



**Tech Policy
Trends in 2020**

**Tech Policy Trends 2020:
Did We Get Them Right?**

VERDICT

Tech Policy Trends 2020: Did We Get Them Right?

As our team is busy surveying the technology sector environment for our Tech Policy Trends 2021 report, to be released in January, we look back at turbulent 2020.

Our [Tech Policy Trends report](#), published at the beginning of 2020, explored contemporary trends in technology policy through a series of articles. 12 months on, we reflect on those trends, review the accuracy of our predictions and examine what has happened since.

2020 was majorly disrupted by the COVID-19 pandemic, and one might have the impression that tech policy was not always top of government agendas. However, if anything, the global pandemic has accelerated certain market trends and exposed weaknesses where particular areas of the market were unable to adapt quickly enough. Governments and industry alike have had to step up and demonstrate that communities can count on them when misfortune hits.

Going forward, the acceleration of digitalisation we have witnessed during the pandemic suggests that the digital economy will play a key role in post-COVID-19 economic recovery. As a result, we expect more governments and international organisations to work towards the formulation of digital policies that promote a responsible digital transformation. Our 2021 predictions will explore what this is likely to look like.

In this report, we rank our 2020 predictions as follows:



We got none of it right



We got some of it right



We got it right but missed key elements



We got it right but missed details



We got it perfectly right

AI Regulation Takes Shape



We predicted that the EU and US would make important steps towards forging their own approaches to AI regulation in 2020. Although the year has proved not to shed any real light on what AI legislation in the EU will look like, it has nevertheless been a seminal time for laying the foundations. As companies await the publication of the EU's first legislative proposal on AI in early 2021, many will have already forgotten the Commission's promise to legislate in early 2019, within the first "100 days" of taking office. The promised legislation was replaced by a White Paper on AI and weeks of fruitful public consultations, both formal and through numerous engagements with industry.

Therefore, as we anticipated, businesses will look back at 2020 as a year of engagement with policymakers and discussion on issues such as what constitutes high versus low risk and which services or sectors should fall within scope of AI regulation. We can expect

that EU AI regulation will indeed be human-centric, and we can see the EU working to develop its own AI capabilities through projects like the upcoming "Digital Decade" and post-COVID-19 recovery funding, in an effort to boost European "technological sovereignty".

Businesses will look back at 2020 as a year of engagement with policymakers around AI

The Digital Services Act: The Next GDPR



Although there is still no concrete proposal on the table, the Digital Services Act was a defining trend in 2020, as we predicted. Political groups, national governments and industry lobbyists spent much of their time trying to shape the proposal, now expected on 9 December. In addition, the European Commission will add the Digital Markets Act, which will impose ex-ante competition rules on large tech firms ("digital gatekeepers").

EU officials are not shying away from trying to set global norms.

Hate speech has so far not figured in the debate as much as we anticipated, although France and other likeminded Member States are pushing to regulate this space. Although we predicted that this would be a “Christmas tree bill”, we did not precisely anticipate that counterfeit goods would become such a durable part of the debate in Brussels. In this sense, the discussion deviated partially from our expectations.

Europe First: A New Wave of Tech Protectionism in Europe



2020 promised to be a year of protecting Europe’s digital sovereignty and promoting regional industry. These promises have been delivered upon. Throughout the year, European Commission officials have been busy drafting and reviewing legislation to (i) address the dominance of foreign digital platforms, (ii) boost Europe’s capabilities on all fronts and (iii) protect European data.

The main objective of the upcoming Digital Services Act (DSA) and Digital Markets Act (DMA) is to address the behaviour and market dominance of large online platforms, but this new legislation will undoubtedly affect most digital businesses and have a severe impact on how they operate.

The COVID-19 pandemic has exacerbated the sense that foreign tech companies have too much power and that nations are overly reliant upon them. However, the EU is now prepared to spend billions of euros through its new seven-year budget and recovery funds to grow European companies and help regain control over the supply chain and digital marketplace.

The EU’s sovereign cloud infrastructure, GAIA-X, will be the gateway to the EU single market for data. It will provide data storage solutions for Europe’s public sector and essential infrastructure operators, but also for growing the number of types of data and services which fall under the definition of either strategic or sensitive. Data localisation will affect every sector – from health to aviation – dealing with European data. Growing data localisation requirements, combined with data flow restrictions under Schrems II, will make it truly challenging to access and serve the European market.

