
Access
Partnership
Tech Policy
Trends in 2019

"During the first weeks of this year Access Partnership has surveyed the environment for the technology sector worldwide. We present below what in our view constitute the top ten trends to watch for 2019. From digital tax to WTO reform, our teams explore how shifts in tech policy could disrupt business globally while highlighting some governments' race to leverage the benefits of artificial intelligence, digital identity and smart cities. In still other jurisdictions, public anger is fuelled by data and cyber breaches, online misinformation and tax avoidance, driving more tech regulation at the very moment when the underpinnings of the global economy seem less solid than any time since 2008.

2019's challenge to all companies with a stake in technology will be to bring forward policy solutions that anticipate law making and regulation setting from governments that will react to public opinion. Some answers from the content below begin to suggest themselves, but this year will require original thinking throughout if the long-term benefits of our sector are to be balanced against the current public mood.

We wish you happy and careful reading about this great challenge of our age."

Greg Francis

Managing Director, Access Partnership

Contents

EU Digital Policy Up in the Air

Simona Lipstaite, Public Policy Manager

2019 will be a year of change, impacting technology companies on different levels. How the first half pans out will have a strong impact on the EU's digital policy for the coming five years in a landscape full of both challenges and opportunities. This year will mainly be shaped by the European elections in May, the shift towards "traditional" policy areas through a digital angle, and Brexit.

With less than five weeks before the UK leaves the EU, policy-makers are preparing for a "no-deal" scenario to address network securities, the free flow of data, professional recognition and intellectual property, taking their attention away from "business-as-usual" digital files.

Key files still in limbo

Given the ambivalent electoral future of MEPs, including Rapporteurs of key files such as Axel Voss on the Copyright Directive, stakeholders will pressure the European institutions to conclude trilogue negotiations on outstanding digital files in the first three months of 2019. The alternative — waiting for the new Parliament and Commission — would result in months of delay. And changing negotiators mid-way through the process has not done EU legislation many favours in the past.

Other outstanding digital and tech files include reports on Terrorist Content Online, Connecting Europe Facility, the EU Space Programme, e-Evidence, Platform-to-Business, Dual-Use of Technology, and the controversial ePrivacy Regulation.

Technology companies and other interested stakeholders looking for a swift conclusion of pivotal files should step up efforts to urge the institutions to come to an agreement by March at the latest. Conversely, the short timeframe may also favour stakeholders less keen for certain files to be concluded. The ePrivacy Regulation is a potent example. The upcoming Romanian Presidency has already expressed reluctance regarding rushing the file through, which means that it may either remain on the agenda for the Finnish Presidency in the second half of 2019 and possibly beyond or be sent back to the Commission for redrafting altogether.

Successfully closed files under the current 2014-2019 digital programme include the General Data Protection Regulation, the Free Flow of Non-Personal Data Regulation, Security of Network and Information Systems (NIS) Directive, the Electronic Communications Code, and, most recently, the Cybersecurity Act.

Campaign season

The outcome of European Parliament elections will shape the agenda and the ability of EU institutions to come to agreements for the next five-year term. More than 700 MEPs and their political staff will rise for election campaigning in the middle of April. This means that tech companies will be spotting early on the future leaders in digital policy and drawing up engagement strategies to create champions and placate critics. Following the election results, much of the summer will be getting to grips with the new European Commission, whose appointment will follow in the autumn.

While we have to wait for 26 May for the results, we already know a number of key MEPs, such as Dutch politician Marietje Schaake, the Rapporteur for the EU's Digital Trade Strategy, Dual-Use Technologies, and Human Rights and Technology reports, will not be running. It is also widely expected that populist politicians will gain even more ground than in the 2014 elections. With the loss of British MEPs, the shrinking of the centre-right EPP group, and the increasing prominence of far-left-wing and far-right forces, the next European Parliament is also likely to adopt a more protectionist approach and to support stronger rules for the tech industry, particularly regarding trade, data protection, and competition rules.

The year of the digital EU

An increased focus on digital under the 2019-2024 Commission's work programme will permeate the Union's work on policy issues not traditionally associated with technology. Usually reserved for DG CONNECT and to an extent DG COMPETITION, digital policy will inform and shape different Directorates-General working on policy areas as diverse as consumer protection, mobility and transport, or trade. This opens up a realm of exciting

possibilities for technology companies. For example, the Romanian Presidency will be prioritising eHealth, an important vertical for cloud companies. We will be also seeing many more interesting synergies emerge as the division between “traditional” and digital policy becomes more fluid.

