten years, but software support keeping the fridge functioning well, might end much sooner, effectively bricking the fridge years before it was otherwise due to be replaced.

Extending the lifetime of a device will help ease the burden of physical systems and hardware on the planet, but challenges recycling our connected technologies when they eventually reach the end of their lifecycle would still remain. Recycling of devices remains almost prohibitively expensive, with particularly the most valuable and hard-to-mine resources such as rare earths and lithium, often present in minuscule amounts, hard to extract. Less than one per cent of rare earths are recovered from devices globally.[43] E-waste is the fastest growing source of new waste, with only 15 to 20 per cent of devices being recycled effectively.[44] Urban mining could be a valuable industry, since the density of gold,

[38] Durairajan, Ramakrishnan & Barford, Carol & Barford, Paul. (2018). *Lights Out: Climate Change Risk to Internet Infrastructure.* 9-15. http://pages.cs.wisc.edu/~pb/anrw18_final.pdf

[39] Belkhir, Lotfi & Elmeligi, Ahmed. (2018). Assessing ICT global emissions footprint: Trends to 2040 & recommendations. Journal of Cleaner Production. https://www.sciencedirect.com/science/article/abs/pii/S095965261733233X?via%3Dihub

[40] https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

[41] https://www.nytimes.com/2016/12/29/technology/iphone-china-apple-stores.html

[42] https://www.stopobsolescence.org/

[43] http://ec.europa.eu/DocsRoom/documents/10882/attachments/1/translations

[44] https://repair.eu/

for example, is higher in a pile of discarded iPhones than in the average goldmine, but the concept remains underdeveloped and underfunded.[45]

The current production processes behind the hardware and mega-infrastructures powering the internet are not only harmful for the environment. They also come at a significant human cost, throwing up questions over their role in sustainable development. Our devices, tubes and wires require inputs and resources that are often generated in unethical and dangerous ways, sometimes using forced or child labour. The unequal distribution and economic value of these resources, which often originate in politically volatile countries, can fuel violent conflict.[46] The production of the devices themselves can similarly rely on exploitative labour practices that do not conform to EU health and safety standards. Ensuring ethical supply chains and greater longevity, repairability and recyclability for connected devices thus also carries with it a strong moral imperative.

The European Commission can play a frontrunner role in strengthening the circular economy for digital devices, which could in turn spur innovation, support job growth and strengthen communities, as some of the value-adding processes, such as repair, sale of refurbished devices, or the collection and recycling of materials, could happen closer to the consumer. This transition to greener digital tech could also help Europe achieve some of its objectives for "open strategic autonomy", as the European market would become less dependent on outside trade relationships, which recent events have shown can be increasingly politically fraught.

Trust:

Issues around trust manifest themselves in different orders of scale within the physical infrastructure layer: we see growing levels of distrust emerge between countries, fuelled by geopolitical tensions, trade wars and an accelerating innovation arms race – with the tug-of-war around 5G currently the most prominent example. At an individual level, consumers feel a growing sense of distrust about their own devices, from webcams to voice-activated smart speakers, unsure whether the technology they own actually does what it claims to do.[47]

The COVID-19 crisis left governments wary of both the neutrality and security of the technologies they purchase, and concerned about the continued supply of these solutions. The pandemic revealed the fragility of global supply chains and the just-in-time economic models they support. Since supply chains are only as strong as their weakest link, more governments now feel that the only way to bring resilience back into the system is to reshore elements of production,[48] remove bottleneck dependencies and diversify across the chain. Particularly investments in mega-infrastructures will come under scrutiny, as the nature of the roll-out of these large projects often leaves little flexibility to change suppliers once deployment has started. We are already beginning to see the impacts of this growing distrust in the 5G debate, where governments who were still on the fence about whether or not to allow Huawei into their 'technology mix' before the pandemic, have now chosen to divest.[49] One of the main drivers in the Huawei debate before the current crisis was the prohibitive cost of non-Chinese alternatives in the 5G market. Might cost become less of a deciding factor in a world where notions of sovereignty and resilience become the new leitmotif? Or will high debt burdens and the looming global recession put these concerns on the backburner?

The interconnectedness of the global internet, and the surprisingly small number of central hubs it relies on, is part of the network's strengths, but also a growing source of geopolitical friction. Since the extent of communications tapping was revealed by Edward Snowden in 2013, we have seen growing concerns about the trustworthiness of global internet traffic.[50] While the sovereignty debate that emerged in its aftermath did not lead to the kind of relocalisation and fragmentation of infrastructures that was then proposed,[51] their underlying concerns are far from resolved, and likely to be relitigated in this politically charged moment. Indeed, we have seen tensions reemerge in the context of Chinese intervention in Hong Kong, with US intelligence services now recommending that American internet traffic should no longer be routed through cables and ISPs in Hong Kong.[52] We will see this trend towards fragmentation and eventual splintering of the net recur across most layers of our power stack model.

The COVID-19 crisis has brought dependencies and systemic opacity back to the fore, and appears to be setting in motion a period of supply chain

[45] https://onezero.medium.com/the-worlds-smartphones-are-filled-with-gold-that-s-a-problem-3a7cc0e71234
[46] https://energypost.eu/twenty-first-century-energy-wars-oil-gas-fuelling-global-conflicts/
[47] https://www.pewresearch.org/internet/2017/08/10/the-fate-of-online-trust-in-the-next-decade/
[48] Barbieri, P., Boffelli, A., Elia, S. et al. What can we learn about reshoring after Covid-19?. Oper Manag Res (2020). https://doi.org/10.1007/s12063-020-00160-1
[49] https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027
[50] https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/
[51] https://en.wikipedia.org/wiki/Schengen_Routing
[52] https://www.nytimes.com/2020/07/07/business/hong-kong-security-law-tech.html

relocalisation and diversification, as well as a renewed push for building trust in technology, for example through open source development and hardware audits.[53] Europe must seize this moment to move some development of technology back onto the continent, but also to champion more transparency across the value chain. This would not only help strengthen Europe's digital single market, but would importantly also allow for more oversight and strategic embedding of security and trust-enhancing measures.

Inclusion:

Our efforts to build a more value-driven and human-centric internet can only go so far if large swathes of our population, including many of the most marginalised groups, cannot access it. In March 2019, the internet reached an important milestone: for the first time, more than half of the world's population was connected to the internet. While this is no unimpressive feat for a technology that only had 16 million users in 1995,[54] it also means that half of the world does not yet have access. In 2019, according to statistics by the ITU, 87 per cent of citizens of developed countries[55] were able to connect to the internet, versus only 19 per cent of those in the least-developed countries. This disparity in access is likely to widen the enormous economic and opportunity gaps that already exist between and within countries.

Even within Europe, at 89 per cent the continent with the highest rate of internet penetration after North America,[56] many million of citizens are yet to go online, with the unconnected largely clustered in the Union's least wealthy Member States. A rural divide is also noticeable, with internet penetration in urban and suburban areas at 91 per cent, versus 85 per cent in rural areas. As many European countries see a growing divide and polarisation between rapidly growing, wealthy urban areas versus left-behind remote regions, this differential needs to be resolved. Indeed, the European Commission has set an ambitious target to ensure broadband is rolled out everywhere in Europe by 2025.[57]

But physical access to the internet is not just an infrastructural issue: many who lack access live within geographical reach of existing internet and mobile broadband coverage.[58] For our roll-out efforts to be effective, we also need to make sure these connections are affordable. Broadband access tends to be more expensive in already economically disadvantaged areas, both in relative and absolute terms. These socio-economic barriers need to be addressed in ways that distribute costs more fairly. Similarly, gender discrimination and pay gaps mean that women also fall behind when it comes to internet access: men are 21 per cent more likely to be connected than women, with this number rising to 52 per cent in the least developed countries.[59] This dynamic is particularly pernicious in countries with large gender disparities, as digital exclusion furthers women's already marginalised position.

European policy will have to acknowledge the multi-faceted nature of inclusion, and take a more holistic approach to resolving structural and social barriers to internet access. The European Commission can play an important role in reshaping the discussion about the digital divide and move it beyond the sometimes narrowly-defined concepts of infrastructure and broadband availability alone.

2.2 STANDARDS, PROTOCOLS AND INTERNET GOVERNANCE LAYER

The protocols, standards and norms governing cyberspace and the inner workings of the internet are a product of the decisions of an opaque and convoluted patchwork of internet governance bodies, increasingly dominated by a handful of corporate and state interests. While the internet's underpinning systems have so far held up remarkably well, the increased scale and complexity of the global internet, a lack of funding for maintenance and collaborative open standard-setting, and increased political and economic fragmentation put the system at risk.

Democracy:

No single entity or organisation governs the internet. Instead, we rely on a complex web of diverse actors involved in its rule-setting, with largely decentralised, independent groups ensuring the various components and layers of the system remain interoperable.[60] While the protocols and standard-setting processes underpinning the internet in its early days were the preserve of an ostensibly apolitical and technocratic community of practitioners, the reality now looks rather different.

As the internet itself has grown in influence, so has the interest powerful actors have taken in shaping

[53] https://fsfe.org/news/2020/news-20200424-01.en.html
[54] https://www.internetworldstats.com/emarketing.htm
[55] https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
[56] https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals
[57] https://ec.europa.eu/digital-single-market/en/broadband-europe
[58] https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
[59] https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centred-method/
[60] https://www.internetgovernance.org/what-is-internet-governance/

its development. Increasingly, governments and powerful private companies set the rules. Of course, powerful technical standard-setting bodies still exist like they used to, but a proliferation of more formalised and government-affiliated governance groupings has introduced new competition. Governments also increasingly enact more and more ambitious internet policy agendas unilaterally, which impacts the global internet in different ways. This new complexity has resulted in a much more opaque and pluralistic landscape of actors, whose values and goals often stand in direct competition. In many cases, it is no longer obvious which body holds the competency and authority to make decisions. That can result in fragmentation and undermining of the internet governance process overall.[61]

Amidst these developments, Western governments still champion a multi-stakeholder model to limit the ability of a small number of actors to dominate decision-making. The idea is that all actors that have a stake in the future direction of the global network (governments private sector companies, civil society and the open source community, engineers and hackers, legal experts) should have a say. While intentions are good, in practice there are high barriers to entry – jargon-heavy, complicated deliberation processes are not particularly accessible. The resource-intensive nature of participating in internet governance fora and pervasive power differentials mean that it is above all the developed countries and larger companies that get to shape the rules.[62]

A lack of transparency and increased involvement of high-powered actors has further increased centralisation of power, with a growing number of participants now funded by large technology companies and statist governments. As a result, initiatives favoured by the largest players usually come out on top.[63] When we see competing standards, the ones that protect vested interests increasingly prevail, which makes the scaling of alternatives which could meaningfully address the internet's intrinsic power concentration dynamics more difficult.

Barriers to participation and a reduced number of actors setting the rules is not only undemocratic, it also negatively impacts the resilience of the system. A notorious example here was the standard-setting process around facial recognition technology led by

[61] https://oxil.uk/publications/eu-us-relations-internet-governance/2019-11-14-EU-US-Relations-Internet-Governance2.pdf
[62] https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf
[63] https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf

Image credit: Davi Mendes via Unsplash

the ITU, where only a handful of Chinese companies managed to write a questionable set of rules. These might now become the de-facto standard in much of the developing world, which, because of resource constraints, traditionally follows ITU standards rather than those set by more Western-dominated internet governance bodies.[64] A narrow set of actors setting the rules,

The European Commission needs to further bolster its role in maintaining an open and multi-stakeholder internet governance space. It should not be afraid to be a strong champion of open, democratically-decided standards. While internet governance is by some still seen as a highly technocratic community affair, removed from headline-grabbing (supra-) national internet policy, the stakes are high. This is the layer of the system where some of the key decisions affecting the whole stack are made. Consequently it is also the layer with a particularly high underutilised potential to make our vision for the future internet a reality.

Resilience:

In technical protocol and standard-setting processes, security of designs is unfortunately not always a priority, with new models often optimised for performance, rather than robustness and resilience. Values like protection of human rights and privacy are also often not at the top of the agenda.[65] While debates about 5G focus on the perceived risk of China building backdoors into telecommunications equipment or eavesdropping on global communications, the fact of the matter is that the underlying 5G protocols and software are not secure to begin with, meaning that vulnerabilities remain, regardless of the supplier.[66] Responsibility for issues like cybersecurity, the prevention of global cyber conflict, or the security of new technologies such as the Internet of Things, have yet to find a steady home in the internet governance community, which means rule-setting in these vital areas remains limited and can lack legitimacy.[67]

It is not just cybersecurity that is a concern. Some of the key protocols that form the internet's very backbone are no longer fit for purpose, and rely on a degree of trust between users that simply no longer exists.[68] We continue to rely on designs and systems that were developed during the very earliest days of the web and never envisioned to have to scale to support a network of billions.[69] Some were literally drawn on the back of a napkin. Even if these systems have held up well to date, the internet risks bursting at the seams. Fixing these kinds of trust and resiliency issues has proven difficult. Finding agreement in the governance community is a first substantial hurdle. Actually implementing new models is often an even bigger one. A good example is the glacial transition from IPv4 to the more long-term sustainable IPv6.[70] Disseminating core backbone fixes through a complex and decentralised system as vast as the global internet has proven incredibly difficult to do.

There are also less existential weaknesses in our systems that could use mending. There is a continuous need for tweaking and improving parts of underlying paradigms to help with infrastructure maintenance and renewal, but these endeavours are rarely profitable: often there are no clear incentives or business models that support patching up an issue, and while there are plenty of open-source developers who would gladly take up the baton, they usually lack the funding to do so.[71]

There is a clear gap to fill, and a space for the European Commission to step in and fund the continued upkeep and maintenance of core internet protocols and standards. It is also in Europe's interest to advocate for a more central role of security in standards design, and ensure we find clearer and more legitimate fora for discussions about cybersecurity and cyber non-proliferation.

Sustainability:

Digital technologies have an important role to play in the transition to a low-carbon society and meeting the ambitious aims of the European Green Deal. Setting standards for green solutions, for example in the IoT space, can help speed up the development and deployment of innovation in this space. Indeed, the ITU[72] and other bodies have dedicated working groups on these topics, thinking about how Green ICT can help further the Sustainable Development Goals.

But these efforts should similarly also focus on reducing the environmental footprint of the internet itself. This means that efficiency and energy use should be top of mind and conditions to optimise for. Internet governance, technical and web standard

[64] https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67
[65] https://dig.watch/issues/digital-standards
[66] https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/
[67] https://oxil.uk/publications/eu-us-relations-internet-governance/2019-11-14-EU-US-Relations-Internet-Governance2.pdf
[68] https://findingctrl.nesta.org.uk/how-the-internet-has-grown/
[69] https://findingctrl.nesta.org.uk/how-the-internet-has-grown/
[70] https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html
[71] https://pointer.ngi.eu/
[72] https://www.itu.int/en/action/environment-and-climate-change/Pages/default.aspx

setting bodies in particular, should continue to play a more proactive role in steering the community towards sustainability, especially as technology and design standards are one of the most effective mechanisms through which to spread better practices through the various layers of the system.

Trustworthiness:

Reduced trust between governments, and the growing role of internet technology in geopolitics is causing an increased politicisation of the standard-setting process. The COVID-19 crisis is likely to accelerate this dynamic, having brought into stark relief how most countries depend on narrow supply chains. This puts them at the mercy of the countries that control supply. Perhaps unsurprisingly, we are observing a renewed push for sovereignty and supply chain relocalisation, decoupling and deglobalisation.

Within this context, autonomy over technological innovation and the internet is becoming one of the main battle grounds, with China's changing position in the world the driving factor in this decoupling. India has banned TikTok, WeChat and many other prominent Chinese apps,[73] the United States, at time of writing, is in the process of doing the same. The United Kingdom has officially decided to divest from Huawei in their 5G infrastructure and Japan has announced it will be spending €2.5 billion to help Japanese businesses move their production out of China.[74]

This muscle flexing vis-a-vis Beijing will not only impact physical internet infrastructure and the production of devices, but could more significantly lead to a fragmentation of standards. While 5G has now firmly replaced AI as the geopolitical playball du jour, we will see the real challenges emerge around the development of 6G standards. Further politicisation of this process could well lead to the breakdown of already intricate global governance processes. In such a world, devices produced in the global IoT capital Shenzhen might not necessarily work in Europe or the US. The rest of the world could be forced to choose between mutually exclusive models, between trust and cost – a difficult choice in a world set to enter an unprecedented global recession.[75] The emergence of a functional splinternet would have enormous implications not just for the future of the internet itself, but for our societies and cohesion as a global community.[76] The open internet would become the largest and perhaps most symbolic nail in the coffin of the globalised world order.[77]

On its path towards open strategic autonomy, the European Commission should not retreat behind its own borders, but instead continue to advocate for an open and diverse internet, that is fully interoperable and truly global in nature.[78]

Inclusion:

Internet governance processes have always been notoriously complicated to keep up with, and even more so in recent years. Taking part in the events of the alphabet soup of competing standard-setting and governance bodies has become increasingly resource-intensive and time-consuming – both in terms of staying abreast with opaque and fast-evolving developments, as well as the actual expense of attending events. Attending internet governance fora remains largely a volunteer activity.[79] This has meant that meetings tend to be dominated by those who represent well-funded organisations, or already well-established members of the community. While there has been progress in recent years in ensuring a wider diversity of participants, more needs to be done.[80]

There are many initiatives, including by the governance fora themselves, which aim to open up internet governance meetings to participants from underrepresented backgrounds, particularly those from the Global South. These efforts largely rely on bursaries and sponsorship, remote participation and access programmes. But representation remains far from balanced. This lack of diversity not only perpetuates existing global disparities, but also leads to suboptimal outcomes for the internet itself, as valuable perspectives go unheard.

Most of the institutions and even many of the protocols and standards they govern were set up during a time when internet users were disproportionately wealthier citizens of Western countries. Today's internet user base is a lot more diverse. As the next billion users connect to the internet, their voices too need to be heard in the development of the protocols and systems that will shape the future of the internet.

[73] https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html

[74] https://www.bloomberg.com/news/articles/2020-04-08/japan-to-fund-firms-to-shift-production-out-of-china

[75] https://www.economist.com/the-world-in/2019/12/25/the-splinternet-of-things-threatens-5gs-potential

[76] Stacie Hoffmann, Dominique Lazanski & Emily Taylor (2020) Standardising the splinternet: how China's technical standards could fragment the internet, Journal of Cyber Policy, 5:2, 239-264, DOI: 10.1080/23738871.2020.1805482

[77] https://thelongandshort.org/forecasts/the-end-of-the-web

[78] https://www.ft.com/content/e8366780-9be5-11e9-9c06-a4640c9feebb

[79] https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf

[80] https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf

2.3 DATA AND TRANSPORT LAYER

We should perhaps think of data as the lifeblood of the internet, the connective tissue binding the various slices of the system together. Indeed, it is discussions about data, and those who own it, that have come to dominate the internet policy debate today. Our mission to build a more democratic, resilient, sustainable, trustworthy and inclusive internet by 2030 will prove fruitless unless we mend the ills of the currently unequal and exploitative data economy.

Democratic:

The business models underpinning the data economy are at the core of many if not most of the current challenges we face when it comes to the internet, and one of the key dynamics we need to break through if we want to move towards a more democratic future.

As we are all acutely aware, surveillance capitalist business models,[81] which rely on access to enormous swathes of user data, so-called data lakes, have allowed a few select actors to centralise power over many aspects of the internet. These large technology companies have also been able to leverage this power to expand their reach offline, for example into healthcare, brick-and-mortar retail, and public service provision, as we will discuss further in the societal impact layer.[82] This concentration of power now means that few truly benefit from the digital economy, with the majority of profits flowing back to just a handful of actors.

The nature of the data economy, where network effects and economies of scale have created an interplay particularly favourable to large incumbents, means that the companies who are already sitting on large data lakes will be the ones best able to capitalise on the next generation of data-driven solutions, making it more and more difficult for new competitors to find their foothold in the market. This advantage will be particularly pernicious in the escalating AI arms race: tech giants like Facebook, Tencent and Alphabet already have access to enormous linked datasets which can be leveraged to train their algorithms, allowing these companies to operate more efficiently and generate more profit, which in turn will reinforce their ability to acquire more users and more data. Unless we find new ways to democratise access to data and break through this vicious circle, today's winners will also be the winners of tomorrow.