With 2020 soon coming to an end, we should prepare for Europe First 2021.

Beyond China: Supply Chain Security from Vietnam to Open Source



In the twilight of 2019, Access Partnership predicted that Europe would finally wake up to and legislate on Chinese supply chain security threats. Furthermore, we expected that, despite the tariff detente, US corporate supply chains would shift to emerging economies (we emphasised Vietnam), that the People’s Republic of China would “strike back” with an “unreliable entities list”, and that there would be a new wave of efforts targeting “supply chain” for software, not just hardware.

How did we do? While the EU moved no major supply chain security legislation, 2020 saw the UK announce market share caps on Huawei, only to rip and replace those with a full-throttle Telecom Security Bill proposing a full ban: Germany openly scoffed at this, before making a U-turn by issuing a rigorous vendor security and governance review policy, itself just short of a full ban. We saw that coming, but we did not anticipate the tsunami of global support for OpenRAN and vendor diversification to spur competition, localise networks and avoid vendor lock-in, especially on the part of Huawei.

While tech supply chains continued to shift to new economies such as Vietnam as we expected, we had not predicted the most brazen US industrial policy in a generation, the CHIPS Act, which offered generous state aid for onshoring semiconductor foundry and manufacturing operations. In retaliation for this and US export and investment restrictions, China’s Ministry of Commerce published provisions for an “unreliable entities list” in 2020, as we predicted, although it has so far stopped short of naming and shaming US corporates. Finally, our bold prediction that the US government’s crusade to proselytise a “software bill of materials” (SBOM) bringing supply chain security to open source software did not see the anticipated pick-up, aside from an honourable and stubborn beachhead in the medical technology sector.

Spectrum Sharing Moves into Mainstream



An annex to the 1906 International Radiotelegraph Convention contained the first

internationally agreed regulations governing the use of radio frequencies. These have since been expanded to become what we know today as the ITU Radio Regulations. It was perhaps unreasonable, therefore, for us to pinpoint 2020 as the year in which spectrum sharing would become mainstream.

However, in line with our predictions, 2020 has seen increased eagerness among national regulatory authorities, equipment vendors and service providers to harness technology to create effective spectrum management practices and facilitate enhanced efficiency in the way spectrum is used. As mid-band and millimetre wave frequencies are being released by administrations for 5G, their corresponding licensing frameworks consider both nationwide coverage and specific localised capacity requirements for industrial and other smart applications and special events. This trend appears globally in North and South America, Europe, the Middle East and Africa, Asia and Australasia. It is being made possible by the application of technologies such as MU-MIMO, software-defined network and radios, mobile edge computing, small-cell technologies, including high-throughput satellites, geolocation databases, spectrum sensing and distributed ledger technology.

5G Security: Time to Decide



In our Tech Trends 2020 report, we identified 2020 as a year for governments across the world to lay out their perspectives on 5G security issues arising from trade and trust tensions between the West and China.

This trend has played out with Western governments solidifying their position on Chinese technology imports, and Huawei in particular, with network security a key concern. Many of these governments have either banned Huawei network infrastructure or chosen to work with local competitors or are reviewing whether to allow the technology onto any part of their 5G networks. However, internationally, the trend is less apparent, with many countries in South America, Africa and Central Asia having already launched 5G networks or conducting tests with Huawei equipment. Our 2020 prediction did not emphasise the ongoing battle in the technical standards space with groups such as 3GPP, with equipment vendors jostling to be the first to patent their solution, persuade the technical Working Groups to approve their technology ahead of their competitors and secure the resulting lucrative licensing fees.

US Privacy Law in the Making



Last year, we were careful to stress that achieving a comprehensive US privacy law in 2020 was unlikely. However, we also predicted that Congress would make further progress to outline a law that may be passed in 2021. In fact, though we enter 2021 in a similar position to that of a year ago, we did see some limited movement forward.

Many hoped that we would make progress on a comprehensive federal privacy bill early in 2020, but we didn't see the grand gesture some had hoped for. As with everything else, COVID-19 threw a major spanner in the works. While the pandemic delayed any action, it also in some ways amplified the focus on privacy, due to public health contact tracing efforts. We saw both Democratic and Republican COVID-19 privacy bills focused on protecting personal health data collected during the public health emergency.