Technology companies are also likely to come under increased scrutiny by policy-makers. The Finnish Presidency, taking over the reins in the Council in the second half of 2019, has already announced that it will be pushing for a reflection at the European level on the power of big tech, as well as the impact of new technologies on human rights. Technology companies will need to strengthen their engagement with policy-makers to demonstrate how they are tackling emerging challenges, such as illegal and terrorist content online, data privacy, digital competition, e-commerce and liability.

Digital Tax in the EU Gets Real

Kirsten Williams, Policy Analyst

Debate around digital tax sparked two European Commission proposals in March 2018 and the issue has only grown in prominence since then. In 2019, technology companies will face growing momentum behind efforts to introduce national levies on the digital sector, continuing and politicised EU-level interventions as we approach the European Parliamentary elections, and preparations for the Organisation for Economic Co-operation and Development (OECD) proposals on a global digital tax solution.

EU-wide digital tax falters

The EU came out of 2018 with their "interim digital services tax" — a temporary levy on certain digital services not currently covered by EU rules — blocked by a coalition of Ireland, Sweden, Denmark and Finland.

France had been a vocal proponent of the tax, but was increasingly isolated as the Nordic countries led opposition, arguing that the focus on taxing revenues where value was created would favour larger countries with more online service users.

Other member states had more fundamental criticism of the plan; concerns about impact on major tech companies headquartered in their jurisdictions were prominent. Others,

with a cautious eye on the US and the prospect of renewed trade wars, agreed that finding a global-level solution to taxing the digital economy would be more productive.

French economy minister Bruno Le Maire, one of the strongest supporters of the tax, was forced back to the drawing board, where he drafted a proposal with his more reluctant German counterpart, Olaf Scholz. The two countries proposed a much narrower EU level digital tax, targeting the advertising revenues of digital companies and excluding several tech giants, including Amazon and Spotify. The proposals would only come into place if international proposals weren't agreed by 2021. However, despite aiming to address concerns from the Nordic coalition, the measures have been criticised by previous supporters for not going far enough, and Le Maire agreed he would give the EU until March 2019 to come up with a solution that the EU-28 could accept.

Member states diverge

France then reneged on that promise and announced its own digital tax regime would be introduced on 1 January 2019.

A tax had been a campaign pledge for French President Emmanuel Macron, and ahead of the European elections has become a defining issue for En Marche's campaign as the president tries to show his reform agenda can bring real benefits. Now, after mass protests from the Gilet Jaunes movement and large budget allocations to try and placate them, the French government sees taxing major technology companies as a way to reduce a swelling budget deficit, redistribute purchasing power, and win popularity with voters.

France claims to remain committed to an EU-level solution. Meanwhile, Italy will probably be next to introduce its own tax. The country had already passed a law introducing a tax, but its implementation had been postponed in favour of finding an EU solution. Spain and the UK, both of which have put forward national proposals, are likely to follow.

What's important for 2019?

The fragmentation of the EU's tax landscape means that digital companies may find themselves in and out of the scope of different measures. Tech companies in scope are likely to try to pass their costs down to their customers, which could include other, smaller digital companies. Taxing revenues could also lead to double taxation of digital businesses.

Despite the flurry of national taxes due for 2019, work on an EU-wide solution is set to continue. The push for a digital tax may well be strengthened by the European Parliament elections in May 2019: we can expect to see political parties from across the spectrum calling for a clampdown on tax avoidance and putting forward suggestions for taxing major digital companies.

Internationally, the OECD will develop a work programme on digital tax for 2019 and is due to issue proposals in 2020. Many EU member states, including Germany, would prefer an OECD agreement and will cooperate on any proposals the organisation puts forward.

What are the policy challenges?

- The fragmentation of the EU's digital tax landscape is the greatest policy challenge facing businesses operating in the EU. Digital companies should make this a key subject of engaging with policy-makers.
- Digital businesses can provide constructive contributions to the debate, explaining the difficulties of separating the digital economy from the wider ecosystem and highlighting the risks of double taxation.
- The focus for policy engagement should be on rejecting the idea of an interim tax and emphasising the need to develop an OECD-level, profit-linked tax that avoids double taxation and continues to support innovative EU businesses.