[81] *Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.*
[82] *https://www.businessinsider.com/amazon-is-killing-these-7-companies-2017-7*

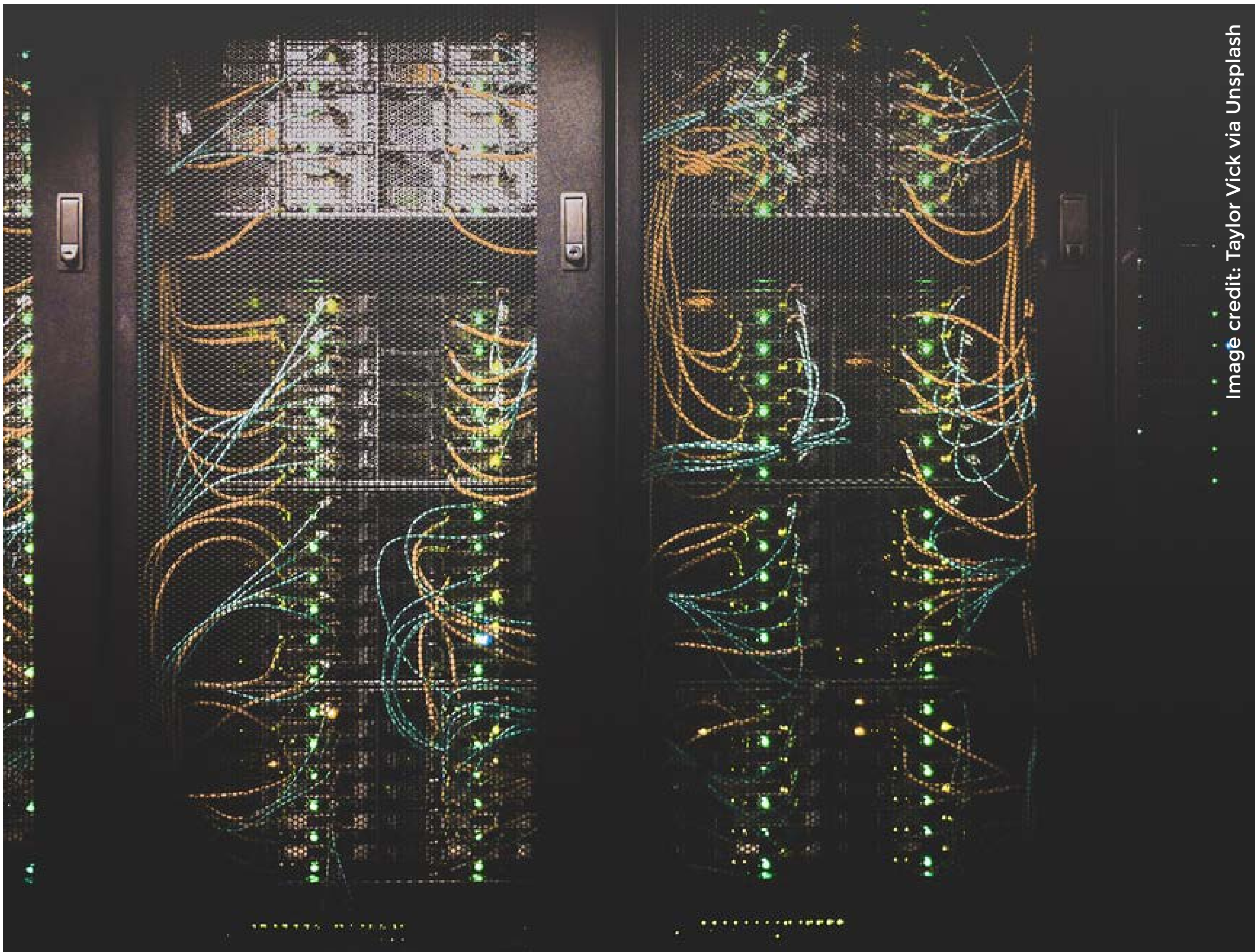


Image credit: Taylor Vick via Unsplash

This lack of a level playing field not only makes it incredibly difficult for new actors to enter the market, but also poses great risks to citizens. Given the economic and political value of data, indiscriminate hoovering of personal information is increasingly becoming an end in itself, powered by an intricate and opaque ecosystem of shadowy data brokers, ad-tech juggernauts and real-time bidding solutions that rival stock markets in their complexity and speed. It has become virtually impossible to opt-out or even understand what happens to our data online, leaving us with very little agency to make our own decisions. Under surveillance capitalism, we are the product, at the mercy of those who have the power to influence our behaviour and shape our online and offline interactions and identities.

This concentration of power similarly manifests itself in the ways data is transported through the system. Net neutrality, the principle that all traffic, all packages that travel over the internet, should be treated equally regardless of its content or the financial or political clout of its sender or recipient, is one of the tenets of the open internet. But net neutrality is increasingly being challenged. While the European Commission passed important legislation in 2015,[83] even stronger rules are necessary to respond to power imbalances in the industry. Already we have seen other governments gradually chipping away at these principles.[84]

We have also seen a flurry of sometimes radical proposals that aim to remedy this current market concentration: from breaking up Big Tech to allowing consumers to monetise their own data. But none of these have managed to get at the heart of the challenge, which is that the current market model rewards scale, concentration of power, and a winner-takes-all approach – centralisation begets centralisation. The European Commission can play an important role in moving away from a reactive approach specifically targeting the excesses of the data economy, to a more proactive model, where we rewrite the rules so that these issues are taken into account in the design phase of new solutions. In doing so, we can create a more level playing-field for new entrants. Innovation around data ownership models and online identity could help create radical new marketplaces, where users can control their own data and engage in mutually beneficial and reciprocal relationships with technology companies.

Resilience:

Questions about the resilience of data systems manifest themselves in a variety of different ways, with data increasingly being weaponised to threaten our societies and economies, but data systems themselves are also at risk of deliberate interference.

Increasingly frequent high-profile data leaks, from Equifax[85] to Easyjet[86], showcase the rising cost and risks associated with these kinds of breaches. Experts suggest the cost of worldwide data breaches could exceed $5 trillion by 2024.[87] While there is value in an individual's data, hacking becomes especially lucrative when practiced at scale. The accumulation of data lakes aggregating information about millions, sometimes billions, of users has created the conditions and incentives to do so.

Single points of failure and the aggregation of enormous, sensitive data sets are not just a cybersecurity risk, but also create the infrastructures for widespread influencing campaigns. The Cambridge Analytica revelations were a watershed moment,[88] revealing the extent to which micro-targeting was being used to sway political outcomes and drive polarisation. But what was most significant about these efforts was their sheer reach, rather than the precision of the manipulation. Facebook has 2.6 billion users,[89] more than the populations of China and India combined. We should be asking difficult questions about whether we believe a single, unaccountable, private entity should wield so much power, and how we can ensure this type of extreme centralisation does not open us up to unacceptable risks to security and social cohesion.

The existence of these large data hoards also makes it possible for nation states to strengthen their surveillance apparatus. We have seen a growing number of countries around the world build infrastructures to collect and link large amounts of their citizens' data, and weaponise this power for illiberal ends, such as quelling dissident speech or targeting persecuted minorities. We have also seen increased government pressure on technology companies to share information on their users. While the internet might at times feel like a lawless space, the tech giants are often forced to give in to government demands to avoid being excluded from important markets altogether. This can have far-reaching impacts on, for example, political activists

[83] https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality
[84] https://www.thenation.com/article/archive/trump-court-internet/
[85] https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
[86] https://www.ft.com/content/7a1f3add-1882-4ff7-b5ec-e454aa16fd9a
[87] https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches
[88] https://www.theguardian.com/news/series/cambridge-analytica-files
[89] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

who trust these systems with their data.[90] The existence of such large infrastructures means there will always be pressure to abuse them for nefarious ends – even if that might not be their creators' original intention.

The decentralisation of data systems, for example through data commons models, personal data stores and self-sovereign identities, could offer a solution here, but is still not being implemented at scale. The European Commission has an important and urgent opportunity to promote the use of these models, for example as part of its new data spaces initiatives.[91]

Sustainability:

It is not just the internet's physical infrastructures, it is also the seemingly more virtual elements of the internet that have a substantial environmental footprint. Every email we send, every picture we store, and every datapoint we collect has an impact, has to be kept somewhere in the cloud. This comes at a cost: the internet already uses nine per cent of global energy, a total that by some of the most extreme estimates could go up to as much as 23 per cent of global greenhouse emissions by 2030.[92]

Increasingly, this explosion in data is not just the natural product of more people using the internet, but also of the number of devices we are using, and the size of the individual and industrial data footprints we create. Gartner famously predicts we will see 25 billion connected devices by 2021[93] – with particularly rapid growth in the Internet of Things and smart sensors space. Each of these devices will collect data, often with the direct objective of making existing systems, such as public transportation or manufacturing, more energy efficient. But we often fail to take into account the impact that all this newly stored data will have.

In the data layer, debates about privacy and sustainability meet: the indiscriminate hoovering of personal data does not only have privacy implications – and is indeed one of the important areas of focus of the GDPR – but should also be part of discussions about reducing our environmental footprint. The principle of data minimisation,[94] where data owners only collect data on users that is pertinent to their stated aims and remove data when it is no longer directly useful, can well be extended to environmental aims, requiring increased awareness among consumers and companies alike.

Induced demand is one of the biggest ironies of economics: building wider roads to ease congestion has been shown to actually increase traffic jams, as more car-owners are lured onto the highway.[95] We see the same phenomenon in the digital space. Some have argued that 5G could be a net benefit for the environment – the software powering the new communications technology uses machine learning to maximise energy efficiency – but the pervasive, real-time connectivity it allows will rather encourage more use than less. Ultimately, this is likely to lead to a net-increase in emissions.

We see a similar dynamic in data centres. Many important technology companies have committed to turning their data centres fully carbon-neutral over the coming years.[96] But turning these energy-slurping mega-infrastructures green requires constant access to large and reliable amounts of renewable energy, which is not always easy to find. A recent example in the Netherlands[97] showed what the hunt for green energy can look like in practice, as a glut of data centres moved into the Wieringerpolder, the site of the country's largest new onshore windpark. While their move made sense, the new arrivals ended up cannibalising new green energy supplies that were initially built to support local farmers and communities. As a result, the local community had to resort to fossil resources once again, leaving society with a net-negative.

The European Commission should spearhead initiatives that could help reduce the environmental impact of our data use by promoting the deployment of more sustainable data storage facilities, already part of the Commission's new digital plans. It should also move to a more conscious approach towards data generation by leveraging the data minimisation principle.

Trustworthiness:

The opacity and complexity of how data is being collected leaves citizens with little agency to determine, or, more fundamentally, to even understand, what happens to their personal data and how it might be used to manipulate their behaviour. The data economy remains a one-way-street, dominated by an ever more complex web of companies and actors trying to get their piece of the

[90] https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed

[91] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

[92] https://www.mdpi.com/2078-1547/6/1/117

[93] https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

[94] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

[95] https://www.wired.com/2014/06/wuwt-traffic-induced-demand/

[96] https://www.reuters.com/article/us-climate-change-tech-factbox/factbox-big-tech-and-their-carbon-pledges-idUSKBN1ZF2E7

[97] https://www.nrc.nl/nieuws/2020/06/05/gebroken-beloftes-hoe-de-wieringermeerpolder-dichtslibde-met-windturbines-en-datacentra-a4001882

pie. Issues of trust not only pertain to the shadowy nature of the data economy itself, but also to the decisions these data-driven systems generate. A recent Pew survey of citizens in the US revealed 80 per cent were at least somewhat distrustful about how companies collect data, with 81 per cent feeling they have little to no control over what happens to their personal data.[98] Smart city systems, which evaluate us even when we are not aware of them, make it impossible for us to give meaningful consent. Trackers in our local supermarket analyse whether we prefer ground coffee or beans; data on our daily train commute is being shared with third parties.

Smart consumer technology has also been the subject of high-profile news stories that fuel the trust deficit. It was revealed last year that popular voice assistants like Amazon Echo and Google Home recorded the conversations of their owners, and shared this data with their parent companies.[99] Smart vacuum Roomba was revealed to create blueprints of the houses it was cleaning, which it could then potentially sell to third parties.[100] These are just two examples illustrating a much-larger, worrying trend. This is yet another manifestation of how new models of ownership, where the devices we purchase and own are merely vessels of proprietary software we cannot scrutinise, disempower users.

While many of these practices are already illegal or at least strongly discouraged under EU law and regulations, the Commission can further curb these practices by filling legal loopholes where they may exist, improving enforcement of existing rules and incentivising the development of more ethical alternatives, of which there are currently not enough on the market.

Inclusion:

As data-driven decision-making becomes more prevalent in ever more aspects of our societies, inclusion is a topic that we can no longer afford to treat as an afterthought. Inclusion in the data economy is multifaceted: we should consider, for example, the consequences of excluding the perspectives and needs of marginalised groups in the design of solutions. We must also improve our understanding of how biases in data can perpetuate existing inequalities, while simultaneously ensuring that citizens maintain the right to opt-out of data collection.

While decisions on the basis of data, particularly in public services and policymaking, are often naively presented as more neutral and objective than those made by humans, we must not forget that the datasets and algorithms underpinning these decisions are the product of human preconceptions and prejudices. Indeed, in recent years we have seen growing public concern about discriminatory practices being reconfirmed by data, think of examples like the UK's A-level scandal,[101] or concerns about predictive policing.[102] Algorithmic decision-making is only as good as the data that goes in, and requires strong governance – deploying these systems will require careful auditing of data quality, robust processes for recourse, accountability and regular due diligence by multidisciplinary and representative groups of domain experts.

Just as incomplete or biased data can lead to unfair outcomes when marginalised groups are disproportionately targeted, being excluded can have similarly harmful outcomes. As we make more data-based decisions about the provision of services, the design of our cities, and policy more broadly, we must ensure that important perspectives are not excluded from our datasets. Many smart city systems, for example, rely on data points from smartphones to understand citizens' travel patterns and behaviours: areas with high amounts of foot traffic will see more frequent bus services or better traffic light coordination. But what about the needs of those without smartphones, including many elderly or low-income people? Their perspectives will not be taken into account in the designs of these systems, and might so even lead to worse service provision – bus routes cancelled, green spaces removed – for groups that need government support the most. Members of certain vulnerable groups are also more likely to distrust public services and may want to avoid being tracked, which can then lead to further marginalisation. If we want to achieve equitable outcomes, we need to balance the 'Right to Opt Out'[103] of connected lifestyles with the 'Right to Representation'.

Over the past few years, we have seen a growing interest in these debates, with a flurry of new ethics codes, frameworks and principles seeking to govern algorithmic decision-making and AI in particular. This type of thinking is important, but the European Commission must now seize on the opportunity to translate this work into concrete action. It can do this

[98] https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
[99] https://www.techhive.com/article/3429568/how-to-keep-amazon-and-google-from-listening-to-your-alexa-and-assistant-voice-recordings.html
[100] https://www.technologyreview.com/2017/07/25/150346/your-roomba-is-also-gathering-data-about-the-layout-of-your-home/
[101] https://www.theguardian.com/education/2020/aug/21/ofqual-exams-algorithm-why-did-it-fail-make-grade-a-levels
[102] https://www.theguardian.com/uk-news/2019/sep/16/predictive-policing-poses-discrimination-risk-thinktank-warns
[103] https://www.nesta.org.uk/blog/ten-challenges-internet/

by setting high, enforceable standards for acceptable and accountable data use – particularly in a public service context – and enshrining the principles of the 'Right to Opt Out' and the 'Right to Representation' into law.

2.4 TECHNOLOGY AND SOFTWARE DEVELOPMENT LAYER

In this layer of the system, we specifically look at the process of developing new digital technologies and software: who gets to shape innovation, and how does this impact how technology is actually used. Technology is not neutral, the political, social, economic and ethical ideas of those creating it invariably shape its design and applications.

Democracy:

It is not just access to infrastructures and data that allows powerful incumbents to entrench their own positions in the internet ecosystem and play a leading role in developing the next generation of digital technologies. Access to talent and in-demand skills is of growing importance in the knowledge economy, and makes it difficult for less well-resourced actors, such as academic institutions or small businesses, to compete. This not only leads to unfair competition, but also means that we limit the range of technologies we see developed, since less profitable applications of innovation in the tech-for-good sphere often fail to come to fruition.

The supply of software developers and other experts, especially in still emerging or highly technical fields such as machine learning and cybersecurity, is finite.[104] Large incumbents can not only afford to pay the highest wages, they can offer employees access to unrivaled amounts of data and research infrastructures. It is not surprising that many in the field consider this an appealing prospect. This means that dominant companies will be better equipped to conduct groundbreaking research into new technology areas, and put this at the service of increasing their own profitability – making today's winners also tomorrow's champions. The battle for talent can hinder efforts to build technology that solves real societal problems or serves the public good. In the now famous words of early Facebook employee Jeff Hammerbacher, "The best minds of my generation are thinking about how to make people click ads".[105]

[104] https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html

[105] https://www.fastcompany.com/3008436/why-data-god-jeffrey-hammerbacher-left-facebook-found-cloudera

Image credit: KOBU Agency via Unsplash

Inequality in technology development also makes it more likely that, in the absence of good governance or more responsible alternatives, negative use cases for technology will find adoption. If it exists, it will be used. We currently see this dynamic play out around technologies like facial recognition, which are being deployed around the world despite concerns among the general public.[106]

In recent months, we have seen a number of market leaders commit to stop development of this surveillance tool. These commitments could be further encouraged if governments enacted moratoria[107] or formal bans.[108]

While Europe trains a lot of technology talent, our greatest minds are not necessarily put at the service of either strengthening our economies or furthering the values we hold dear. The European Commission, together with Member States, should scope out policy solutions and incentive models to help retain more technology talent across key disciplines. Similarly, we must be more proactive about shaping the trajectory of potentially harmful new technologies, such as facial recognition and autonomous weapons. Where we can be proactive about steering their development in positive directions, we should. But we should also be unafraid about placing moratoria on technologies we deem too dangerous.

Resilience:

Resilience in the technology development process requires us to think about how open innovation can lead to new risks, and how systemic weaknesses can manifest themselves in the design phase.

While this paper argues that we should democratise ownership and agency over the future direction of the internet across all layers of the system, we must also recognise that this democratisation can sometimes come at a cost. Many of the technologies underpinning or enabled by the internet can be used and developed by a much wider set of users than is the case in other fields. Anyone with access to a computer in principle has the tools at their disposal to learn how to code; maker culture and relatively cheap devices like the Raspberry Pi have broadened access to hardware development and tinkering at home.

This is a great good, and makes professional careers in areas like software development more accessible to those with a non-traditional education. But it also has a flipside. Cyber crimes and more ambitious cyber attacks can be carried out by any individual or informal grouping of hard-to-identify hackers – attribution is difficult, as is understanding the full range of capabilities that these opaque, distributed actors might have. Some governments have made effective use of informal non state-actors, funding or encouraging attacks, while keeping a formal distance in the international arena.[109] As such, it continues to be difficult to conclusively prove state involvement in cyber attacks.

We see the same challenges around democratisation in the development of deepfakes and similar disinformation techniques. Deepfakes are an AI-based technology that makes it possible to easily create fake videos or audio recordings of individuals that are nearly indistinguishable from the real thing.[110] As the sophistication and accessibility of the underpinning technology continues to improve, so does the ease with which nefarious actors can perpetuate harmful misinformation.

The European Commission should continue to promote an open approach to innovation, and invite citizens and less formal groups to play their role in shaping the internet. But we must also stay alert to newly emerging technologies and applications, including those developed in informal contexts, which are unlikely to show up through traditional mapping processes.

Sustainability:

Most Europeans now agree climate change is one of the most pressing societal issue of our time,[111] requiring wholesale societal and economic reform, but also technological innovation to mitigate its worst impacts. Digital technologies have an important role to play in this revolution, as was indeed exemplified by the European Commission’s ambitious goal to put the green and digital twin transition at the core of post-COVID-19 recovery efforts. But while there is growing recognition that the two are fundamentally interlinked, in practice developments in the realm of connected technologies and greentech remain separate, with the latter seen as a distinct field of innovation, rather than a design philosophy that should permeate all R&D efforts.