While there wasn't much further movement from either the Republican or Democratic camps throughout the year, nor did we see a withering on the vine of a privacy law. Throughout 2020, both parties (especially in the Senate) have reiterated their positions in hearings and further bills – each perhaps hopeful to have a stronger position in the next Congress – and consolidated support within their parties.

The new Congress looks much like the old in terms of party balance and chairmanships, meaning the same dividing lines remain. However, these dividing lines are perhaps even clearer than they were before, and focused around the main Senate bills.

Data-Sharing Regulations Heat Up in 2020



We expected several policy trends surrounding data-sharing to emerge in 2020. Countries have certainly made progress on data-sharing policy, but its technical complexity means that efforts to drive data-sharing will be carried out over the next few years. We saw the Australian government delaying the implementation of the Consumer Data Right for the banking sector. They will continue to push ahead with the energy sector next, so we should expect to see the preparatory work being done in late 2020 and early 2021.

Other countries have also made progress. Singapore has amended its Personal Data Protection Act to introduce data portability, while India is finalising its non-personal data governance framework, which will determine how data will be shared. COVID-19 has also spurred governments to rethink their data strategy. The New Korean Deal, which was a response to the COVID-19 pandemic, puts forward an agenda to build a data dam for the country.

Meanwhile, Japan, a country that was quite severely affected by the postponing of the Olympics due to COVID-19, sees its new Premier pushing for a Digital Agency that will almost certainly accelerate Japan's discussion around data-sharing. More importantly, the European Commission released its Data Strategy, which was followed by a report on Business-to-Government (B2G) data-sharing. Given the Commission's influence on data policy issues, it is likely that their actions are being followed globally.

What's Next for IoT Regulation?



At the end of 2019, we posed the question “What's Next for IoT Regulation?”. Our predictions included a push for new regulations around network and device security, e-SIM technology and roaming. How well did we do in our predictions?

We have cautioned that adjusting regulations around IoT services will be a gradual process. However, our expectation that several jurisdictions would follow the UK's example on IoT security or the UAE's example on IoT-specific regulation have not been met. This may be explained by the disruption to regulatory priorities due to the pandemic. However, we were not altogether misguided. An IoT Cybersecurity Improvement Bill has emerged in the US and the UK took further steps to regulate smart device cybersecurity, while an IoT security consultation is expected soon in Brazil.

Additionally, there were signs of movement from the other side of the world, where Pakistan published a Consultation for the Preparation of an IoT Regulatory Framework. Furthermore, as predicted, the first specific rules on portability obligations on accesses exclusively intended for the connection of IoT devices were addressed, this time by the Brazilian regulator. Thankfully, Brazil also acknowledged the need to encourage IoT innovation and decided that the services provided by IoT devices will have a lower tax burden than telecommunications. Considering that the majority of the above developments happened in Q3/Q4, 2021 might a year of rising IoT policy-making. On the

other hand, perhaps the regulatory uncertainty currently faced by stakeholders in the IoT value chain will persist. This is yet to become apparent.

The Rise of “Green Technology”: Policy Implications for ICTs



We noted that increasing concern for the planet in global policy-making was likely to continue to be a priority in 2020. The COVID-19 pandemic effectively delayed national and international regulatory policy processes for the implementation of Paris Agreements into the legal frameworks of various leading jurisdictions. However, the impact of this was mitigated somewhat by the announcement by several governments, including the EU, of “greenish” COVID-19 recovery measures that bundle sustainability policy objectives into recovery spending.

International organisations took more of a back seat on sustainability issues this year, as focus and resources were shifted toward COVID-19 recovery measures. As such, the major international treaty-binding conferences on carbon emissions (COP 26), biodiversity protection and ocean protection were delayed until 2021, and the UN has noted with dissatisfaction the negative impacts of COVID-19 on the attainment of the 2030 Sustainable Development Goals.


Climate action continued to gain momentum, with about 49% of the world’s annual GDP now being generated by nations, regions and cities with an actual or intended net-zero target, highlighting just how quickly policymakers are grasping the science of climate change and, in the case of certain cities and regions, deciding to take their own action to address it.



We lead countries to fair tech

Access Partnership is the world's leading public policy firm that provides market access for technology. Our team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data and connectivity.

9th Floor, Southside
105 Victoria Street
London SW1E 6QT
United Kingdom
Tel: +44 (0) 20 3143 4900
Fax: +44 (0) 20 8748 8572

 AccessAlerts
 AccessPartnership

www.accesspartnership.com