Finding the "Right" Regulation for Online Platforms

Mike Laughton, Policy Analyst
Héloïse Martorell, Policy Analyst

In Europe, policy-makers' attitudes are hardening towards a policy of benign neglect that has characterised the last 20 years of technological expansion. Instead, it is now routine to see promises to crack down on the "new wild west". The prime target: revisiting intermediary liability safe harbours in 2019.

Policy-makers face difficult trade-offs when trying to regulate tech companies. The current environment has fostered growth and innovation, but the pace of technological change has made it difficult for countries seeking to contain bad actors proliferating on online platforms. Online platforms in the EU have been protected since the turn of the millennium by versions of the eCommerce Directive which categorises them as being "mere technical, automatic, passive" intermediaries. Under this law, online intermediaries are protected from liability of the dissemination of harmful content through safe harbours and only lose such protection when failing to remove it after receiving notice of it.

Today, one does not have to look far to see these provisions under sustained criticism. Even the platforms themselves are questioning the responsibility of online platforms in the dissemination of harmful content, ranging from misinformation — or 'fake news' —

and cyber bullying to the spread of terrorist content. Following the Cambridge Analytica scandal, Facebook's Mark Zuckerberg expressed willingness to work with legislators to develop the "right regulation".

In the EU, previous steps taken to limit harmful content include the directives for child protection and combatting terrorism, as well as non-legislative measures like the Code of Conduct on Countering Illegal Hate Speech or the European Strategy for a Better Internet for Children. These liabilities are also considered the major obstacle to those seeking to contain pirated content, although efforts to make platforms license copyright content are stalling in EU negotiations.

With providers now curating content with algorithms, many fail to see how this editorial control differentiates them from publishers. While there is no proposed legislation, a 2017 communication from the European Commission recommended online platforms actively monitor, identify, and remove harmful content. While not legally binding, the stance taken by the EU demonstrates an inclination to establish new obligations and place new responsibilities on online platforms. It remains to be seen whether this communication will lead to legislation.

Even in the UK, traditionally soft on regulation, attitudes have hardened just as the point where it can depart from the EU rules comes into view with Brexit. Initiatives, starting with the Digital Economy Act 2017 which in part aimed itself at protecting children online, have piled up. An Internet Safety Strategy, due to tackle a full range of online harms from cyber-bullying to child exploitation, is due early this year. Many of these measures will certainly raise the cost of maintaining these safe harbours, if not entirely remove them, but the direction of travel was made clear by the election manifesto of the Conservatives in 2017 calling on the UK to become "the global leader in regulation of the use of personal data and the Internet".

In 2019, there is every reason to expect the debate to be re-opened. Not least, there will be a new European Commission in place under pressure to re-open them. Compounding this, revelations about the harms propagated on online platforms do not appear to be going away and, be it election tampering, cyber-bullying or hate speech, legislators are poised to step in to what they see as the common denominator. The risk in Europe, as it is elsewhere, is that these regimes fragment and contradict each other, while each claim the right to enforce their views outside their borders.

The question of platform regulation challenges liberal societies by magnifying the tensions inherent in their set of liberties: freedom of speech, freedom from discrimination, the right to exploit one's intellectual property, the right to anonymity and the necessity of identity to enforcing laws. In a continent with important cultural differences defining the relative importance of these rights, online platforms must come prepared with answers on responsibilities they can accept.

GDPR Goes Global

Logan Finucan, Public Policy Manager

The European Union's globally applicable General Data Protection Regulation (GDPR) has set the global benchmark for data protection standards. In 2019, it will continue to reverberate far beyond Europe; more countries around the world will adopt GDPR-like standards, often creating headaches for global business in the process. Will the GDPR now inevitably become the world standard?

The EU has successfully branded itself and the GDPR as the gold standard for data protection. Rightly or wrongly, the GDPR and its standards now connote unimpeachable credibility on consumer protection and are firmly establishing the idea of data protection as an issue of fundamental rights.