While citizens are starting to become more aware of the environmental footprint of their internet use, buying a more energy-efficient smartphone does not save us as much in energy costs as purchasing

[106] https://www.visualcapitalist.com/facial-recognition-world-map/
[107] https://euobserver.com/science/148839
[108] https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police
[109] https://content.sciendo.com/configurable/contentpage/journals$002fjms$002f4$002f1$002farticle-p1.xml
[110] https://www.nesta.org.uk/feature/ten-predictions-2019/deepfake-videos-get-weaponised/
[111] https://ec.europa.eu/clima/citizens/support_en

a more environmentally-friendly washing machine or fuel-efficient car.[112] Sustainability is thus not yet the same kind of market motivator in the digital sphere as it is in other consumer product verticals. Addressing this would require actions both on the supply and demand side, yet in practice we often see the opposite. Cheaper production and more pervasive connectivity have enabled a proliferation of ever more internet-enabled devices. Unbridled innovation in the Internet of Things in particular has led to a flurry of new solutions in search of problems – from WiFi-enabled water bottles[113] to connected food labels nominally preventing food waste.[114] Many devices that are sold as "smart" and energy-saving, actually have a very substantial environmental footprint across their lifecycle.[115] More transparency about the impact of devices and a mindset change away from 'smart equaling good' is urgently needed.

This lack of consideration of the environmental impact in development processes is not just the purview of hardware design. Emerging technologies like machine learning or the blockchain and other distributed ledgers require very high amounts of processing power and energy to function, but are seen as instrumental to the digital transition and Europe's industrial future.[116] Mining Bitcoin – the cryptocurrency continues to be the most prominent application of blockchain technology – requires more energy than mining gold.[117] Training a complex machine learning system can take the equivalent amount of energy as five petrol cars over their lifetime.[118] It is critical that the European Commission ensures all technological development considers sustainability, and so prevents lock-in into systems that are unsustainable in the long-term.

Trustworthiness:

As internet technologies become more complex, scrutinising their inner workings becomes harder to do. As discussions about the trustworthiness of the internet and the solutions we rely on are increasingly coming to the fore in the geopolitical arena as well as in more consumer-facing settings, this lack of transparency in the design phase is becoming unsustainable. Security holes and opaque uses can be deliberately built into solutions – this is a concern that is at the root of many of today's discussions about technological sovereignty. But just as often, they are simply the product of poor development processes.

As Europe and countries like the United States, China, Russia and India are increasingly embroiled in a so-called technology cold war, we see a rising number of efforts to "rehome" technology development.[119] This is seen as a way to regain control over the direction of technological innovation and benefit domestic economies, but it also serves to address perceived trust deficits – triggered by fears over secret backdoors being built into solutions we import, enabling cyber attacks or data breaches. Yet aggressive moves to ensure more independence could well lead to more fragmentation and a further breakdown of global governance systems.

Silicon Valley's mantra of "move fast and break things", which has become the globalised ethos of most technology development, unsurprisingly does not always lead to robust outcomes. As Big Tech companies are starting to play a more important role not just in the development of consumer apps, but critical infrastructures and systems such as healthcare and education, we must be able to scrutinise how these solutions work, and evaluate their trustworthiness and security.

This mantra has also started to permeate government-led technology development, an area where trust and transparency is especially important. As governments around the world scramble to rapidly roll out crisis tech solutions in response to COVID-19, privacy advocates fear this will lead to the permanent normalisation of intrusive tracking and data collection tools, and so contribute to the further entrenchment of the surveillance state. Human rights are easily brushed aside in times of a pandemic, and we have already seen many governments use this crisis as an excuse to push pre-existing authoritarian agendas.[120]

While decisions to deploy these kinds of tools are usually quite deliberate and strategic, surveillance creep is also often the byproduct of governments feeling like they need to keep up with any newfangled technology, just in case it turns out to be the golden ticket. This is partly owed to their tendency towards 'solutionism', tech as a silver bullet for all our problems, but it appears there is more going on in the COVID-19 crisis. While we have seen a heartening amount of cross-border co-operation, we have also seen countries compete to create the first vaccine,

[112] http://energycoalition.eu/sites/default/files/Energy%20Savings%202030%20IEEP%20Review%20of%20Cost%20and%20Benefits%20of%20Energy%20Savings%202013.pdf
[113] https://www.techradar.com/uk/news/what-is-a-smart-water-bottle
[114] https://hvm.catapult.org.uk/news/smart-food-labelling-set-to-slash-food-waste/
[115] http://ftalphaville.ft.com/2019/06/27/1561608044000/Green-technology-will-not-save-us/
[116] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_264
[117] https://www.nature.com/articles/d41586-018-07283-3
[118] https://searchenterpriseai.techtarget.com/feature/AI-and-climate-change-The-mixed-impact-of-machine-learning
[119] https://www.prospectmagazine.co.uk/magazine/dani-rodrik-globalisation-trade-coronavirus-who-imf-world-bank
[120] https://privacyinternational.org/examples/tracking-global-response-covid-19

race to build hospitals in less than a week and engage in an odd form of PPE Potlatch, where give away medical supplies (even if it means domestic shortages) has become a symbolically important soft power tool. In this context, no country can afford not to have their own contact-tracing app, regardless of whether they work or not, because not having one can be seen as falling behind in the innovation race.

By rushing to deploy in this way, governments have put themselves in a difficult position, forced to play an unfamiliar role as early-adopter and procurer of experimental tech, all while under intense public scrutiny. Some have taken on the difficult task of building these tools themselves, to differing degrees of success and often skipping due process. Others have turned to secretive but fast-moving companies to do the job for them – another pathway to insidious surveillance creep.[121]

We believe it is important for Europe to have more agency over different nodes of the supply chain if we want to be proactive about embedding our values in systems and solve some of the challenges described in this chapter. But we do not believe closing ourselves off from the world and engaging in techno-nationalism is the answer. Instead, we should be advocating for more openness and scrutiny in technology development worldwide – opening up the black box and engaging in productive technology governance processes could help reduce tensions. Similarly, we have learned from the pandemic that involving the public and inviting outside expertise and evaluation are crucial ingredients for building trust. Our vision for 2030 offers several suggestions for how we can do this in a systematic way.

Inclusion:

Technology is not neutral: the biases, contexts and values of those developing new innovation are reflected in the ultimate design of a solution itself. The lack of diversity in the development phase of new internet and connected technologies is therefore an important problem, and can perpetuate existing inequalities if the perspectives of already underrepresented groups are not taken into account.

Technology development, from private sector R&D departments to academia, continues to be dominated by a very homogeneous group. Women only make up 17 per cent of the UK tech workforce,[122] and only 15 per cent are from minority backgrounds.[123] Globally, R&D and innovation is concentrated in wealthy countries in North America, Europe and East Asia.[124] During the early days of the internet and the web, the developers, researchers and entrepreneurs building most of its underlying technologies and systems quite closely resembled the demographics of the people actually using it. With half of the world now connected, and another billion set to come online in the next few years, we need to ensure that their perspectives and needs are also reflected in the technologies we get to use.

Increasing diversity in the technology development process is not just a matter of opening up an important and powerful job market to a wider set of people, but also necessary if we want to avoid technology causing ever wider societal divides and exclusion. Caroline Criado Cortez' influential *Invisible Women*[125] has shown how a world designed for men has led to worse economic and health outcomes for women. From the size of smartphones – which are too large for the average female hand – to voice recognition systems that are trained on male voices and about 70 per cent better at recognising them than women: in the aggregate this lack of representation has a real impact. Designing services and solutions that are optimised for only a relatively small slice of the population not just hurts those groups excluded, but also societal and economic outcomes overall.

The European Commission can play an important role in improving diversity in the technology industry by playing a coordinator role in stimulating digital capacity-building efforts, collecting better data and evidence, and practicing what it preaches by setting conditions for diversity in its own funding and procurement conditions.

[121] https://www.cnbc.com/2020/06/08/palantir-nhs-covid-19-data.html
[122] https://www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf
[123] https://technation.io/news/what-of-people-working-in-tech-are-from-bame-backgrounds/
[124] https://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2019.pdf
[125] Criado-Perez, C. (2019). Invisible women: Data bias in a world designed for men.

2.5 APPLICATIONS LAYER

We have discussed the technical underpinnings and governance structures that make the internet function, but it is the applications layer that forms the main interface to the internet for most users. Applications, from online banking services to social networks, are increasingly walled off into separate, centralised apps. We follow the rules of these platforms and solutions with very little reciprocity involved. While we would need to break the dynamic that allows this kind of concentration and power accumulation further down in the system, it will be the application layer where success would be most visible to the general public.

Democratic:

For many users today, the internet is no longer a blank canvas, an open space which offers access to unlimited amounts of information and opportunity. Instead, we spend our time scrolling through a shrinking number of well-known applications. We narrow our horizons not only by relying on a small number of companies' solutions, but also seeing our options limited *within* those solutions. What we are presented with in these apps is optimised to fit our patterns of behaviour, increasingly pushing us away from serendipitous finds and ideas that might challenge our worldview, towards opaque algorithmic-driven filter bubbles and reinforcement of our existing preferences and priors. Rather than opening our window to the world, the centralised platform economy actually limits the internet's democratising potential.

Dominant platforms and applications not only indirectly mediate our online interactions in this way, their power and the siloed environments they create also allow them to explicitly set the rules within their own walled gardens. The large platforms in particular offer few opportunities for reciprocity and mutual accountability between user and solution, with users expected to abide by the rules and norms set out by the technology companies in charge – governance through terms and conditions. Of course, private entities are allowed to decide what kind of interactions and behaviours they allow on their own services, but we must also be wary of a reduction of outside oversight or involvement in the setting of the rules over such powerful intermediaries, and recognise these platforms do hold a duty of care. An example of how this form of corporate power could harm democracy is in the realm of content moderation – where popular social networks like TikTok carefully curate and censor politically-charged

Image credit: Rami Al-zayat via Unsplash

speech in order to not upset host governments or harm their business interest in key markets.[126]

The walled-off nature of these platforms also limits users ability and willingness to switch to alternatives. This is partially a factor of simple economics: network effects make it difficult for new platforms to gain traction, as the value is in other connections, such as family and friends, using the same services. Established platforms can leverage their existing large user bases for training data to continuously improve their services, and have the means to optimise user experience – something that small solutions, particularly those in the open source realm, struggle to do. But this platform lock-in is also the product of deliberate design: many platforms make it exceedingly difficult for users to carry their data and identity with them across different platforms. Social media users do not want to build their network again from scratch elsewhere, lose their followers or have to reupload all their pictures; gig economy workers and small businesses are not able to transfer carefully cultivated reputations and five-star reviews with them to new solutions. Platform lock-in plays an important role in further cementing the power of the large tech incumbents.

The pernicious, entrenched nature of some of these problems has left many well-meaning policymakers with their hands in their hair – existing competition law and internet policy levers seemingly no longer fit for purpose. As we will continue to show throughout this paper, there is a need for institutional innovation and a reconsideration of how policymakers should be empowered to address some of these challenges.

One way for the European Commission to help break this dynamic is by strengthening the rules around interoperability and data portability. While the GDPR has set rules around data portability of users' personal data,[127] it remains agnostic and fairly non-prescriptive about how this data portability should be executed, allowing platforms to make their outputs of as limited utility as possible. We have to work with the practitioners community to set practical standards for what meaningful, functional data portability and interoperability looks like. Going further, we should incorporate these standards into, for example institutional procurement conditions and funding to help unleash the power of public spending, accompanied by more prescriptive regulation.

Resilience:

Concerns about resilience in the application layer are manifold: from increased fragmentation to worries over the security and robustness of designs and the fragility of the business models enabling them.

Walled gardens not only take agency away from users and make it hard to compete in the digital arena. They also further accelerate internet fragmentation. While we usually think of nation states when we talk about battles over internet sovereignty, internet companies similarly want to set their own rules and stay in control. As some of the more prominent walled gardens have more users than most countries, their global reach is now so vast they are almost able to operate in an extrajudicial manner, making it increasingly difficult for policymakers to regulate their excesses and ensure the openness of their systems.

The sheer size of these platforms also opens up important questions about the security of their infrastructures: a well-targeted attack or breach could indirectly – and directly – affect billions. The opacity and walled-off nature of their solutions makes external scrutiny difficult, unless explicitly invited.

A somewhat different aspect of resilience in the application layer, but one no less important, is the over-reliance of these solutions on ad-tech supported business models. Services where the user is not directly a paying customer, but even increasingly those where the customer is, sell their personal data in an arcane and complicated web of data brokers and intermediaries all built on pay-per-click. This system does not only threaten the resilience of key social infrastructures like journalism and the media industry, as we will discuss in the information layer, but is itself built on very shaky foundations at best, since the benefits to advertisers are more limited than sometimes thought.[128] Should the adtech edifice collapse,[129] it could have an enormous impact on not just the digital economy, but our economies across the board. Devising sustainable business models through some of the mechanisms discussed in this paper should therefore be a key priority for the European Commission.

Sustainability:

Not only are more of us than ever before connected to the internet, each of us on average uses more devices, and uses these devices in ever-more energy intensive ways. Streaming video content, from gaming to making video calls, to binging our favourite

[126] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing
[127] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/
[128] https://www.axios.com/giant-ad-tech-bubble-may-soon-burst-sizmek-bankruptcy-1781544f-2e77-426c-9b4f-25d315c101cb.html
[129] https://thecorrespondent.com/100/the-new-dot-com-bubble-is-here-its-called-online-advertising/13228924500-22d5fd24

series, has been one of the fastest growing areas of internet use and now makes up 60 per cent internet traffic.[130] One hour of watching a series generates far more impact than spending an hour reading articles on Wikipedia. In 2018, online video viewing generated more than 300 megatons of greenhouse gases, as much as the entire country of Spain.[131]

The pandemic has shown the pressure these bandwidth-guzzling applications can place on the system, as users en masse turned to their favourite streaming websites to replace their usual evening entertainment, and both schoolchildren and remote workers came to rely on video calls for their education and daily business. This move to remote work has some notable benefits for the environment, reducing the impact of daily car commutes and work travel to far-flung places. But if the pandemic leads to a more permanent change in behaviour, it will also require us to be more proactive about reducing the impact of this additional demand.

In an internet increasingly dominated by audiovisual content, making video streaming more efficient should be a particular priority.[132] There are relatively straightforward interventions possible on the design side that policymakers and regulators could help encourage, such as throttling background and auto-plays, more energy-efficient streaming and buffering, and reducing video quality during hours of peak demand, but we also need significant behavioural change on the side of the consumer. We therefore introduce the concept of *conscious connectivity* in this paper: we need to raise awareness among the general public about the impact their individual behaviour has on the environment. As more of us want to live sustainable lifestyles, we must become conscious of wasteful internet use. That could mean not letting HD video run in the background, deleting old media and duplicate photos from the cloud or unsubscribing from newsletters we no longer read – in the aggregate even seemingly insignificant tweaks make a difference.

Trustworthiness:

Issues around trustworthiness in the application layer can be divided in roughly two categories: distrust in the applications and those arbiting them, and lack of faith in the interactions facilitated through these platforms.

The lack of transparency about how our data and online interactions are being mined and used by the services we rely on is a growing source of distrust, particularly in the wake of highly public scandals and media stories. As long as we do not know what is going on under the hood, this trust deficit is unlikely to be resolved. The recent COVID-19 tracing app debates have revealed the importance of ensuring public buy-in and open innovation processes. More nefarious still are examples like the Chinese Zao app, a temporarily incredibly popular 'deepfake' app, which allowed users to superimpose their own face on famous movies and videoclips, but was banned in China and the rest of the world soon after the app's lacklustre security and draconian terms and conditions for image usage were revealed.[133] Lack of awareness about which solutions can instead be fully trusted and have been verified to do what we gave consent to them to do, further compounds the problem. Trustmarks and auditing of particularly high-risk solutions, such as online banking and health applications, could help mitigate some of these challenges.

The trust deficit also manifests itself *on* platforms: how do we know who we are interacting with? Can we trust our online transactions? Data breaches and cyber crimes are becoming more commonplace, further enabled by centralisation of databases, which introduce dangerous single points of failure, as we discussed in the data layer. The lack of reciprocity in online interactions means it is difficult for users to build reputations independently, like we can in the physical marketplace. That forces us to increasingly rely on middlemen and depersonalised reputation scores to mediate our online interactions – rather than building a society on trust we are moving to one that is trust*less* by design.

At the root of all of these problems is one of the internet's original sins: the identity problem. Now more than thirty years into the web's development, we still have not solved this challenge, meaning that it remains incredibly difficult for users to control their own online interactions, build trusted relationships with others, and determine which information about themselves they share with whom. In the offline world, we usually get to determine which side of ourselves we show when we purchase something in the supermarket. On the internet, there is rarely a choice between full anonymity or oversharing to build a reputation (think about how often we are now asked to share our social media accounts when signing up for a service). Some governments have tried building online identity systems to help solve this problem, but the centralised nature and rigidity of these

[130] https://theshiftproject.org/wp-content/uploads/2019/07/Excutive-Summary_EN_The-unsustainable-use-of-online-video.pdf
[131] https://theshiftproject.org/wp-content/uploads/2019/07/Excutive-Summary_EN_The-unsustainable-use-of-online-video.pdf
[132] https://media.nesta.org.uk/documents/Internet_of_Waste_-_The_case_for_a_green_digital_economy_1.pdf
[133] https://www.theguardian.com/technology/2019/sep/02/chinese-face-swap-app-zao-triggers-privacy-fears-viral

systems has meant they tend to be more appropriate for facilitating interactions with government, such as paying our taxes. There are many exciting developments in the realm of decentralised self-sovereign identities, where the middleman has been removed completely and users have complete control – but while these solutions show much promise, their lack of accountable governance, and therefore trust in the robustness of the underlying systems, has allowed few to gain traction.

The European Commission can play an important role in bringing more trust into existing internet services and applications, and helping a new ecosystem of trust-by-design solutions thrive. The establishment of an auditing body which can verify the trustworthiness and security of solutions, as well as assign trustmarks to those who meet its standards has long been called for within the internet community,[134] but such an approach has yet to find the backing of an institution with the political and financial clout to help it gain momentum. The European Commission could help make this possible.

Similarly, online identity systems have been touted as a solution, but we have yet to strike the right balance between centralisation, which could bring robustness, and decentralisation, which would bring trust necessary to make these systems scale. In the *European Democratic Data Space Framework* section of this report, we discuss a model for how the European Commission could help give every European citizen, and beyond, access to a trusted and self-sovereign online identity.[135]

Inclusion:

The internet is playing an important role in mediating our interactions with businesses and increasingly also public services, which makes it more important than ever to ensure these applications are accessible and beneficial to all to use.

Today, less than 10 per cent of websites and applications are fully usable to those with a disability,[136] even though accessible design models are very much available.[137] Governments should set even more stringent conditions for accessibility in their funding and public procurement calls, and help raise awareness to ensure the private sector adopts these practices more proactively. But we must recognise that the internet will simply not be the interface through which all of us want to interact with our government, with digital skills and lack of trust in some cases an insurmountable hurdle. Just as we should have the right to accessible services, we should therefore also have a right to opt out of digital services altogether, and maintain analogue alternatives in public service provision. The pandemic has shown how little recognition there is of this digital divide: groups most vulnerable to COVID-19,[138] such as the elderly, are also least likely to have access to smartphones or other connected devices.[139] Therefore, many are unable to participate in tech-based solutions like the new contact tracing systems.

The forms of exclusion described in the previous paragraph are often the product of a lack of awareness or consideration on the part of the developers, but can also be more deliberate and sometimes driven by profit or political motives. Meaningful access to the internet means users should have access to the full, open internet, not just a series of pre-selected walled gardens. Restrictive governments in several, often lower-income, countries are known to scuttle access in this way.[140]

As users become more aware of the privacy implications of their online presence, demand for alternatives has risen. We must be careful to not end up in a situation where the well-off can afford solutions that better safeguard user privacy, and those who lack the means continue to have their data harvested under the motto: “If it is free, you are the product”. Our discussion about meaningful access to internet services and applications does not end there. For inclusion to be meaningful, this access also needs to be safe, and have the best interest of users in mind. The deliberate addictive designs of many applications, particularly in the social media sphere, can also lead to too much access – with studies suggesting adverse mental health impacts on already vulnerable groups, such as teenagers.[141]

The European Commission can play an important role in ensuring both the public and private sector incorporate the latest standards around accessible design in their solutions, and ensure the internet does not become the only interface through which we can interact with our governments or make use of important public services. Similarly, through regulation and use of market-creating levers as described in various sections of this papers, the

[134] https://www.nesta.org.uk/blog/trustmark-internet/
[135] https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2020_en
[136] https://abilitynet.org.uk/news-blogs/web-accessibility-guidelines-turn-10-still-less-10-sites-are-accessible
[137] https://laurakalbag.com/book/
[138] https://www.nhs.uk/conditions/coronavirus-covid-19/people-at-higher-risk/whos-at-higher-risk-from-coronavirus/
[139] https://tech.newstatesman.com/coronavirus/only-40-per-cent-of-most-vulnerable-likely-to-use-nhsx-contact-tracing-app
[140] https://www.accessnow.org/keepiton/
[141] https://www.oecd.org/els/health-systems/Children-and-Young-People-Mental-Health-in-the-Digital-Age.pdf

European Commission can support the normalisation and universalisation of privacy-by-design and similar practices, ensuring they do not become the exclusive preserve of those with the means to afford them.

2.6 INFORMATION LAYER

Never before has so much information been created at such rapid pace, and by such a wide variety of voices. This revolution in access to knowledge is one of the great goods the internet has brought us. But the democratisation of information and reach has also been at the root of some of the largest problems we face online today. From the spread of disinformation and the amplification of polarising voices, to the fragility of business models ensuring the production of trustworthy, high-quality news, the internet's information layer is at risk.

Democratic:

The internet has often been described as the great democratiser: removing the gatekeepers of mass media, allowing each and everyone of us to have a voice and share our views with the world. But the ways in which views expressed online get amplified has turned out to be far from equitable, with a new class of content middlemen – the large platforms – playing an outsized role in deciding what type of speech gains traction. As controversy drives clicks, and clicks drive profit, the business models fuelling the platform economy have instead led to an emancipation of the kind of voices we might not originally have had in mind when we spoke about the democratising power of the internet.

While in previous decades, the internet enabled a flourishing of weblogs, personal websites, niche communities and more, the large platforms now form the main conduit through which we discover new information and share our own views with the world, each governed by opaque ranking algorithms and content management preferences which we cannot control or even understand. These platforms disproportionately profit from original content shared online, but usually do not create it. Facebook and Google together command a staggering 60 per cent of total U.S. digital advertising revenue,[142] with news media now so reliant on these two behemoths that they are increasingly forced to play by their rules.[143] This is one of the key dynamics at the root of the media industry's profitability crisis, which we will discuss further in this layer's resilience section,

[142] https://www.emarketer.com/content/podcast-regulating-the-tech-giants-why-now
[143] https://www.theatlantic.com/technology/archive/2018/10/facebook-driven-video-push-may-have-cost-483-journalists-their-jobs/573403/

Image credit: Bank Phrom via Unsplash

and has led to many complicated questions about whether platforms ought to spread a larger share of their profits with content creators – a debate policymakers continue to grapple with.

Probably the biggest concentration of market power we see is in the search and discovery space: In Europe, Google's search engine accounts for 95 per cent of clicks.[144] This means the tech giant wields incredible power over what we see, and has been shown to use this power to its own advantage. On average, 60 per cent of the first page of search results is now made up of entities owned by Google's mother company Alphabet.[145] This ability to control the order of results will become even more important in a world where search moves from our phones and computers into the 'real' world – think of voice assistants or object search – where queries often defer to a single result, rather than an ordered page.

The gatekeeper role of large platforms not only creates an unfair economic advantage, it also harms public debate. Advertising business models are built around clicks: the more we click, the more profit is generated. But as it turns out, optimising for profitability usually means optimising for controversy: the most extreme views on the political fringes are the ones that get most attention from readers, which has led to a democratisation in a direction we did not expect and most of us do not favour. There is the amplification of extreme political speech, which many have argued has further aided the worrying revival of the extreme right and other dangerous political groups.[146] Antivax campaigns, alleged links between 5G and the coronavirus, QAnon, and other fanciful but dangerous conspiracy theories have been particularly pernicious during the pandemic and notoriously difficult to weed out, especially as removal risks reinforcing this distrust in the "powers that be''. Social media platforms, which have started to take more forceful action,[147] and regulators struggle to keep track of these developments and strike the right balance between safeguarding free speech, while ensuring the safety of users and upkeep of societal trust.

The emergence of filter bubbles, and polarisation of news sources across the board, leads to an erosion of our shared context and demos as a public, fuelling distrust in political systems in general and undermining democracies. It is of course not just private companies that have undermined the public sphere. Illiberal governments across the world do their part by censoring speech and undermining critical voices. According to American NGO Freedom House, 67 per cent of the world's population live in countries that actively undermine internet freedom.[148]

The European Commission already plays an important role in holding the large platforms to account, and should continue to advocate for diverse, trustworthy and open news and information ecosystems. Continuous research to improve our understanding of the underlying forces driving harmful speech is a key part of this, as much a social problem as a technological one. The EU should furthermore consider investing in the creation of an Open Web Index, which would help alternative solutions in the search and discovery arena compete on a more equal footing, and could help challenge the current search engine monopoly by reducing the reliance of smaller actors on the bigger players' infrastructures.

Resilience:

While the flow of information is growing, the ecosystem that creates this information is fragile. Democracies and resilient societies thrive on access to high-quality and trustworthy information; journalism holds our leaders to account. But high-quality journalism is expensive, and often unsustainable under the current business models fuelling the internet economy.

Since the dawning of the digital age, the profitability of traditional news outlets has all but collapsed. Between 2015 and 2019, annual European newspaper industry revenues have fallen from €39bn to an estimated €33bn.[149] Online advertising has proven far less profitable than print advertising was back in the day. The once hugely valuable classifieds market has disappeared, and subscription rates have fallen amidst the deluge of freely available online journalism.[150] In Germany, still Europe's largest market for journalism, print subscriptions to daily newspapers fell by 66.000 - a staggering 15%. That development has not been compensated by modest increases in their paying online readership, with less than 9.000 new e-subscriptions registered for that same period.[151] This is not because readers do not trust or value high-quality journalism – we consume more media than ever before. Instead, experts cite a lack of awareness about the precarious state the industry is in, and the

[144] https://gs.statcounter.com/search-engine-market-share/all/europe
[145] https://themarkup.org/google-the-giant/2020/07/28/google-search-results-prioritize-google-products-over-competitors
[146] https://www.voxpol.eu/the-far-right-online-an-overview-of-recent-studies/
[147] https://www.telegraph.co.uk/technology/2020/04/23/twitter-bans-tweets-encouraging-attacks-5g-stations/
[148] https://freedomhouse.org/report/freedom-net/2016/silencing-messenger-communication-apps-under-pressure
[149] https://reutersinstitute.politics.ox.ac.uk/risj-review/what-can-be-done-digital-media-policy-options-europe-and-beyond
[150] https://www.theguardian.com/media/2019/sep/29/local-newspapers-closing-down-communities-withering
[151] https://www1.wdr.de/nachrichten/themen/coronavirus/corona-zeitungen-krise-100.html

mismatch between how we consume information in the digital age, picking and choosing from a wide range of publications rather than limiting ourselves to a one-stop-shop, and the ways in which subscription models work.

The COVID-19 crisis has further revealed the fragility of an industry already in steep decline. The already barely sustainable advertising models online publications have come to rely on all but collapsed during lockdown, fuelled by a precipitous fall in consumer demand.[152] Digital advertising was down by as much as 80 per cent in Germany.[153] Prestige publications like The Guardian, The Economist and Neue Zürcher Zeitung have all been forced to cut editorial jobs. Local media outlets are even worse-hit: in the United Kingdom, 245 local news titles shut down between 2005 and 2018,[154] resulting in so called "news deserts", whole cities or regions that no longer have journalists covering them. A lack of local news provision not only harms community cohesion, but also makes it extremely difficult to keep local politicians and institutions to account. According to research by Kings College, a declining journalistic presence thus leads to a decline in the quality of governance and sometimes even an increase in institutional corruption.[155]

New, profitable business models are sorely needed, particularly for news publications in smaller markets, which have a smaller potential reader base to tap into. Reflecting the tendency towards centralisation, which we witness again and again across the various layers of our power stack model, we see another winner-takes-all dynamic emerging in the information space, where only the largest – often English-language – publications have found a path to profitability through record-high subscription rates, leaving smaller outlets, particularly those in smaller language-markets, in the dust.[156]

Given the fragmented nature of the news industry in the European Union, the European Commission and Member States have an important role to play in ensuring a diverse, independent media ecosystem can continue to thrive, and continue to explore alternative, more sustainable business models.

Sustainability:

'Too Much Information' is a growing problem on the internet, when studied from a sustainability lense. The current economics of the online information ecosystem reward quantity rather than quality. The sheer volume of content – an increasing share of which is now duplicates or low-information word salad generated by bots – serves not only to overwhelm the news consumer. It also has a substantial environmental impact, each and every piece stored somewhere in the cloud, generating its own footprint.

Here, we should make a distinction between what we can call clutter and meaningful information, with the former a category of content creation we should try to curb altogether, and the latter a space where innovation to increase the efficiency of archiving and information distribution can be improved.

Current ad-tech business models and inefficient SEO practices reward the creation of volume. Bots create duplicates of popular news articles, not for consumption by humans but crawlers, while the use of buzzwords and dark patterns incentivise unwitting users to engage with perpetually reposted clickbait. To illustrate the sheer magnitude of some of this content proliferation: analysis by US author Franklin Foer found more than 3.2 million individual 'articles' dedicated to the infamous case of Cecil the Lion, a viral news story several years ago.[157] Unsolicited marketing campaigns and spam similarly leave their mark. Like the principle of data minimisation we discussed in the data layer, also here data protection legislation can play a role. GDPR rules have reduced the total number of emails sent each day by 1.2 billion by clamping down on unwanted emails and newsletters, reducing our emissions by an estimated 360 tonnes of CO2 every day, equivalent to the energy required to power over 20.000 homes.

Bots are not just the main generators of online information flows, they are also their chief consumer. By some estimates, bots crawling the web, for example those indexing the web for search engine purposes, make up about 40 per cent of internet traffic.[158] The development of green search provides solutions to this, but remains nascent, with alternative search engines finding it hard to gain a foothold in an incredibly centralised market.

We should also start to consider the impact of information that we see as more eminently valid or valuable. Archiving information on the internet is a challenge, and over time we risk losing access to important snapshots of human and technological

[152] https://www.ft.com/content/b6fdec4c-e3e7-43b9-a804-03c435de65bb
[153] https://meedia.de/2020/03/23/stornowelle-wegen-corona-krise-anzeigenblaetter-sind-besonders-betroffen/
[154] https://www.pressgazette.co.uk/more-than-40-local-news-titles-closed-in-2018-with-loss-of-some-editorial-275-jobs-new-figures-show/
[155] https://www.kcl.ac.uk/policy-institute/assets/cmcp/local-news.pdf
[156] https://www.nytimes.com/2020/02/06/business/new-york-times-earning.html
[157] https://www.theatlantic.com/magazine/archive/2017/09/when-silicon-valley-took-over-journalism/534195/
[158] https://thenextweb.com/security/2019/04/17/bots-drove-nearly-40-of-internet-traffic-last-year-and-the-naughty-ones-are-getting-smarter/

history, through the depreciation of digital materials, removal of online archives, information overload and walled garden platforms. We want to make sure we continue to have access to what we deem important, but improvements to how we store this information are necessary. Though few websites implement them, there are design principles[159] that would, for example, reduce the quality of bandwidth-intensive pictures in articles that no longer see significant traffic, such as old weather reports; relatively modest tweaks that in the aggregate could have a real impact.

The European Commission should work together with the private sector to encourage the adoption of these low-carbon design practices, and effect a transition to an advertising and search model that rewards quality over harmful SEO practices. This would not only help reduce the internet's environmental footprint, but would leave us with a more pleasant and useful internet.

Trust:

One of the most discussed news topics of recent years, and one that reared its ugly head once again during the pandemic, is the wicked problem of fake news and deliberate undermining of democracy using the internet. Despite all this debate, we still lack a conclusive answer on how to combat it.

Weaponisation of information on the internet, either by organised political actors or more informally by a motley crew of fringe groups, click farms and online provocateurs, has proven to be a particularly effective way of sowing political discord and further fuelling societal fragmentation. Disinformation campaigns have been used to great effect in elections around the world, and have been shown to have a particularly damaging effect in countries with lower digital literacy rates.[160] As we discussed in the democracy section above, misinformation can also have dangerous public health outcomes, with conspiracies and fake news discouraging mask wearing or social distancing during the pandemic.[161]

The effectiveness of these efforts is in part a function of technology – the internet allows enormous reach at relatively low cost, but in particular thrives on the current lack of trust in many of our societies. The general public have lost faith in the authoritativeness of information from media, governments and institutions, while malign actors are empowered to more directly compete with them in a romanticised 'marketplace of ideas'. In this kind of climate, fake news is as much a symptom as a cause. A low-trust environment means that deliberate misinformation campaigns do not even have to be particularly credible or high-quality to be effective, as long as false stories reflect our pre-existing political beliefs, and are sufficiently high-volume to sow confusion.

Governments and social media platforms, which are the main conduits through which the public consume misinformation, want to crack down on these campaigns. But they are also wary of inadvertently harming free speech, thereby reducing public trust even further. Given the important accountability role that the free media and journalism play, governments ought to steer clear from attempting to police the voices we consider harmful, but at the same time we cannot let the current 'Wild West' scenario continue.

The sophistication of misinformation techniques is set to improve enormously in years to come. One example is the development of deepfakes, AI-based technology that allows for the creation of fake videos and audio of a person nearly indistinguishable from the real thing.[162] It is now possible to create a passable deepfake with only a small amount of input material, as algorithms become more efficient and need smaller amounts of audiovisual training data.[163] The tools to create deepfakes are also becoming more accessible and easier to use to anyone with a decent computer and some degree of tech-savvy. This democratisation of technology might lead to a future where deepfakes are commonplace and trust in audiovisual reporting and evidence declines even further.

As the development of deepfake technology is moving so rapidly and in a decentralised way – we see lots of similar tools emerge all over the world – it is hard for those building detection solutions to keep up. It is also an open question whether technological solutions are the right remedy to begin with. As we have seen in the case of fake news, truth becomes subjective, particularly when politics are involved. Viral videos can reach an audience of millions and make headlines within a matter of hours. A technological arbiter telling us the video was doctored after the fact might simply be too little too late. Imagine the kind of damage this could do in a closely-run election.

While the problem of fake news and more sophisticated tools of information manipulation is a serious one, we should be wary of treating it as a root cause of our current political discord and polarisation.

[159] https://www.lowtechmagazine.com/2018/09/how-to-build-a-lowtech-website.html
[160] http://www.digitalnewsreport.org/survey/2018/the-impact-of-greater-news-literacy/
[161] https://www.bbc.co.uk/news/53108405
[162] https://www.nesta.org.uk/feature/ten-predictions-2019/deepfake-videos-get-weaponised/
[163] https://www.ft.com/content/9df280dc-e9dd-11e9-a240-3b065ef5fc55

The European Commission can play an important role here by advocating for global norms regarding election interference, bringing more transparency to political advertising and money flows, and improving our understanding of the nature of these hybrid threats.

Inclusion:

An inclusive information ecosystem is an ecosystem where everyone has the ability to access knowledge and ideas, and is able to have their voice be heard.

The nature of the internet's current information ecosystem is particularly harmful for already marginalised groups, who are often at the receiving end of racist, sexist or otherwise harmful speech and victims of targeted harassment. One in four Britons report to have been the victim of cyberbullying or other forms of harmful speech.[164] Women are far more likely to be the victim of these kinds of attacks than men, according to research by Pew.[165] One particularly egregious example showcasing the intersectional nature of online abuse is the case of Diane Abbott, a prominent black, female Member of the UK Parliament. According to one analysis, Abbott was the unfortunate recipient of over half of the online abuse received by *all candidates* during the 2017 UK parliamentary elections.[166] This creates an unsafe space, which, given the importance of social media and other platforms as an amplifier of political messages, further holds back the emergence of underrepresented voices in the public sphere.

These structural barriers to access manifest themselves also on the information consumption side. Poor accessibility of many online information services – for example, still few podcasts, livestreams or other audiovisual formats are available with subtitles, which makes this content difficult to consume for hearing-impaired users.[167] Adding a description to an image in a tweet or news story increases accessibility for visualy-impaired users.[168] Making these kinds of small tweaks is often easy to do, but unfortunately not yet the norm. This unfairly excludes already marginalised groups from fully participating in public debate.

Accessing the full breadth of information and richness of content the internet has to offer is difficult for those who do not speak a major world language. There are roughly 6,000 languages in use today, yet the top ten languages, such as English, Mandarin, French and Spanish account for 82% of the total of the content on the internet.[169] Many key applications and services are not available to smaller language communities. Some key development frameworks do not even support less-used alphabets or writing systems.[170] This leaves speakers of less common languages at a disadvantage to benefit from the true breadth of knowledge and services available online.

The European Commission can play an important frontrunner role in making access to information more inclusive, by harnessing Europe's linguistic diversity to spearhead innovation in translation software, and setting higher standards for accessibility in its own procurement and funding practices.

2.7 SOCIETAL IMPACT LAYER

The boundaries between offline and online are becoming blurrier. Indeed, the internet's presence and influence over our physical spaces, societies and economies continues to grow. This means that those who do not have – or want – access to the internet will find themselves increasingly excluded from important public services and face new barriers to participating in education and the economy. Our laws and systems have not yet caught up with this pervasive digitalisation, which calls for more accountability, local ownership and collective decision-making power over what we want our communities to look like in the digital age.

Democratic:

As the internet continues to "seep" offline, this does not only have an impact on our ability as individuals to give consent and meaningfully opt-out of being part of opaque decision-making systems, it will also make it increasingly harder for non-digital businesses and initiatives to exist in the non-digital sphere. Already today we see local shops and restaurants subjected to being rated by online review websites, without having much agency in the process. While we may find it useful to look up whether that rustic-looking tapas place in front of our hotel is the real deal or a tourist trap, we often do not realise that the platforms running these review websites rely on business models where the restaurants required to pay to have good reviews made visible. Research has shown that businesses with a lower score or those not featured at all can lose a substantial amount of revenue, effectively coercing small businesses to pay up.[171]

[164] https://yougov.co.uk/topics/technology/articles-reports/2019/04/28/cyberbullying-afflicts-quarter-brits
[165] https://www.pewresearch.org/fact-tank/2017/07/14/men-women-experience-and-view-online-harassment-differently/
[166] https://www.theguardian.com/politics/2017/sep/05/diane-abbott-more-abused-than-any-other-mps-during-election
[167] https://www.britishdeafnews.co.uk/web-and-online-accessibility-for-deaf-people/
[168] https://usability.yale.edu/web-accessibility/articles/images
[169] http://labs.theguardian.com/digital-language-divide/
[170] https://findingctrl.nesta.org.uk/imagining-a-multilingual-cyberspace/
[171] https://www.nytimes.com/2018/06/13/smarter-living/trust-negative-product-reviews.html

This virtual layer on top of the normal economics of the high street or nightlife district will become more pronounced as use of digital technology in the physical space continues to increase: a large corporation can pay up to have their shop recommended by our GPS systems or local voice search. As augmented reality becomes more commonplace, a major fast-food chain might see the benefit of having customer-only perks for those that use a popular app within their store. While we have strict rules for competition and advertisements in physical spaces, this type of location-bound digital advertisement is largely unregulated – with time, we might have to start thinking about introducing a concept of augmented neutrality to our material environment,[172] extended fair advertising and competition rules to the blended virtual-material layer.

Similarly, we need to give communities more agency to decide how tech businesses operate in their neighbourhoods, towns and cities. Opaque systems often make this difficult, as we will discuss in the trust section, but unequal power differentials similarly make it hard for local organisers to make a fist. We see the discontent with some of these developments across the world. Residents of popular tourist hot spots are fed up with the impact of AirBnB on their housing markets and the livability and affordability of their cities. Ride-sharing services undercut the existing taxi markets, causing local job losses, while profits flow abroad. In recent years, there have been a number of noteworthy successes curbing tech power: cities like Amsterdam, New York, Barcelona and Berlin, connecting through networks like the Cities Coalition for Digital Rights, used their shared power to set new rules for house-sharing platforms.[173] Activists in Toronto managed to put a stop to SideWalk Lab's much-maligned Quayside redevelopment plans.[174]

The European Commission can help strengthen the ability of local actors to set their own rules by helping to facilitate knowledge-sharing and setting up the platforms and structures for collective action.

Resilience:

We must be cautious that the new push for internet-enabled resilience, fueled by the global pandemic will not widen existing inequalities and further fracture fragile economic systems.

[172] https://www.nesta.org.uk/blog/pokemon-go-and-the-marketing-agencies-of-the-augmented-world/
[173] https://citiesfordigitalrights.org/
[174] https://www.theverge.com/2020/5/7/21250594/alphabet-sidewalk-labs-toronto-quayside-shutting-down

Image credit: Markus Spiske via Unsplash

While resilience will no doubt be the watchword for public and private sector alike in the coming years, it is a term easily repurposed to mean whatever we want it to mean. The post-COVID-19 recovery offers an important opportunity to think about the future robustness of our physical and social infrastructures. The fragility of the barely-holding-on economy, of operating at extreme margins and relying on just-in-time supply chains and work forces that live paycheck-to-paycheck, has been made crystal clear. A model that affords no slack to respond to unexpected crises does not only come at substantial human cost but is simply unsustainable in a world of rising uncertainty, where climate-induced shocks will only become more frequent. What will be particularly important to watch is whether these socio-economic questions will change the way we think about the risks of anchoring ourselves to our physical surroundings. The role of the internet in these discussions will be a crucial one.

Whereas most digital economy workers have fared just fine working from the safety of their own homes during this lockdown, the gig economy workers who put themselves at risk to deliver them their daily bowl of ramen have not. Demand for Ubers and similar ride-sharing companies all but collapsed during the pandemic,[175] with drivers losing their already precarious incomes. Airbnb hosts might never see their booking numbers return to pre-COVID levels as norms around travel and hygiene could permanently change.[176] While the companies that facilitated our new reliance on connectivity saw their stocks go through the roof,[177] businesses reliant on operating in the material world saw profits crater. In the new normal, we might come to see that kind of dependency as a liability. One vision of this world is one of 'contactless delivery', where the ‘have-nots’ have to brave the dangerous urban outside, while the privileged can enjoy the miasma-free countryside, networking over Zoom-cocktails.[178]

But a more digital-dependent post-COVID-19 economy also offers opportunities that the European Commission should seek to seize. Normalisation of remote work might offer up more job opportunities to those living in areas left behind in the current economy, which could help reduce regional inequality. This could also improve the affordability of current superstar cities[179] like London, Paris and New York, which in turn might add to their diversity and vibrancy.[180] Consumers may have heavily relied on e-commerce for their lockdown deliveries, but few would be pleased to return to even further hollowed-out high streets and sterile city centres. We could well see the solidarity showcased during this crisis through mutual aid groups[181] and community support for favourite mom-and-pop shops and neighbourhood cafes, translating into a more permanent reinvigoration of local communities, tying the internet closely to our built and natural environment.

Sustainability:

As we have discussed throughout this paper, the accumulated cross-layer impact of the internet on the environment is significant, and if we fail to make changes, it will indubitably further societal challenges brought about by the climate crisis. But the internet does also enable unsustainable behaviours offline.

According to a growing body of analysis, the convenience and ease of online shopping encourages wasteful behaviours.[182] While online shopping, which enables shorter supply chains and reduces the transportation footprint of goods, is in principle more environmentally-friendly than going to a brick-and-mortar shop, in practice the story is more complicated. More than 30 per cent of products purchased online are returned, versus only six per cent of items bought in store. Same-day delivery and seemingly infinite choice also drive unsustainable levels of consumerism.[183] Aspirational social media platforms like Instagram have fuelled a boom in travel, which has a local impact on the photogenic locations which are the recipients of this new wave of mass tourism, and grows the footprint of aviation.[184] At a smaller scale, but exemplifying well some of this culture of disposability, is the case of micro-mobility services. In recent years, many cities have seen their streets littered with shared bicycles and electric scooters, which residents and tourists can rent with a simple click of a button. While such schemes may encourage a shift to more sustainable forms of transport, the average lifespan of these bikes and scooters is shockingly low. The average shared scooter only lasts between one and two months on the street.[185] There is more policymakers can do to

[175] https://techcrunch.com/2020/03/19/uber-coronavirus-update/
[176] https://www.theguardian.com/technology/2020/apr/06/disrupting-the-disruptors-how-covid-19-will-shake-up-airbnb
[177] https://www.telegraph.co.uk/technology/2020/04/30/first-real-recession-big-tech-era-double-edged-sword-silicon/
[178] https://www.nesta.org.uk/blog/great-unwinding-charting-post-covid-futures-internet/
[179] https://www.sciencedirect.com/science/article/pii/S1051137719301469
[180] https://www.theatlantic.com/ideas/archive/2020/04/how-pandemic-will-change-face-retail/610738/
[181] https://covidmutualaid.org/
[182] https://eco-age.com/news/online-shopping-impact-on-environment
[183] https://eco-age.com/news/online-shopping-impact-on-environment
[184] https://www.dw.com/en/how-instagram-is-ruining-the-environment/g-50912616
[185] https://www.theinformation.com/articles/inside-birds-scooter-economics

address these issues, but behavioural change is also necessary from the side of the consumer.

The internet can also help reduce our carbon footprint in the material world. COVID-19 has shown, for example, how we can move to a world with less business travel and carbon-intense commutes. The European Commission, with Member States, should seize this period of recovery, to test and develop new tools and solutions for remote working and collaboration that could make these modes of online engagement more effective, participatory and efficient.

Trustworthiness:

One consequence of the increasing "seeping out" of the internet from our smartphones and laptops into our material world, is that it has become even more difficult to understand when we are being tracked, or part of data-driven decision making processes. This presents a further encroachment on our public spaces. Giving consent is already difficult in carefully bounded-off online environments. The average terms and conditions document is many thousands words in length and riddled with legalese, meaning very few read them[186] and check-box ticking is no more than a meaningless formality. This problem is made even more difficult in the physical world, where people are often unaware these systems exist. There are currently no meaningful ways through which we can give consent to digital tracking or surveillance in the public.

The European Commission should explore ways in which we can make these processes more transparent and empower both individuals and communities to opt-out of systems. Without agency, these systems can quickly turn into surveillance creep, and further reduce trust in our societies. A first step is offering more transparency to citizens, by making clear where sensors, AI-enabled cameras or other smart devices are being deployed. To give one example, the City of Amsterdam has done this by releasing a public map, which shows all publicly-owned IoT devices and their specific locations.[187] A second step is to give local communities more rights to collectively come up with acceptable models for the deployment of new systems. As Internet of Things devices become more pervasive in our public space, the Commission should explore whether to extend an online identity scheme, as proposed in our European Democratic Data Space Framework, to also include objects.

Inclusion:

The global pandemic has in dramatic fashion exposed the perils of the digital divide, and the inequalities they can perpetuate. COVID-19 showed that digitally excluded people face worse and less secure job prospects, receive a lower-quality education, and can be left out of public health and other important services, further widening the quality of life gap.

Technology, for better or worse, has become a key component of many countries' lockdown exit strategies. Most of these solutions, with the much-discussed contact-tracing apps the most prominent example, rely on citizens having access to a smartphone with regular, reliable internet access. But it is exactly those most vulnerable to COVID-19 – the elderly, people with disabilities, ethnic minorities and those on the fringes of society[188] – who are least likely to own one. Gaps in public health provision during an emergency provide just one example, but we see this disparity in digital service provision become more frequent across a range of government services.[189]

The digital divide is also leading to unequal labour market outcomes. During the crisis, those in jobs with a strong digital component, which can be done remotely, were relatively secure. Even before COVID-19, those in more 'offline' jobs were on average paid less.[190] During the pandemic, they were also more likely to find themselves furloughed or exposed to greater risks as essential workers. At the same time, finding new employment or signing up for government assistance relied to a greater extent on digital skills and access to the internet. As cafes and libraries remained closed during the lockdown, those without home access lost an important lifeline.[191]
Of course, socio-economic disparity is the central dynamic driving the divide in these cases, a gap only set to widen on our current trajectory.

The COVID-19 cohort, the children and students who have seen their education interrupted by the global lockdown, will feel the impact on their professional and social outcomes throughout their lives.[192] But we must not forget that it will, in particular, be those children that do not have access to home computers and reliable internet connections that will bear the brunt of the impact. The best-funded schools and universities can more quickly transition to effective

[186] https://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/
[187] https://slimmeapparaten.amsterdam.nl/
[188] https://www.theguardian.com/uk-news/2019/sep/16/predictive-policing-poses-discrimination-risk-thinktank-warns
[189] https://www.researchgate.net/publication/221547605_The_digital_divide_and_e-government_services
[190] https://www.economist.com/britain/2020/03/26/how-covid-19-exacerbates-inequality
[191] https://www.nytimes.com/2020/05/05/technology/parking-lots-wifi-coronavirus.html
[192] https://www.brookings.edu/blog/education-plus-development/2020/04/29/the-covid-19-cost-of-school-closures/?preview_id=802677

online teaching where others struggle;[193] tech-savvy parents are better able to support their children in making most of these new resources. As remote and blended learning is here to stay after the crisis, we need to ensure all children can benefit from these resources on an equal footing.

Of course, many of the root causes of these inequalities go far beyond the internet itself, and sit at the top of the social policy agendas in many European countries. However, the European Commission and Member States should ensure discussions about the digital divide, and its complex, intersectional nature, continue to feature prominently in recovery policies and public debates as the worst and most immediate effects of the pandemic wear off.

[193] https://www.bloomberg.com/opinion/articles/2020-07-28/coronavirus-will-be-hard-on-colleges-and-college-towns-this-fall

3.

WHERE DO WE WANT TO GO: A VISION FOR 2030

3. WHERE DO WE WANT TO GO: A VISION FOR 2030

While the challenges we have discussed so far in this paper may sound overwhelming and too complex for us to be able to ever meaningfully address, we believe that Europe is particularly well-placed to get at the root of so many of these harmful dynamics. We need to untie this knot one string at a time, without losing sight of our end goal of building a more democratic, resilient, sustainable, trustworthy and inclusive future internet.

That is why in this section, we move away from diagnosis, towards a positive vision for what could be by 2030. We have outlined the kind of internet we do not want to see, so what do we want to see instead? The COVID-19 crisis has given us an opportunity to press pause and reassess our priorities. During this time of great uncertainty, rapid change and moving goalposts, a coherent and shared European vision can serve to guide otherwise heterogeneous policymaking and funding decisions towards a common set of goals and steer Europe's recovery to meaningfully address the twin challenge of greening and digitally transforming our economy.

It should be noted that this vision – while ambitious and sometimes necessitating a radical rewiring of the internet's very foundations – is grounded in reality. There is no need to pull the plug and start from scratch. The future we paint in the following chapter can emerge as a product of tangible and realistic interventions. The European Commission, working in collaboration with the European Parliament, Member States, regions and cities, should have the competencies and means to act on this vision, harnessing Europe's regulatory power, global position of trust and existing, strong innovation ecosystem.

3.1 A DEMOCRATIC INTERNET

As citizens, we increasingly feel we have lost control: technological development mostly happens to us rather than for us. We are the subject of data-driven decision making rather than its chief beneficiaries. And while demand for ethical, privacy-preserving alternatives is rising, centralisation of power has made it near-impossible for new solutions to meaningfully compete. In our vision for 2030, we directly address the root causes setting in motion this vicious circle, by opening up access to data, levelling the playing field in the digital economy, and harnessing the true power of the internet as a democratising force.

Democratising data

In our vision for 2030, we will have radically upended the surveillance-capitalist business models that previously dominated the digital economy. We will have done this by democratising access to data through proactive regulation and a competition framework that is fit-for-purpose and more confidently enforced. Alongside a secure online identity for every European, all residents will have their own personal data wallet, which allows them to decide on a case-by-case basis what data they want to share with whom: transportation data with their favourite mobility app, health data with a trusted healthcare provider. If a user wants to rescind this access, they can do so unilaterally and at any moment.

This has not only allowed citizens to better understand and control how their data is shared and used, it has also given a boost to smaller businesses. Where previously only the largest technology companies had access to big quantities of user data, now any solution can tap into this vast, decentralised data lake. This means that new companies and initiatives who want to use data in more ethical ways no longer face an insurmountable disadvantage when taking on large incumbents. No longer will they feel pressured into creating their own proprietary data hoards, instead taking advantage of – and contributing to – shared data commons.

The European Commission, Member States and local governments, in collaboration with trusted public institutions and civil society organisations, will have led the way in sharing their own valuable data, providing citizens easy access, and building their own tools on top of the commons.[194] The

[194] https://www.nesta.org.uk/report/common-knowledge-citizen-led-data-governance-better-cities/

immediate success of this new model has led to a flourishing of value-led, data-driven innovation in Europe, and has instilled an ethos of sharing across the private sector as well. This data commons blueprint has become central to the design of the data spaces infrastructures proposed in the European Commission's Strategy for Data,[195] opening up access to highly-valuable but previously siloed industrial data in lock-step.

Protocols not platforms: interoperable ecosystems

By 2030, we will strengthen the emerging ecosystem of solutions built on top of our universal data commons infrastructure by using public sector purchasing power to set high standards for interoperability for any solution we fund, and bolstering regulation.

We will have developed a common approach, together with the practitioners community, with regards to interoperability and data portability, which any R&D project is required to follow as a condition for receiving government funding. With time, this has led to the creation of a whole host of fully-interoperable applications and solutions, enabling users to carry their data and online identities with them across apps and tools, which now work together more efficiently. While public procurement was previously not high on the agenda as a potentially highly effective policy lever, in our vision we have learned how to harness the power of public spending as a market-creating mechanism.

This has not only benefited users and reduced lock-in. It has also empowered small businesses. Where developers of European solutions previously found it nigh-impossible to compete with the highly centralised walled-garden applications out of Silicon Valley, they have now begun to band together with other developers of alternatives, operating together as a suite of responsible tools, consciously streamlining mutual integration and leveraging their cumulative user base. Users are now able to easily plug their open-source calendar solution into their fully-encrypted email service and secure video conferencing app, despite coming from separate developers. To the benefit of all, this alternative ecosystem of solutions has made it much easier for new entrants to gain traction and find a sustainable user base. We will come to see this moment as the transition from the platform economy to the open protocol economy.

Collective intelligence and public engagement in shaping technology

The rapid pace of technological development has led to increased fears about its potential negative impacts, from automation-induced mass unemployment, to totalitarian social credit systems. It is therefore no surprise that we see growing opposition to some emerging technologies and further digitalisation. In our vision, we see the involvement of citizens in decision-making about the trajectory of innovation as key to not just increase public acceptance of emerging technologies, but also to ensure the connected solutions we develop effectively serve the public good, meet users needs, and avoid potential harms.

We will therefore have made public engagement and user testing, involving diverse perspectives, a key component of any government-funded R&D. This has become a particularly stringent requirement for solutions that are deployed in high-stakes environments, including many algorithmic decision-making tools and tech that requires and collects personal data. Surfacing the general public's concerns about a specific solution, while also gaining an understanding of how average, non-expert users want to engage with a tool or service, has helped us develop tech that works, and is actually adopted by users – an important lesson brought to the fore during the COVID-19 crisis, where lack of user testing proved to be a problem. Involving a wider range of voices has allowed us to better tap into the expertise of the crowd, harness collective intelligence, and so ultimately produce better, and more creative outcomes.

Our commons-based approach towards data and extensive public engagement on technology development will also provide benefits to our wider knowledge and innovation ecosystem: insights generated by European-funded research and technology will be freely available to all. Open-access, open innovation and open science will be the new leitmotif, further strengthened by our collective intelligence approach.

Digital democracy and strengthening the open internet

A democratic internet is an internet where everyone has the opportunity to have their voice heard, but we do not confuse freedom of speech with freedom of reach. We have thus focused on creating conditions where no one is excluded by design. This has meant breaking through the advertising-led business models that favour extreme and divisive speech, promoting

[195] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

nuance and fact-checked reporting instead. This has also meant giving dissidents, whistleblowers and other necessary countervoices keeping us to account, the tools to communicate and share valuable information without being under the government's gaze – the so-called Right to Whisper. Media freedom and open democratic discourse are under threat all over the world, with internet censorship and shutdowns becoming more frequent. In our vision, the European Commission plays an active role on the world stage preserving the open internet, while also supporting the development of trustworthy and secure encrypted tools that allow for healthy political conversation and organising, establishing a fund following the model of the American Open Technology Fund.[196]

We not only democratise the development of new technologies and conversations about the future of the internet itself. We also become much more innovative in how we use digital technologies to strengthen democracies. In a time of increased polarisation, finding new ways to make the general public feel involved in politics and decision-making becomes an imperative. In our vision for 2030, the European Commission leads the way in employing more digital deliberation solutions into its own institutional processes, including regular Conferences on the Future of Europe.[197]

Giving citizens a stronger voice is not only a matter of privacy and rewriting the rules of amplification. It is also about moving from an individual lens to a collective one. As we seek to strengthen citizens' rights online and give users more agency over the direction of the internet, we have shifted our approach from one focused on championing individual rights to one that has collective rights at its core. This is more in line with the realities of the digital economy, where the real value of data is in the aggregate, as are the harms it can effect. The impact of large linked datasets involving many subjects is far larger than just the sum of its constituent parts. We have therefore come to realise that proposals allowing individuals to monetise their own data are ineffectual, and data protection regulation could be much stronger and more meaningful if we looked at the rights of communities, rather than each individual user.

Introducing augmented neutrality

Net neutrality is one of the central tenets of the open internet, but increasingly under threat. In our vision, we will have further strengthened net neutrality rules in Europe, and promoted similar policies worldwide, but have also taken the concept one step further.

While we continue to see it as vital that traffic routed through the internet is treated fairly, we have also begun to realise that this principle of neutrality should be extended to include our physical, lived environment. As the internet increasingly started to seep into the material world, with new technologies like voice-recognition and augmented reality growing more sophisticated and omnipresent, we saw our physical space increasingly connected to the digital realm. A voice command leads our GPS to bring us to the nearest *sponsored* coffee shop and large supermarket chains pay AR game developers to place in-game rewards inside their stores, luring in young customers. This dynamic brings online advertising and competition from the digital economy into our public spaces, worsening existing inequalities. In our vision, we develop proactive rules that help govern this new virtual layer on top of our living space.

3.2 A RESILIENT INTERNET

As we endeavour to build a more democratic and human-centric internet, we must not forget about the vulnerabilities in the internet's infrastructures that threaten its resilience. In our vision for the future, we will have addressed some of the most pernicious underlying technical, economic and political issues that could bring harm to its backbone, as well as the dynamics that have made the internet itself a source of fragmentation in our societies and economies.

Resilient infrastructures

While the internet's underlying systems held up remarkably well during the COVID-19 crisis, we realised we might not be so lucky next time. Indeed, as climate change-induced extreme weather events and shocks were becoming increasingly more frequent, and also geopolitical conflict became a growing source of man-made disruption, an ambitious rethink became necessary. In our vision for 2030, we will have made substantial strategic investments to improve the internet's physical infrastructures by updating outdated systems, and will have designed and deployed systems that could withstand these new types of pressure and risk. Sovereignty became an increasingly important concern in these debates, as we sought to reduce our reliance and exposure to potentially adversarial governments and companies.

As we have sought to expand access to the internet – not just to every European but to all global citizens – and have better harnessed the potential of connected

[196] https://www.opentech.fund/
[197] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_89

devices as described in our vision for a sustainable internet, we also ensured the internet could cope with this increased demand. This has meant working together closely with internet service providers to ensure sufficient bandwidth and principles of good governance, but also required more proactive systems maintenance and updating of existing protocols and systems, many of which were not designed with the future scale of the internet in mind. To ensure these improved protocols and processes gain traction, the European Commission has adopted a frontrunner role as a funder and promoter of more sustainable and resilient models in the global internet governance community.

A champion of good governance and the open internet

With signs of fragmentation and the erection of walled gardens picking up pace around the world, Europe is one of the few remaining powerful voices championing the open internet. In our vision for 2030, Europe has taken a more active role in strengthening global norms and standards in the internet and technology space. This means we have taken the lead on bolstering global governance rules around cyberconflict, previously a worryingly under-governed domain, through the development of a series of international treaties covering cyber conflict and the newly emerging class of cyber weapons. To ensure the accelerating global technology arms race would not lead to further fragmentation, we have harnessed Europe's buffer role between China and the United States and facilitated a continuous dialogue, advocating for interoperability between their regulatory and standards regimes. Setting high standards for transparency and auditability of technology systems sold within the European Single Market further helped reinstill a degree of trust in the global innovation ecosystem.

Europe will also have become a more active voice in strengthening internet governance processes across the board, ensuring governments, large corporate players and other key stakeholders continue to collaborate and invite diverse perspectives in the development of the standards and protocols that form the internet's backbone. Decision-making processes about the design and use of next-generation technologies and potentially hugely influential global systems should be transparent and based on genuine multi-stakeholder governance.

The European Commission will therefore have provided more bursaries for otherwise underrepresented voices, particularly those in civil society and the digital rights community, but also funded and adopted open standards and more collaborative projects. The identity and interoperability standards of Europe's Democratic Data Space (EDDS) Framework are a prime example of this approach, which not only helps to make the internet more trustworthy and level the economic playing field, but also makes systems more resilient, as they can constantly be scrutinised and iterated upon.

Cyber-resilience and technology sovereignty

In our vision for a more resilient internet, Europe will adopt a more proactive leadership role in maintaining the open internet and championing a more rules-based cyberspace. Doing so effectively will require us to strengthen our credibility and sovereignty in the digital space. That means becoming more deliberate about protecting critical European infrastructure through stronger regulation for businesses and substantial investments in cyber-security, as well as diversification and relocalisation of production supply chains.

In our ambition for 'open strategic autonomy', we will have developed greater influence and ownership over the various nodes of the digital economy's value chains, and begun actively producing and developing technologies and critical solutions within the Single Market. After we opened up Gaia-X to become a more distributed rather than top-down initiative, it became one of the first success stories of this new wave of sovereignty initiatives, and was followed by similar joint projects, like the development of a European Web Index, commons-based data spaces for both industrial and personal data, and trustworthy identity solutions. These efforts continue to be primarily focused on building decentralised infrastructures and protocols for new initiatives to thrive on top of, rather than new, centralised verticals which themselves will come to dominate the market.

To turn these individual efforts into a thriving ecosystem of new solutions, we have also taken action to ensure we build a sufficiently skilled European technology workforce that can act on these new opportunities. This meant training a high number of graduates each year in relevant fields, but also creating the conditions to retain and attract new talent. To ensure governments are better able to respond to the complexity and fast-moving nature of the digital space, we made ambitious moves to recruit more technology, cybersecurity and internet policy experts into government directly, which allowed us to better anticipate developments and set out longer-term policy horizons, as well as build and commission technology in-house.

The European Commission will have played a key role in helping the continent regain its internet sovereignty, but we also relied on concerted efforts by Member States and local policymakers, the private sector, as well as citizens in sharing responsibility for protecting their own systems and adopting domestic alternatives.

An open-technology revolution

Secure and resilient technology can be scrutinised by experts and updated as innovation and their threat landscape evolves. By 2030, as governments sought to move more of their functions and services online, it was revealed again and again how difficult it could be to develop reliable, fit-for-purpose solutions that keep users' personal data secure. The crisis technology debate fuelled by the pandemic unleashed a radical rethink about the role governments should play in developing and commissioning technology solutions.

In our vision for 2030, this has led to governments across all layers of jurisdiction – from the regional and city level, all the way up to the Commission itself – adopting an open-technology-first approach. This means solutions are built on top of open standards and, where appropriate, open sourced. Taking this kind of approach has had many advantages: it has helped to create a market for alternative, non-extractive solutions, led to more robust and adaptable technology, and increased government's bargaining power, no longer locked into expensive proprietary tools.

To help strengthen these efforts, we will have launched a *FOSS and Open Standards* fund, which plays a triple role. Firstly, it serves as a conduit, encouraging cities, regions and countries to collaborate, procuring and developing new solutions together, and sharing code and best practices for tools already used by peers. In doing so, it will help reduce reinvention of the wheel, and grow the user bases of initially small solutions. Secondly, it oversees and supports the development of new tools. Where we see gaps in the market, the fund will provide coordination and challenge funding for open source developer teams to come up with solutions. Thirdly, it will ensure the maintenance and continuous security of open standards and open-source technologies already in use, providing funding for upkeep and improvement of building blocks.

This initiative will not just have helped governments improve the quality and safety of their technology stack, but also bolstered the open source community. Through the *FOSS and Open Standards* fund, we will have normalised the use of open source technology in more formal settings, allowing more diverse communities to find the funding to participate, and preventing innovation in the open standards and open source communities from being appropriated by profit-making endeavours.

3.3 A SUSTAINABLE INTERNET

If we continue on our current trajectory, more of us than ever before will be connected to the internet, each of us owning more individual devices, and using those devices in more energy-intensive ways. This rise in connectivity is of course a great good: bridging the digital divide through access is crucial to ensure everyone can benefit from the digital economy and reduce broader inequalities in our societies. But in our vision for a more environmentally-sustainable internet, we also have to start considering how much connectivity is enough, requiring us to think more carefully about the costs and benefits of each additional system or device we deploy, and every datapoint we collect. The internet has a key role to play in making the ambitions of the European Green Deal a reality, but it also has a significant environmental impact of its own. Living within planetary bounds means striking the right balance between these two conflicting forces.

A fully circular economy for digital devices

By 2030, we will have made sure that digital hardware has become fully part of the circular economy. Europe will become a global frontrunner in developing greener devices and manufacturing processes, optimising both the lifespan and durability of our devices themselves as well as the environmental footprint of their production. Smartphones, laptops and smart sensors will be built according to principles of modular design, which allow broken or outdated parts to be updated, ensuring maximum repairability. Significant investments will have made urban mining and recycling of discarded devices more efficient and financially viable, creating new local, secure and high-quality technical jobs in the process.

Strengthening the digital circular economy will have substantially reduced the environmental footprint of our devices, but also lessened Europe's dependency on import of resources from politically volatile countries or otherwise unreliable trading partners – an important step towards achieving greater technological sovereignty. More efficient reuse of valuable materials, alongside a responsible international development policy, has also helped us steer away from conflict minerals, while disincentivising morally questionable mining processes and the indefensible use of child and forced labour.

Improvements in production processes have moved in tandem with legislative change, such as enshrining the Right to Repair as a central tenet in the Commission's digital agenda. We have also passed groundbreaking regulations that limit manufactured

obsolescence and have made it compulsory for companies to continue to update software on their sold devices for as long as the expected lifetime of the hardware itself. As a result, users replace their devices less often, and feel empowered to tinker with their own hardware again – reawakening some of the maker mentality we had almost lost.

Data minimisation

In our vision, we have also made a significant effort to reduce the environmental footprint of data collection and storage. By 2030, all data centres in Europe will be carbon-neutral and we will have actively encouraged other countries and companies to follow suit. In doing this, we will have moved away from the language of net-zero, which can be propped up by emissions trading schemes of questionable efficacy, and towards concrete emission reduction targets.

Importantly, we did not stop there. but also became more conscious about the types and quantities of data we collect. While smart city systems can help reduce energy use in cities, we also began to consider that their sensors and the large quantities of data they collect have an environmental impact. We have thus introduced new accounting systems that allow us to keep better track of whether the environmental impact of a newly introduced smart system actually outweighs the energy savings it hopes to generate. Employing the principle of “data minimisation” as introduced in the GDPR moves us into a new paradigm where we deliberately reduce the amount of data we keep and store to only those datasets that are actually beneficial, not just to enhance privacy, but to reduce strain on the environment.

Conscious connectivity

This increased awareness about the impact of our internet use has also extended to the general public, who have started to demand greener, less wasteful services. Sending spam emails and unwanted advertising newsletters has now become as stigmatised as leaving litter in the park. Auto-playing videos and bot-generated clickbait articles are proactively curbed by the large platforms. We have popularised an ethos of “conscious connectivity”, where we have become more aware of our individual digital footprint, mindful that an extra hour of video streaming or storing another twenty photos of our lockdown sourdough bread is linked to tangible CO2 emissions. This new awareness has also led to a flourishing of green innovation, responding to consumer demand for zero-emission lifestyles. Europe has led a push in investments in green innovation by launching a large, dedicated fund as part of the Next Generation Internet initiative, which has resulted in significant advances in previously understudied areas such as green search and less energy-intensive machine learning methods, which have now become the new global standard.

Digital tech and the European Green Deal

By addressing the internet’s substantial environmental footprint, we can now fully harness the power of digital technology to make the European Green Deal a reality. The ever-elusive smart city – once a lofty PR promise – will have begun to meaningfully and positively transform our urban spaces, supported by advances in AI and the hyper-connectivity allowed by 5G and later 6G. Above all, we will have become much more deliberate in identifying where smart systems can truly reduce our environmental footprint.

Processes developed to reduce the digital supply chain’s impact now also help inform the deployment of other green systems. Our deliberate push for longevity, agility, and updateability leaves us with greater flexibility to respond to new developments and unexpected shocks, while also ensuring that we do not lock ourselves into expensive mega-infrastructures that quickly become outdated.

Savings do not just come from the deployment of AI-powered energy and mobility systems. The COVID-19 pandemic has further normalised remote working and online conferences, while wasteful business travel habits have become a thing of the past. By 2030, working from home will have become the norm rather than the exception, allowing those living in structurally weaker regions to access high-quality jobs previously only available to those living in major cities. A flurry of new innovation making online collaboration tools more reliable and usable has further enabled this transition.

3.4 A TRUSTWORTHY INTERNET

Trust is one of the vital ingredients of a functioning society, but sorely missing on the internet. In our vision, Europe will have played a significant part in strengthening the trustworthiness of the internet’s infrastructures and systems, and addressed some of the root causes of political polarisation and societal fragmentation.

A market for trustworthy technology

By 2030, Europe will have leveraged its respected role as a global regulator of technology to become a proactive developer of trusted solutions. *“Made in Europe”* has become a stamp of quality, signifying technology that is secure and ethically produced, and embodies principles of privacy-by-design and openness to scrutiny. A new European-Commission-funded and endorsed auditing body has begun administering a series of globally-recognised trustmarks, which are given out to European and non-European applications as well as devices that meet our high standards of quality. This has provided citizens around the world with accessible and reliable information about trustworthy internet alternatives that were previously so hard to find.

We have further bolstered this approach by setting high standards for cyber security, privacy, interoperability and ethical data use in the technology solutions we procure or fund. This has helped us build a sizable market for these responsible tools, which previously often failed to thrive in the absence of more sustainable business models. Where we noticed clear gaps in the market for alternative tools, we will have provided funding – ultimately culminating in a fully interoperable, open-source suite of the most popular software solutions, and a range of sustainable and trustworthy hardware devices. This *“Made in Europe”* approach has finally allowed citizens to choose alternatives that are more trustworthy and responsible, and public-interest focused alternatives across the globe to flourish.

What’s under the hood?

In order to build trust in systems and technologies, we need to be able to understand and scrutinize how they work. We have already put policy levers like public procurement, anticipatory regulation and trustmarks at the service of building an ecosystem around more responsible and trusted technology. But we will also need the tools and expertise to assess whether these new solutions actually meet our standards. As technology, particularly in the realm of algorithmic decision-making and security, becomes increasingly opaque and complex, we have to get a better understanding of what is going on ‘under the

hood'. That is why, by 2030, we will have launched an independent European auditing body, which helps us audit software and hardware solutions, develops standardised processes for continued evaluation and administers trustmarks for solutions that meet strict conditions. This auditing body, which is made up of technology and security experts, is fully independent, but funded by the European Commission and partners, and has become the standard-bearer for auditing processes of this kind around the world.

Still, auditing complex technologies and opaque apps will not be enough: we must also actively promote more transparent and scrutinisable development processes, such as the use of public, or preferably open-source code and open standards. Solutions that follow these kinds of good practices get preference in the trustmark-administration process, an increasingly strong incentive for both small and large companies as demand for trusted tech continues to grow.

Saving the news

We cannot have healthy democracies without a robust information and news ecosystem, that helps keep our elected (and unelected) officials to account. As the internet is now the main conduit through which most of us consume the news, we need to focus on ensuring the business models underpinning this key social infrastructure are sustainable and reward high-quality rather than controversial outputs. In our vision for 2030, we will have made significant headway in finding a resolution to this most central and complex of challenges.

We will have found new, novel ways of funding online journalism while ensuring our neutrality as a government – a crucial separation that was necessary to rebuild public trust, especially in European countries where freedom of press was not always maintained. We have done this by levying a dedicated Digital Tax on the large platforms, which previously benefited disproportionately from the content produced by these trusted outlets. The proceeds of this tax were partially used to fund a dedicated *Centre for Innovation in Journalism*. This centre will continue to provide funding to trusted online and print media outlets, particularly those covering local or smaller language markets to help adapt to the pressures of the digital economy.

More importantly, this Centre for Innovation in Journalism is funding ambitious cross-border collaborations and an Erasmus-style programme for journalists, both of which serve to strengthen the European demos. The fund also makes funding available for radical experiments with new business models beyond the traditional winner-takes-all subscription and advertising models, such as decentralised micropayments and new community-ownership models. This Centre will not only act as a funder, but also as an important source of knowledge and learnings, collecting data on media pluralism and the health of the industry, and making this data publicly available to other researchers. With time, outlets will have become less reliant on the proceeds of the digital tax, and find their own, independent pathways to sustainability through the centre's work.

Countering misinformation

Trust extends beyond the workings of the underlying technologies to how they are used. With the growing scale and importance of the internet, weaponisation of information will only become a more potent tool for the manipulation of public opinion and political polarisation. In many ways, the effectiveness of online misinformation was merely the product of wider social dynamics, such as rising inequality, eroding social cohesion and declining public trust. But there were also dynamics intrinsic to the internet that we had to address: economic models that favoured controversy and extreme views, a lack of moderation and stewardship by information gatekeepers, and the rapid, viral nature of information dissemination this allows.

In our vision, we will have addressed some of these root causes by investing in high-quality online journalism, devising business models that can serve as an alternative to the platform economy and promoting more community-led moderation in the online public sphere. By solving the online identity puzzle, we will have helped identify bots or otherwise "identity-free" accounts, and users who might be spreading news from different locations than they purport to be. Our online journalism fund will also have funded fact-checking experiments and can provide media outlets and large platforms with easy-to-use tools and models for automatically labelling content with disclaimers. We will have managed to toe the line between promoting healthier online discourse and information flows, without resorting to direct censorship or other draconian measures that would risk further eroding public trust in our media and democracy.

In our vision, Europe also plays a frontrunner role in mapping out and developing resilience strategies to counter new forms of deliberate misinformation. We will have funded ambitious research initiatives to study deepfakes, AI-based technology that makes it possible to create fake videos or audio recordings of individuals nearly indistinguishable from the real thing, and developed tools that could help spot these doctored files near-instantaneously. This initiative will also have helped formalise and regulate the development of deepfake tools, which has allowed us to harness this promising technology for more positive ends, such as supporting the creative industries.

Who am I? Fixing online identity

The identity problem is one of the internet's original sins: whereas interactions in the real world allow us to build our reputation, verify who we are engaging with, and establish mutual trust, the internet does not have a universal, portable model that allows us to do so. Identity management tends to be siloed, created on the terms set by the respective platform or service we are using, and is rarely designed to instill trust or agency on the side of the user.

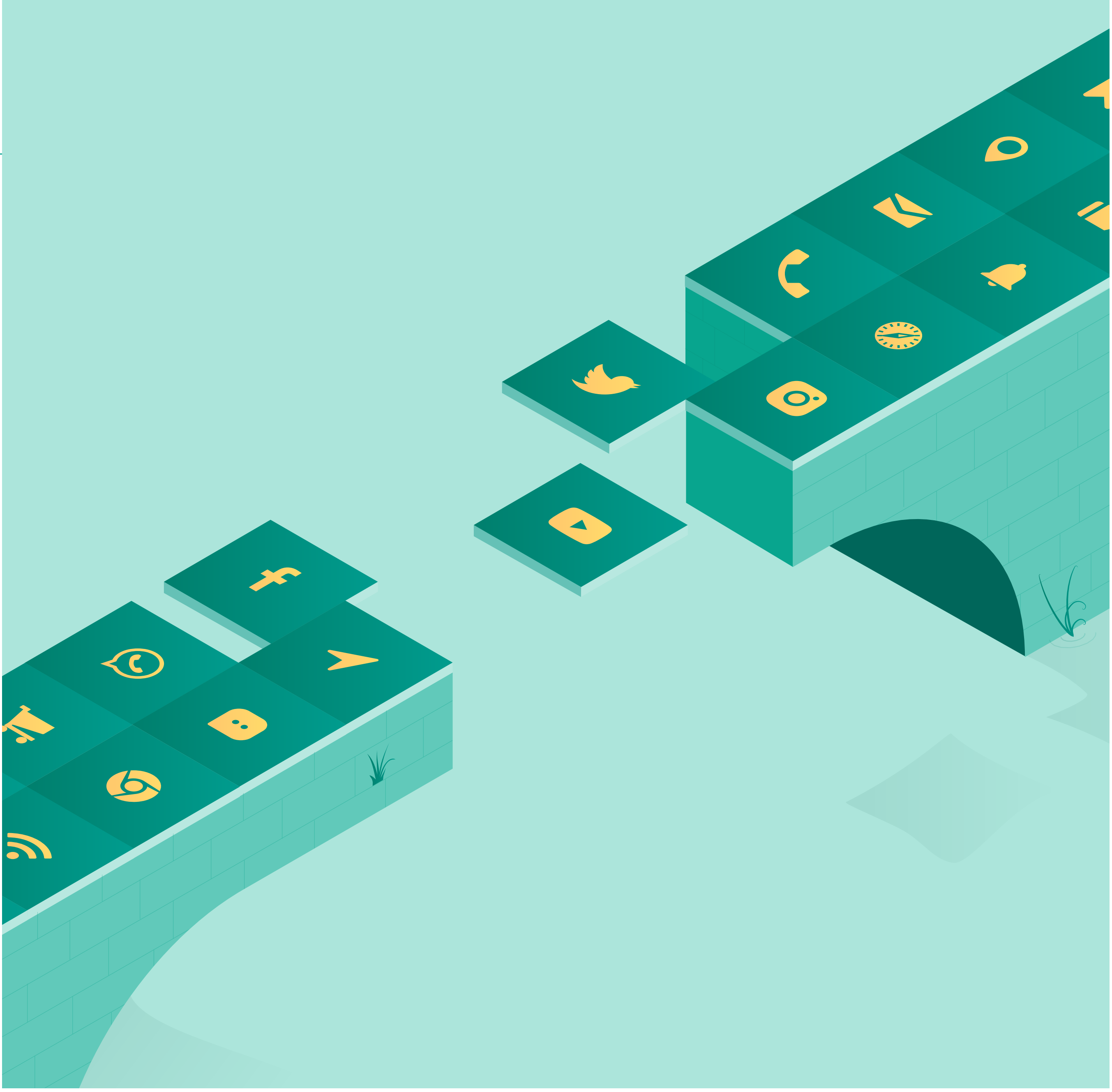
In our vision for a more trustworthy internet, we will have provided each citizen with a trusted, self-sovereign identity, allowing us to control our own online interactions and presence. Such a self-sovereign identity has allowed users to move between different services more easily, and preserve their privacy. Rather than sharing a lot of our personal details to establish trust, we now only have to share data pertinent to the interaction. This new identity model was also a vital piece of the puzzle in correcting the growing asymmetric power balance between users and online services: users now control their own data, through linked personal data stores. They can choose to share information with an app or platform on their own terms, and retract this access whenever they want to. Workers and small businesses who previously relied on large platforms as intermediaries, such as gig economy workers, restaurants, and e-commerce companies, can now take their reputations, rankings and reviews with them across solutions, releasing them from platform lock-in.

The key to this initiative's success was the fact that we struck the right balance between centralisation and decentralisation: while the technology to build universal SSI-systems had already been around for a while, their completely self-governed nature meant few had gained real traction. Government-led initiatives to build centralised identity systems remained mostly confined to the provision of government services, as their systems proved too rigid.

Within our European Democratic Data Spaces (EDDS) framework, instead, the European Commission extended its e-IDAS systems to be fully decentralised and continued to play an important role in both funding the continued maintenance and security auditing of the underlying protocols and technologies. The Commission and Member States also played a pioneering role in instilling trust in this system, acting as intermediaries and providing verified user credentials and attributes such as birth dates, evidence of nationality, or school diplomas. Our European Democratic Data Space Framework has not just improved user privacy and helped secure digital rights, but also helped facilitate cross-border trade and provided the backbone for new ways of doing business, such as smart contracts. In doing so, it will have significantly strengthened the Digital Single Market.

Meaningful consent and collective rights

For years, the opacity and pervasiveness of many emerging technologies made it difficult to devise new models for citizens to give meaningful consent to tracking by connected technologies, particularly when it came to technology rolled out in public spaces. This left many distrustful and uncomfortable with the gaze of machines, from cookies to AI-powered CCTV. That is why we have moved to a model where communities collaboratively decide how they want smart solutions to be deployed in public and living spaces and what kind of data these systems can collect. This way we, as a collective, protect the rights of the most vulnerable among us. We guarantee the possibility of opting out of systems by law, while simultaneously not excluding anyone from using or being represented in the design of a solution. We will, as neighbourhoods, cities and local areas, have taken back control over the way technology companies operate in our communities: we get to decide the rules by which, for example, micromobility companies get to distribute bikes and scooters in our public space, and we get to set limits to holiday rentals and ensure some of the generated profits flow back into the local economy.



3.5 AN INCLUSIVE INTERNET

Our vision for a more inclusive internet should ensure equal opportunities for all Europeans to connect to the internet and benefit from the digital economy, without exacerbating existing disparities. At the same time, it must establish a fair set of rules and norms for all to engage online and exchange views, without excluding or disadvantaging already marginalised groups.

Access for all

In our vision, we treat the internet as important public infrastructure, having given all Europeans the opportunity to get connected to the internet and ensuring high-speed, affordable broadband is rolled out across the whole of the Union, even remote and less economically developed areas. We will also have made a significant contribution to removing the physical barriers to internet access in the rest of the world, by capitalising on Europe's frontrunner role in the development of satellite technology. We explore whether the deployment of large satellite mesh networks can enable billions to get a reliable and usually free connection anywhere in the world, even in places where other core infrastructures, such as electricity provision, are still patchy.

Societal barriers to access

To bridge the digital divide, we have not just focused on reducing infrastructural barriers to access, but also looked at the more pernicious social and economic root causes that prevent large groups of people from fully participating in the digital economy. We have harnessed Europe's full linguistic richness and taken the lead on building a multilingual internet, where key services are available in minority languages, and instantaneous, high-quality translation has opened the door to more international exchange and cooperation, strengthening the Single Market.

The COVID-19 crisis provided an opportunity to address some of the more systemic issues around accessibility from a disability, inclusion and digital skills angle. Starting with digital public services and other solutions built using government funding, we set the standard for technology to be fully accessible to disabled users. By 2030, this will also have become the new paradigm for businesses operating in the Single Market, with advances in accessibility technology and the inclusion of a much broader developer and user base seen as important sources of innovation.

For example, our more stringent standards have led companies to experiment with voice-recognition solutions, spurring innovation in voice technology more broadly. We have also become much more proactive about designing services for user groups that were traditionally excluded from the internet, such as elderly people, and have rolled out ambitious programmes as part of the COVID-19 recovery to increase basic digital literacy.

Representation and bias

We are not just proactive users of the internet, but also an object to be analysed by connected technologies. With the increased deployment of predictive analytics, artificial intelligence and smart city systems over the second and third decade of the 21st century, we have come to realise how important it is that the gaze of the machine treats us fairly. Rather than relying on corporate self-governance and ethics frameworks, Europe has therefore taken the lead in funding and setting real legal standards for responsible AI systems. These standards extend beyond the inner workings of systems and include minimum requirements for the quality and completeness of the data that goes into them. Recognising that the way in which data is collected, interpreted and used can perpetuate social inequality and power asymmetries, we will have put in place strict rules for how algorithmic decision-making tools and similar data-reliant systems can be deployed publicly, ensuring they are accountable and open to scrutiny.

Putting inclusion and citizen rights first also means that we have sometimes had to decide there simply was no responsible way of deploying a new technology. In some cases, such as facial recognition, this has led to longer-term moratoria on the development of systems.

A safe space

We have also made the internet a safer place for marginalised and vulnerable groups, who were disproportionately often falling victim to online harassment and targeted abuse – an important barrier to access. We have done this by promoting healthier discourse and encouraging community-led moderation, as was the norm during the earlier days of the internet, but fell out of favour as the internet’s public sphere continued to grow at explosive rates. We have also ensured law and enforcement practices were better able to respond to these relatively new types of crime.

We have also managed to strike a healthier balance between protecting the safety of children on the internet and ensuring that user privacy can be preserved, through the development of harmful content filters that are compatible with end-to-end encryption. We will always face difficult trade-offs, but in the battle between safety and privacy, solutions do exist.

Shaping the internet

We recognise that inclusion is not just about access and being a “consumer” of the internet, but also about widening who gets to play a role in shaping it. Many groups are underrepresented in the technology industry, which does not only mean they miss out on lucrative jobs, but also see their unique perspectives go unheard in the technology development phase. By 2030, we will see the fruits of ambitious training and access schemes that were designed to bring in more diversity into computer science and STEM degree programmes. We will have spearheaded initiatives to collect better data on the diversity across the sector, and made the diversity of teams an evaluation criteria in procurement and funding decisions. One added benefit of governments increasingly building technology in-house, is that we will have the ability to launch apprenticeship programmes that offer a space to those from non-traditional backgrounds, and those who otherwise would have had a hard time finding a path into the tech industry.

Of course, we recognise that diversity in the development phase is not just about bringing a wider range of technologists on board, but also about hearing the voices of non-experts, and more multidisciplinary perspectives. All future government-funded technology, particularly those used in the provision of public services, should therefore undergo rigorous user testing, looking not just at the direct usability and user-friendliness of solutions, but also at unexpected societal impacts and less well-understood user needs.

4. CREATING A EUROPEAN DEMOCRATIC DATA SPACES FRAMEWORK

4. CREATING A EUROPEAN DEMOCRATIC DATA SPACES FRAMEWORK (A WORKING MODEL)

Our proposal for a European Democratic Data Spaces (EDDS) framework shows how the various ambitious elements of our vision can work together in one elegant, comprehensive model. This model can give citizens back control over their own personal data and online identities, helps level the playing field in the digital economy for public-interest focused businesses, and rewires the internet to become more resilient and trustworthy across the stack.

Putting in place this framework asks the European Commission, Member States and local governments to assume a new, market-creating role that can feel unfamiliar, but for which they already have all the levers at their disposal. This type of institutional innovation is necessary if policymakers want to address the unprecedented challenges brought to the fore by digitalisation. A host of ambitious new funding programmes and the need to spearhead a green, digital revolution means that this is the moment for Europe to experiment with new approaches. The model laid out in this section would help Europe strengthen its sovereignty, but should not be restricted to European citizens alone. Instead, it offers a blueprint for how a more human-centric internet could work globally. Indeed, the ambition should be for this model to eventually be opened up to citizens across the world.

We have already put a lot of stock into emerging innovations like distributed ledgers, online identities, personal data stores and data spaces – but we have not yet been able to fully leverage these new solutions. The blockchain remains, to use a platitude, a solution in search of a problem; online identities show great promise but have failed to gain traction at a large scale; and shared data repositories rely on use cases and proactive buy-in from data owners to reach a critical mass. In the sections below we describe how these technologies can be combined to lay the foundations for new ethical innovation to thrive, supporting the emergence of a fully interoperable ecosystem of trustworthy tools. All the constituent parts of this framework already exist or are eminently feasible to develop, it just requires political will to get off the ground.

EUROPEAN DEMOCRATIC DATA SPACES

Our EDDS framework is made up of three key elements:

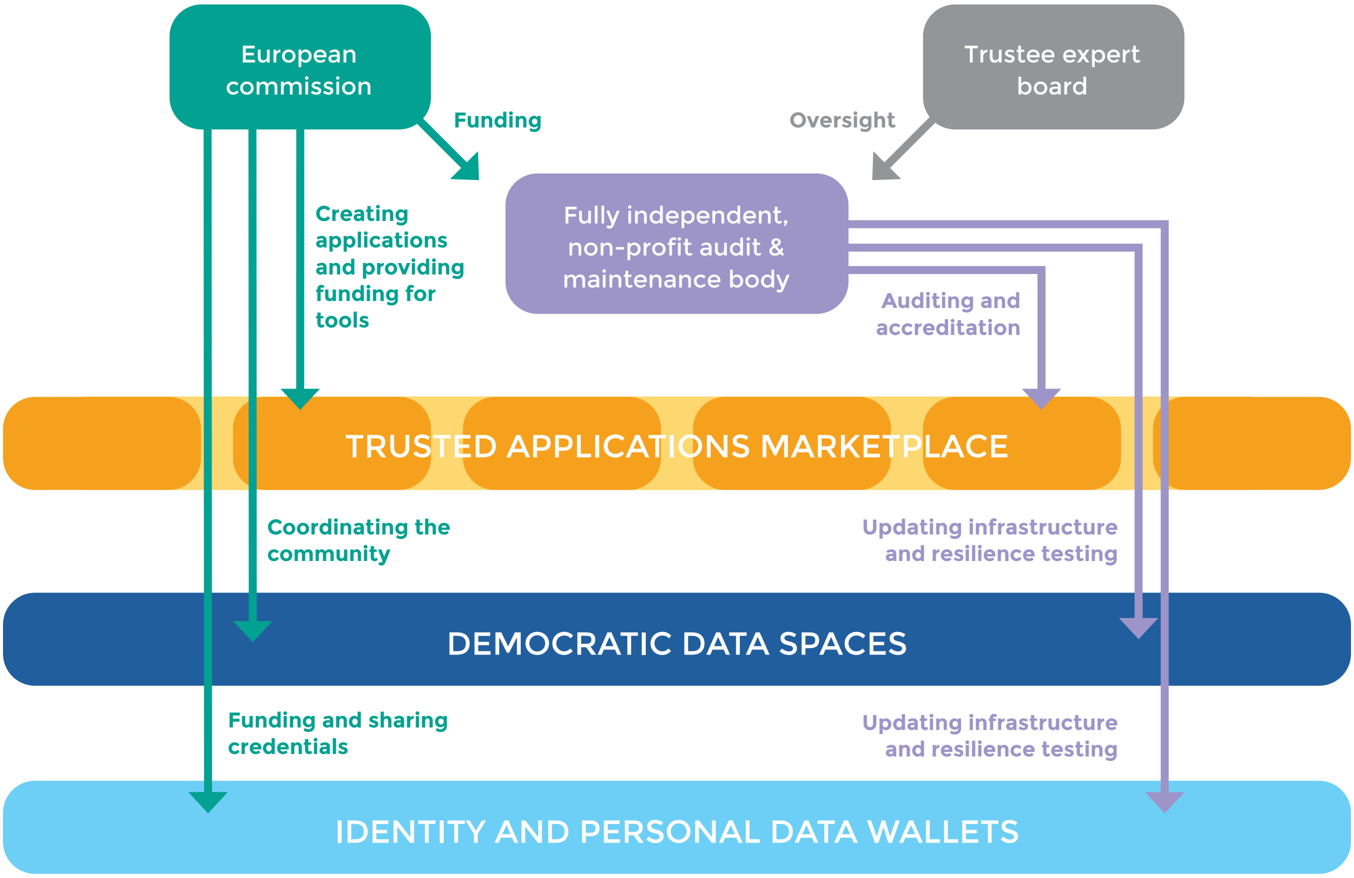
1. The issuing of a trusted online identity and personal data store or 'wallet', initially to every EU resident.

2. The creation of democratically governed data spaces or 'lakes' for pooled personal data. Here, citizens can choose to share information from their 'wallets' (i.e. personal data stores) with trusted applications. One way to think of it is as a decentralised, ethical data marketplace, built on commons principles.

3. On top of these foundations, we incentivise the development of an ecosystem of interoperable and trustworthy applications.

In order to make all of this work, we have to strike the right balance between centralisation and decentralisation: too little oversight and governance have meant that few truly decentralised solutions have been able to generate sufficient amounts of trust and participation from large actors to leave their mark. Too much top-down involvement risks repeating the mistakes that have left the current digital economy so concentrated. We want to move from a platform economy to an open protocol economy, but to do so, we need to ensure that underlying systems are secure, maintained and collaboratively agreed upon. A key feature of our approach – different from most online identity and data commons models – is the creation of an independent audit, maintenance and trustmarks body, which ensures the continued upkeep of underlying systems, and stimulates the development of trusted new solutions built on top of these foundations.

The various facets of the system


European commission
Trustee expert board
Funding
Oversight
Creating applications and providing funding for tools
Fully independent, non-profit audit & maintenance body
Auditing and accreditation
TRUSTED APPLICATIONS MARKETPLACE
Coordinating the community
Updating infrastructure and resilience testing
DEMOCRATIC DATA SPACES
Funding and sharing credentials
Updating infrastructure and resilience testing
IDENTITY AND PERSONAL DATA WALLETS

4.1 A SELF-SOVEREIGN ONLINE IDENTITY FOR ALL

How it works:

Every European is issued their own, personal, self-sovereign online identity, building on the work started by eIDAS.[198] As the internet becomes a more integral part of our lives, such an online identity can, with time, become as important as our birth certificates or our passports. Where we now rely on intermediaries, from social networks to siloed password protection models, to verify our identities and build an online reputation, decentralised digital identity systems allow us to do so on our own terms.

Online identities can be incredibly empowering: self-sovereign identities grant us the freedom to choose which aspects of our own identity to share with whom (so-called "attribute-based credentialing"), to carry our data and reputation with us across services to prevent lock-in, to give trusted services permission to access our data and to retract this permission at any time, and much more.

The self-sovereign online identity space is rapidly evolving, but the decentralised and fragmented nature of the community driving its development forward has meant no single solution has managed to gain sufficient traction, nor have we agreed on how these systems should be governed. In our model, we therefore mobilise and fund the standard setting and developer communities to collaboratively "pick a winner" and to continuously upgrade and maintain its underlying protocols and designs; combining top-down with bottom-up approaches.

Part of the strength of self-sovereign online identity models is that third parties can help bring trust to an interaction between two other parties. For example, city halls could issue a "credential" linked to our online identity which provides evidence of our home address. We can now use this same credential as "proof of address" when setting up a new bank account. Governments can therefore play an important role in instilling trust and creating critical mass in this system from the start by issuing these types of trusted credentials.

[198] https://ec.europa.eu/digital-single-market/en/discover-eidas

Some examples of how online identities can be used:

Example 1 (Privacy-enhancing): A student wants to buy a bottle of wine in the supermarket. To prove her age, she now no longer has to show an identity card (which reveals personal details like her full name and date of birth), but can simply use her phone to verify the relevant data point – that she is old enough.

Example 2 (Sovereignty): A recent refugee has lost access to all of his physical documentation on his journey to a safer haven. The immutable aspect of his online identity allows him to still show evidence of his nationality and academic credentials, helping him to maintain his personal agency, navigate bureaucratic hurdles, and find a job in his new host country.

Example 3 (Trust): A local government launches a new digital deliberation and voting system, but finds it hard to prevent ill-intended outsiders from joining in. Participants can now easily prove they are in fact residents of the local community, using their government-issued credential, while maintaining their anonymity.

How we instill trust in the system:

While governments can play an important role in creating trust in this identity layer (and other aspects of our EDDS framework), we must also recognise that many citizens and private businesses may not like the idea of government involvement when it comes to their personal data and interactions.

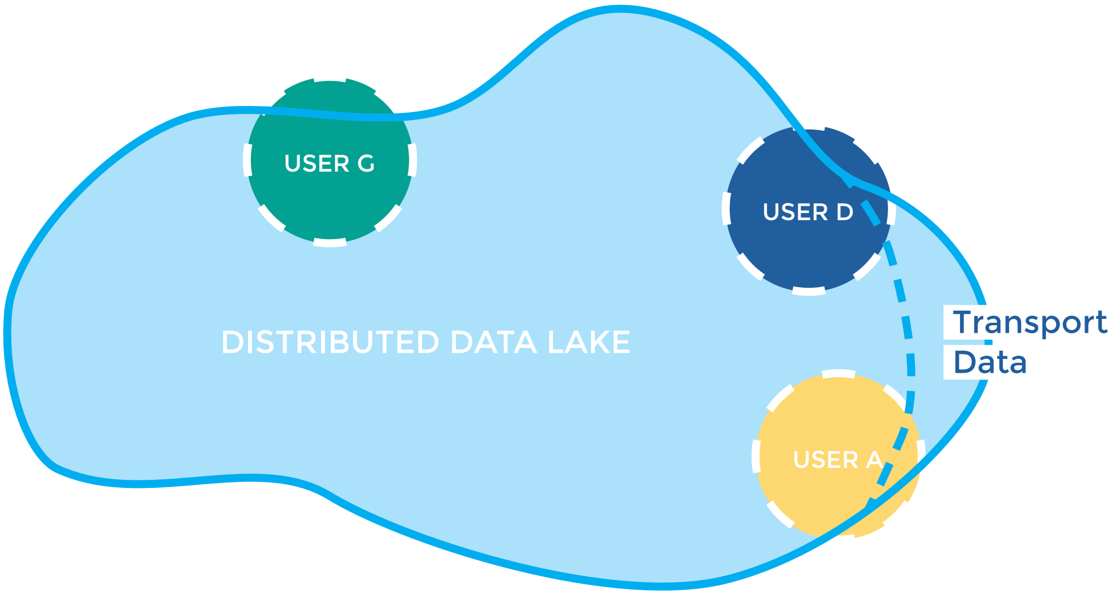
The European Commission should therefore provide the funding for an independent body, charged with the continued auditing and upkeep of the underlying system. Oversight over this body happens through a similarly independent, neutral trustee board made up of technology and ethics experts. To increase trust and usability of the system from the start, government bodies as well as trusted, public entities such as public libraries, can provide credentials to users, and ensure their own services work on the system.

4.2 FROM DATA LAKES TO DATA COMMONS

How it works: Data is central to the digital economy, and key to leveraging many newly emerging innovations. Yet, most personal data is currently locked up in large, usually proprietary, databases – what we are referring to as data lakes. This uneven, and economically suboptimal, distribution of resources means that those owning the most data are best-placed to harness new technologies like artificial intelligence. While the creation of data lakes is diametrically opposed to our value-led vision for the future of the internet, without access to large amounts of high-quality data, it will be incredibly difficult for European businesses to compete. That is why we seize on the idea of data spaces, as introduced in the Commission's new Strategy for Data, but propose to extend this concept to personal data, rather than just industrial data.

Under our EDDS Framework, every European will be given access to their own encrypted personal data store, or wallet, which allows them to keep stock of their own identity attributes and data points, and decide on a case-by-case basis which data points they want to share with solutions built on top of this model. This works not unlike an API, but on a much larger scale, and brings reciprocity to the relationship between data supplier and issuer. Solutions that tap into our new data space are expected to also contribute to the commons themselves, allowing users to again share relevant data generated through their solution with other trusted apps on a fair, consent-based basis.

To ensure value from the very start, the European Commission and Member State institutions will agree to immediately make their own datasets available through the system, allowing citizens to, for example, share data about their education, or health with verified solutions.



Some examples of how these decentralised data spaces can be used:

Example 1 (Fair access): A small transportation startup wants to help disabled travellers plan out accessible trips; to do so, they need to tap into large amounts of travel pattern data to understand and optimise route planning. Through this consent model, new users can easily share their travel history.

Example 2 (Collaboration): A large health company, which previously relied on just its own data lake for analysis, can now easily collaborate with a range of other actors across sectors by sharing anonymised data mutually, with full consent from users, adding more layers of depth to their research.

How we instill trust in the system:

Like in the identity layer, our independent maintenance body ensures the continued upkeep of the underlying systems, patches security flaws and updates code. The ways in which data is distributed through individual data stores or wallets also makes widespread data breaches virtually impossible, removing single points of failures by decentralising previously enormous accumulations of data in one space.

As is discussed in the applications section below, we verify which applications can be trusted and that they function in the way the user consented to, making it harder for companies to use our data in different ways than was advertised. The consent model offered by our favoured self-sovereign identity approach additionally means that users can retract access to their data at any point .

4.3 A NEW WAVE OF ETHICAL INNOVATION

How it works: Small businesses could benefit tremendously from access to large swaths of valuable, new data, without having to individually solve the security challenge of identity management or entering into asymmetric business partnerships with large, private tech platforms. But these benefits are not entirely without conditions.

While anyone is allowed to build on top of our protocols and so partake in the ecosystem, we will only champion the most trusted and verified solutions. We do that by empowering our maintenance body to audit solutions for their security, handling of personal data, trustworthiness and other key indicators. We favour solutions that use an open source-first approach. Trustworthy apps will be assigned a trustmark endorsed by the European Commission.

Furthermore, we can ensure that all R&D projects funded by the European Commission, and eventually those commissioned by Member States and other public funders, design their solutions to be compatible with the framework, and set careful conditions in public procurement and funding calls around interoperability and data portability. Through our separately proposed FOSS fund, discussed in the resilience vision, we fund open source, interoperable tools. With time, this allows us to create a suite of fully integrated, trusted and open technologies that can compete with the large, proprietary platforms.

Just like governments will have shared credentials and data on the system, they will also be frontrunners in making their own services easily accessible through this new framework. Booking an appointment with a GP or social worker, paying a bill or signing up your child for football classes can be done easily and securely using our new online identities.

Some examples of how this new ecosystem might thrive:

Example 1 (Interoperability): An international law firm wants to move its software stack to open source tech, tired of being locked into expensive, outdated solutions. Where that was difficult before, they can now easily integrate a range of different solutions, from open-source apps to arrange meetings and optimise scheduling to encrypted email services, into one coherent system.

Example 2 (Public awareness): A teacher wants to find a good study app for their students to use, but is worried about the privacy implications of some edtech solutions. Trustmarks and audit results help them identify which tools they can trust.

How we instill trust in the system: For our new framework to succeed, we need to make sure there are a sufficient number of trusted applications using the underlying systems. This means instilling trust and building critical mass as governments deploy their own services first. But adoption and user trust can be supported further through the creation of an auditing and trustmark-issuing body, which can independently verify the privacy credentials, security and other aspects of third-party apps.

Benefits:

In summary, we envision this framework to have the following major benefits:

- It gives citizens back control over their own data and identities: citizens can have more agency about shaping their one online interactions, protect their privacy, and are better able to harness the value from their own data.
- New businesses will be able to meaningfully compete: we level the playing field in the digital economy by opening up access to more diverse sources of data.
- A thriving ecosystem of trustworthy and fully interoperable solutions emerges: by issuing trustmarks and funding alternatives, we build a vibrant and diverse commons of trusted applications.
- Resilient, more secure systems and infrastructures: taking a flexible, modular and above all transparent approach, we ensure the underlying systems are secure and constantly updated to reflect the latest standards.

5.
HOW DO WE GET THERE?

5. HOW DO WE GET THERE?

This paper has looked at the complexity and the interconnected nature of the problems we face on the internet today, and set out a tangible alternative future we can move towards. Moving us closer towards this ambitious vision will require a diverse palette of technological, legal, regulatory, economic and social interventions across the internet's power stack, and a mobilisation of Europe's ecosystem working on building a more human-centric internet.

We believe that only an ambitious, dedicated mission for shaping the future internet can meaningfully address this thematic complexity and diversity of stakeholders. In the following section we lay out the potential design parameters of such a mission and a set of proposed objectives that it should achieve for each of our five pillars.

Alongside the missions model described below, we have developed a series of policy recommendations that we believe would help further bolster these efforts, which can be read in our accompanying Policy Roadmaps paper.

5.1 WHY WE NEED A NGI MISSION

The European Commission's ambitious Next Generation Europe post-COVID-19 recovery plans aim to not just kickstart economic growth and recovery of jobs, but want to use this as a moment to catalyse the digital and green revolution. The internet and related connected technologies are often seen as instrumental in these efforts, but we cannot fully harness the power of the internet if we do not solve many of its underlying issues. As this paper has made abundantly clear, the challenges we face on the internet today are incredibly complex, interconnected and mutually-reinforcing and require the involvement of a wide set of stakeholders to address. Only through considering the system holistically can we move towards our vision for 2030. That is why we urge the European Commission to consider including the Next Generation Internet as one of the topics in the new Horizon Mission framework.

Innovation is an important catalyst of economic growth, but is more effective when designed to have a specific end goal in mind. Too often do governments opt for an innovation-for-innovation's sake approach, jumping headfirst into joining the rat race to develop technologies like Artificial Intelligence, rather than treating new innovation as a means to an end. Mission-based innovation turns this thinking around: we set ourselves ambitious targets to solve particularly wicked societal problems, but remain agnostic about the ways we get there - instead mobilising the full innovation ecosystem and range of interventions available to us to set in motion the necessary societal transitions. From private sector companies, to regulators, to universities, to civil society to the general public: everyone has their role to play. Mission-based innovation famously brought us Apollo 11 (the illustrious "moonshot"), but, appropriately, also the internet itself, in the early incarnation of the ARPANET, funded by the US Department of Defence.[199]

Missions will play an integral part in the Commission's Horizon Europe programme, which will be launched in 2021, convening Europe's innovation community to help solve important challenges, such as cancer, the health of our oceans and climate change. The internet and digitalisation indubitably have an important role to play in helping achieve the Missions the Commission has set out so far, but should also be considered as one these missions itself, given the growing importance of the internet on our societies and economies, and the power it has to improve our lives.

The current institutions and regulatory frameworks we have at our disposal simply cannot keep up with the rapid pace of development, complexity, and unprecedented accumulation of power we are currently witnessing in the internet economy. We need a new generation of institutional innovation and bold new approaches to how we regulate and spur technological innovation. Through treating the Next Generation Internet as a Mission, we can do just this.

[199] https://www.socialeurope.eu/mission-thinking-a-problem-solving-approach-to-fuel-innovation-led-growth

5.2 RECONCEPTUALISING THE NEXT GENERATION INTERNET AS A MISSION

As we have discussed, there is a strong case for turning Europe's digital agenda and ambitions for the Next Generation Internet into a mission. The specific nature of a mission such as this needs to be carefully designed, involving expert stakeholders, and retaining the necessary flexibility to adapt to changing circumstances over time. However, we can already define several areas of intervention that are likely to form part of the solution. In this section, we discuss how a Next Generation Internet mission could be designed, and what goals it should strive to meet.

As this paper has made clear, the internet is too complex and multifaceted to be treated as one single entity for the purposes of policy and funding interventions. That is why we suggest setting out an overarching mission, with goals for each of our five respective pillars or sub-targets.

> *"We build a more democratic, inclusive, resilient, trustworthy and sustainable future internet by 2030".*

Each of our sub-targets will require the mobilisation of different stakeholder communities, and require interventions across different layers of the stack. We believe that they together can bring the kind of systemic change that we need.

We have ten years to reach our goal. Our mission is ambitious, and reaching our five sub-targets requires a radical rewiring of how the internet works today. While we believe Europe has the momentum and the ingredients to make substantial headway in making these objectives a reality, we need to make sure we spend our time and resources effectively.

Our objectives should not be treated in isolation: interventions under one pillar will help strengthen our efforts in others; through collaboration and keeping the holistic view we have championed throughout this paper, can we help these different pieces of the puzzle fit together and reinforce one another:

1. Democracy: We democratise the internet by giving citizens control over their data and the future trajectory of innovation, and create a single market for ethical data use and technology worth 1 trillion Euros by 2030.

2. Resilience: We build internet infrastructure and systems that can withstand environmental, economic and cyber shocks, and strengthen our role as a global champion of good governance and the open internet.

3. Sustainability: We move to a fully circular and carbon-neutral economy for digital technology by 2030, strengthening the joint objectives of Europe's twin green and digital transition.

4. Trust: We establish a globally recognised "Made in Europe" brand for trustworthy and privacy-preserving technology, and play a leadership role in ensuring citizens around the world have access to trustworthy technology, data and information flows.

5. Inclusion: By 2030, all Europeans can meaningfully access and participate in shaping the internet.

5.2.1 DEMOCRACY:

We democratise the internet by giving citizens control over their data and future trajectory of innovation, and create a single market for ethical data use and technology worth 1 trillion Euros by 2030.

Building a more democratic internet requires us to open up the fruits of innovation and opportunities offered by the digital economy beyond the handful of currently dominant actors. It also means ensuring we can collectively decide on its future trajectory, as well as harness the internet itself as a tool to strengthen democracy.

European citizens currently have little to say about what happens to their own personal data or identities online, let alone about the direction of innovation more broadly. We need to be collectively able to decide what we consider ethical uses of technologies such as facial recognition systems or artificial intelligence, and ensure these more responsible use cases also actually come to bear.

While we have put a lot of effort into regulating the excesses of the current digital economy, these efforts need to be combined with the more proactive creation of self-sustainable markets for technology and solutions that serve the public interest and use personal data in ethical ways. Lack of access to resources, specific technical skills and above all data has meant that many of the promising new technologies currently being developed are not being put at the service of solving important societal problems or serving the public good.

To level the playing field and to empower more ethical solutions to find a market, we therefore set ourselves the ambitious mission to create a Single Market for ethical data use and technology worth €1 trillion by 2030. We do this by creating infrastructures and systems that enable new ideas to thrive, supporting new and more responsible business models, widening access to data for businesses and citizens alike, and opening up knowledge and innovation.

These efforts should not just be restricted to Europe. Not only do we aim for these new solutions to benefit all, we also set ourselves the goal to build strong safeguards that will help strengthen democracy and the open internet worldwide, and proactively deploy digital tools and solutions that can make our own democracies more accountable and participatory.

While the strength of a mission-based approach lies in remaining relatively agnostic about how we achieve our aims, we do set out four specific practical objectives that we believe are vital for reaching our target. These four objectives are discussed in more detail in the European Democratic Data Space Framework section, democracy vision and our accompanying Policy Roadmaps paper:

Four objectives:

1. Every European gets access to their own secure digital identity and personal data store (data wallet) by 2025.

2. We level the playing field in the digital economy by opening up access to data through the creation of commons-driven decentralised data spaces for personal data as well as strengthening interoperability and data portability rules.

3. We democratise the technology innovation process by supporting open innovation and knowledge, and harnessing the wisdom of the crowd through collective intelligence.

4. We rejuvenate democratic processes across all layers of governance, from the local level all the way up to the European institutions, by proactively implementing digital deliberation tools, and protect freedom of speech and the Right to Whisper around the world.

5.2.2 RESILIENCE:

We build internet infrastructure and systems that can withstand environmental, economic and cyber shocks, and strengthen our role as a global champion of good governance and the open internet.

We want an internet where our values are more forcibly embedded, but for these efforts to be worthwhile we also need to ensure the internet itself is secure and resilient against any external shocks. We set ourselves the target of becoming more strategic about setting out Europe's role in the digital arena, strengthening our own internet sovereignty but above all ensuring we mitigate the threat of escalating cyber conflict by championing the open internet and more robust governance processes.

For Europe to improve its internet sovereignty in the digital space, we need to ensure our infrastructures and systems – from supply chains to information flows to favourite applications – are secure and ready to withstand not just mounting cyber security threats but also increasingly frequent climate change-induced shocks. This requires us to put these concerns at the core of our thinking as we roll-out of new infrastructure, practice long-term thinking, and evaluate emerging risks. We make it our goal to develop robust processes for this kind of evaluation, and have these processes become common practice across all of our efforts as part of our NGI mission.

Alongside the need to strengthen the internet's physical backbone, we also need to improve the security of the solutions built on top of it. We believe that resilient and trustworthy solutions thrive on an open approach – which allows for scrutiny and constant updatability. We therefore make it our goal to effect a public sector transition towards open-source technology and open standards, and champion these approaches globally. To do this, we need to mobilise a wide set of policy actors as well as facets of the development community. Only through collaboration, knowledge sharing and a transparent approach will this effort gain the necessary traction; our mission-based approach is the ideal lever to achieve this.

While the strength of a mission-based approach lies in remaining relatively agnostic about how we achieve our aims, we do set out four specific practical objectives that we believe are vital for reaching our target. These four objectives are discussed in more detail in the resilience vision in section two, and our accompanying Policy Roadmaps paper.

Four objectives:

1. We transition to a model of open-source technology and open standards first across all layers of European governance, from the local to the supranational.

2. We play an active role in strengthening global governance of the internet, by opening up internet governance processes to a wider community, reviving the multi-stakeholder model and protecting global digital rights.

3. We roll out an ambitious infrastructure renewal plan as part of Europe's Green New Deal plans, protecting critical infrastructures and building in more flexibility to leave us agile to adapt to changing threat horizons.

4. We build up Europe's cybersecurity capacity through an ambitious retraining programme, building skills within organisations and among the general public, and strengthening the rules for secure design and deployment.

5.2.3 SUSTAINABILITY:

We move to a fully circular and carbon-neutral economy for digital technology by 2030, strengthening the joint objectives of Europe's twin green and digital transition.

The green transition and digital transition go hand in hand. Indeed, digital technology has an important role to play in achieving the ambitious goals of the European Green Deal and Next Generation Europe's aims for the twinned green and digital transition. But to do this, we must be more proactive about reducing the internet's own environmental footprint, strengthening the circular economy for digital devices, decoupling internet use from energy-use, and raising awareness about the sizable impact of the internet among the general public.

We set as our goal to create a fully circular economy for digital technology by 2030. By ensuring the sustainability of hardware, the greatest contributor to the internet's footprint across the value chain, and minimising wasteful storage and usage, we can substantially reduce the internet's environmental impact, and contribute to achieving technology sovereignty for Europe. The recently published Circular Economy Action Plan has laid important groundwork for this effort, but its implementation and long-term future remain imprecisely defined. Recognising the environmental footprint of the intangible economy, Europe must also strengthen its ambitions for the long-term sustainability of digital services.

Reaching a fully circular economy for digital devices and internet services is no easy task – addressing or even measuring the environmental impact of services and devices across their lifecycle remains complex, with underlying supply chains opaque and made up of an exceedingly large and diverse set of actors. Treating the digital circular economy as a mission will allow us to mobilise the necessary ecosystem of stakeholders, strategically coordinate policy interventions, and target funding well. This has the potential to give rise to a more localised economy of sustainable services and digital solutions that will bring about a better quality of life, innovative jobs and upgraded knowledge and skills

Beyond reducing the footprint of digital devices, and the increasingly carbon-intensive uses they facilitate – from indiscriminate data storage to high-impact video streaming, we also set ourselves the goal of unleashing the power of digital technology to help mitigate the worst impacts of the climate emergency. This should involve investment in new green tech solutions to support the green transition in the energy and transportation sectors, as well as tools that could, for example, enable more remote working and reduce work travel.

While the strength of a mission-based approach lies in remaining relatively agnostic about how we achieve our aims, we do set out four specific practical objectives that we believe are vital for reaching our target. These four objectives are discussed in more detail in the sustainability vision in section two, and our accompanying Policy Roadmaps paper:

Four objectives:

1. We move to a fully circular economy for digital devices by 2030, by improving production processes, ensuring longevity and repairability of individual devices and expanding our e-waste recycling capacity.

2. We reduce the energy use of the data economy by raising awareness among the public about the impact of their use, extending data minimisation practices to include sustainability measures, and developing less energy-intensive technologies and data analysis methodologies.

3. Europe becomes a global frontrunner in the market for green digital devices, software and technologies, the backbone of a market for trustworthy technology worth 1 trillion Euros by 2030.

4. Seizing on the twin digital and green transition, we invest in digital technologies that can meaningfully help address the climate crisis, a central tenet of the European Green Deal.

5.2.4 TRUST:

We establish a globally known "Made in Europe" brand for trustworthy and privacy-preserving technology, and play a leadership role in ensuring citizens around the world have access to trustworthy technology, data and information flows.

We live in a time of political and social polarisation, with reduced trust in public institutions, our economies, democracies – and also the internet. Technological innovation is increasingly seen as a black box, leading to new solutions that do not necessarily have our best interests at heart, from facial recognition to data hoovering panopticons. To ensure we reap the full benefits of the digital revolution, without alienating large groups from participating, and above all set the conditions for reliable and positive technologies to emerge, we need to bring trust back into all layers of the internet system.

From hard-to-scrutinise hardware devices and critical communication systems that we fear might harbour backdoors to free apps that do not do what they say on the tin: it is increasingly difficult for technology experts and policymakers, let alone the average citizen, to know which solutions they can trust and which they can not. This lack of trust can lead to geopolitical tensions, as exemplified by the 5G debate or concerns about applications like TikTok. Where distrust affects public acceptance and adoption of emerging technologies, it also harms the digital transition of our economy. That is why we take it upon ourselves in this sub-target to help restore global trust in new innovation, and act as an independent voice championing ethical and transparent solutions.

Europe prides itself in having a global reputation as a trustworthy actor in the digital space, promoting a value-driven approach and protecting citizen rights through landmark legislation such as the GDPR. We must leverage this reputation by setting up systems to audit and scrutinise new solutions and issue trustmarks for technology that meets our standards, as well as build our own high-quality "Made in Europe" technology.

One of the most visible and pernicious challenges on the internet today is the undermining of trust and democracy through weaponisation of information. Beyond trying to solve the fake news and misinformation issue, we need to ensure that we maintain a vibrant ecology of trustworthy, pluralistic and multilingual media outlets that can challenge these dynamics through high-quality reporting. Given the financial sustainability issues in the media industry, we set ourselves the goal to ensure Europe's news and information ecosystem can thrive independently.

While the strength of a mission-based approach lies in remaining relatively agnostic about how we achieve our aims, we do set out four specific practical objectives that we believe are vital for reaching our target. These four objectives are discussed in more detail in the Trust infrastructure and trust vision in section two, and our accompanying Policy Roadmaps paper.

Four objectives:

1. We launch an auditing body that scrutinises the security, trustworthiness and privacy-awareness of hardware, software and digital services, and administers European Commission-endorsed trustmarks to those solutions that pass the test.

2. We build a healthy ecosystem around trustworthy, high-quality journalism and information flows, ensuring reputable media outlets can find sustainable business models without undue levels of market concentration or government interference. We do this through the creation of a dedicated News Innovation fund.

3. We relocate and diversify aspects of the internet technology supply chain, bringing more development of devices and solutions back to Europe.

4. We find new modes for citizens to give meaningful consent to being tracked or subjected to data-driven decision-making tools and systems, bringing reciprocity to our relationship with smart city solutions.

5.2.5 INCLUSION:

By 2030, all Europeans can meaningfully access and participate in shaping the internet.

We can make the internet itself more human-centric, democratic and resilient, but if we fail to ensure that all of us have equal access, such an internet would not be inclusive or harness the strength of Europe's diversity. We therefore set ourselves the mission to remove structural and social barriers to access, ensuring that all Europeans can have affordable or even free access to the internet by 2030, and are empowered to use and shape that internet in a meaningful way.

Barriers to access extend beyond questions of broadband availability, with cross-cutting issues like socio-economic status, digital skills, disability inclusion, gender disparity, racial or national discrimination all playing a role in perpetuating a digital divide which sees already underpriviliged groups marginalised even further. With the internet now so pervasive in so many sectors of our economy and society, not being connected increasingly means being left out altogether. The pandemic has shown how the groups most vulnerable to COVID-19 were also the least likely to have access to a smartphone, and thus less able to access many public health solutions, such as contact tracing applications.

As a society, we need to be aware of these impacts, and take a more holistic view of inclusion. One important way of doing that is to increase the diversity of those developing and designing new technologies, which ensures the perspectives and needs of currently underrepresented groups are reflected in the solutions we come to rely on. Over the next ten years we should therefore set ourselves the target of ensuring all Europeans have sufficient digital skills to use the internet, while also training a new generation of more diverse computer scientists, developers and other key technology-shaping vocations.

While the strength of a mission-based approach lies in remaining relatively agnostic about how we achieve our aims, we do set out four specific practical objectives that we believe are vital for reaching our target. These four objectives are discussed in more detail in our inclusion vision in section two, and our accompanying Policy Roadmaps paper.

Four objectives:

1. We ensure all European have the opportunity to get affordable, high-speed internet access by 2030, and have the skills to safely and effectively use the internet.

2. We broaden access of more marginalised groups across all layers of the internet, with a particular emphasis on making the internet governance and technology development layers more inclusive and diverse.

3. We build a multilingual internet, where minority languages are equally well-represented and all services accessible.

4. We reduce barriers to access, by improving the accessibility of services for people with disabilities, and address the cultural and socio-economic dynamics that mean marginalised groups are less likely to participate.

6.
CONCLUSION

6. CONCLUSION

The world was perhaps never more globalised than during the COVID-19 lockdown. For billions of humans, the internet – in many ways globalisation's greatest triumph – became their sole remaining window onto the world.

Having a Zoom chat meeting with team members holed up in their apartments three streets down, was suddenly no different than having a call with colleagues in Singapore or San Francisco. We temporarily consumed the same information, battling the same global enemy. But this temporary untethering from physical space did not last and as governments have started to chart pathways out of this crisis, the general tendency seems to be towards a world that will actually be less globalised than before – a Great Unwinding.

We see similar tensions in other areas accelerated during the pandemic: will we see the incumbent tech giants seize the opportunity offered by COVID-19 to further solidify their power or are we entering a period of more government control? Could the push for further centralisation be counterbalanced by an emergence of more bottom-up, grassroots redistribution efforts? In this tug-of-war between centralisation versus decentralisation, rising inequality versus redistribution and openness versus a retreat behind walled gardens, it is more important than ever before to take a strong stance on where we want to be as a continent.

In this paper, we have set out a tangible and actionable vision for the future, that helps the European Union articulate a compelling story for a more human-centric future, and consider the trade-offs we face on the path there. We intend for this document to be a starting salvo, and serve as a call to arms for the European Commission, as well as Europe's internet community, from national and city-level policymakers to civil society, innovators to the general public, to take concerted action to make these ideas a reality.

For the remainder of the NGI Forward project and beyond, we will work on putting the central ideas proposed in this paper into action, and build a network of like-minded organisations and individuals to join us on this mission.

NEXT GENERATION INTERNET
INTERNET OF HUMANS

NGI FORWARD

This report was created by Nesta for NGI Forward, part of the Next Generation Internet initiative, a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N°825652

Websites:
https://www.ngi.eu
https://research.ngi.eu

Twitter
https://twitter.com/ngi4eu
https://twitter.com/ngiforward