Now, when country "X" is looking to update its data protection laws, the GDPR is the first jar on the shelf they reach for. Countries are emulating the GDPR, in whole or in part, proliferating standards to empower individual consumers like providing affirmative rights for data subjects, defining legal obligations for data controllers and data processors, requiring adequacy for cross-border transfers, and imposing heavy fines for non-compliance, among others.

Why now?

This trend has been long building. When the EU established the GDPR in 2016, their first-mover advantage was helped along by fortuitous timing, intersecting with a string of troubling revelations about the privacy practices of tech giants. Scandals like the Facebook/Cambridge Analytica revelations or repeated privacy failures in India's enormous Aadhaar digital ID system have made treatment of personal data online a pressing political issue, impossible for policy-makers to ignore. Europe has capitalised on these problems with a tough line on unpopular US tech companies.

We have already seen the GDPR's normative power in 2018, with the adoption of a new data protection framework in Brazil that bears substantial similarities to the EU's system, as well as policy proposals in India and elsewhere that have been deeply influenced by the GDPR framework.

Why does it matter?

The GDPR is a stringent framework for data protection with costs for businesses; the spread of these norms will raise costs for firms of all sizes around the world. Companies have scrambled in the past year to achieve compliance amid an uncertain enforcement climate. The focus now is getting the right type of consent from citizens and proving good faith efforts upfront to regulators, absorbing substantial time and energy.

However, what is more difficult than the spread of GDPR standards is the imprecise copying of GDPR standards, which threatens to multiply compliance and cross-border data transfer burdens. Each country is putting their own spin on the ideas of the GDPR and arriving at subtly different standards for how to implement general principles.

Further, some popular elements of the GDPR, even if copied exactly, have the effect of fragmenting global data flows. For example, the concept of "adequacy" for international transfers of personal data requires each country to stitch together a network of bilateral determinations and negotiated agreements — a laborious and time-consuming approach.

What is next?

India promises to be the next biggest development in global data protection norms. The government is due to propose a comprehensive data protection legislative package in the summer of 2019. Early drafts bore significant resemblance to the GDPR.

In a twist that would have been unthinkable even a few years ago, we are now seeing the EU set the terms of the policy debate even in the US, which is in the early stages of developing a long-deferred comprehensive consumer data protection regime at the federal level.

While the legislative process will be long and painful, momentum has grown substantially. Many, even some in Congress, would be happy to import the GDPR as a US solution.

The extent to which GDPR-inspired ideas creep into US and Indian models in 2019 — two of the largest and most influential data markets — will have ramifications for decades to come. This year, we may see policy-makers surrender the idea of creating an alternative model to the GDPR altogether.

Cyber Policy in the Global Arena

Ryan Johnson, International Public Policy Senior Manager

The global cybersecurity debate will be more fractious in 2019, following significant controversies in both the United Nations (UN) and International Telecommunication Union (ITU) on cyber policy. Infringements of norms by major players could reduce other states' willingness to abide by them and, as the primary operator of the global Internet infrastructure, businesses will continue to be caught in the crossfire.

In 2019, policy solutions will be harder to achieve, and the risks of cyber conflict will increase until states find an incentive to cooperate. While there won't be a cybersecurity angle at the major ITU conference this year (the World Radio Conference concerns itself primarily with spectrum usage issues), the debate will proliferate into new venues, including a likely renewal of the Global Conference on Cyber Space (GCCS). While the 2017 GCCS, in India, was focused primarily on that government's priorities, the 2019 host (TBD) has a chance to harness and reinvigorate the international policy dialogue.

For example, the Asia-Pacific region, which is rapidly improving its national cyber policies and capacities, could serve as a global example — both good and bad. For example, Viet Nam's recently-enacted cybersecurity law criminalises public criticism of the government, mandates data localisation, and grants authorities access to private data without a

warrant. Conversely, Singapore's recent creation of a regulatory framework to protect essential services and to invest in skills and defence training demonstrates an understanding that cybersecurity requires a sustainable ecosystem focused on both immediate and long-term actions.

In 2019, we will likely see a proliferation of cybersecurity laws like these in Asia, particularly Indonesia, and will need to monitor how they balance freedom with security. Leaders like Australia, Singapore, and Japan are already providing invaluable assistance to less-developed countries in the region. With a growing commitment to mutual defence, adoption of cyber norms, and regional-level capacity building, the Asia-Pacific region is responding to the significant geopolitical risks facing it.

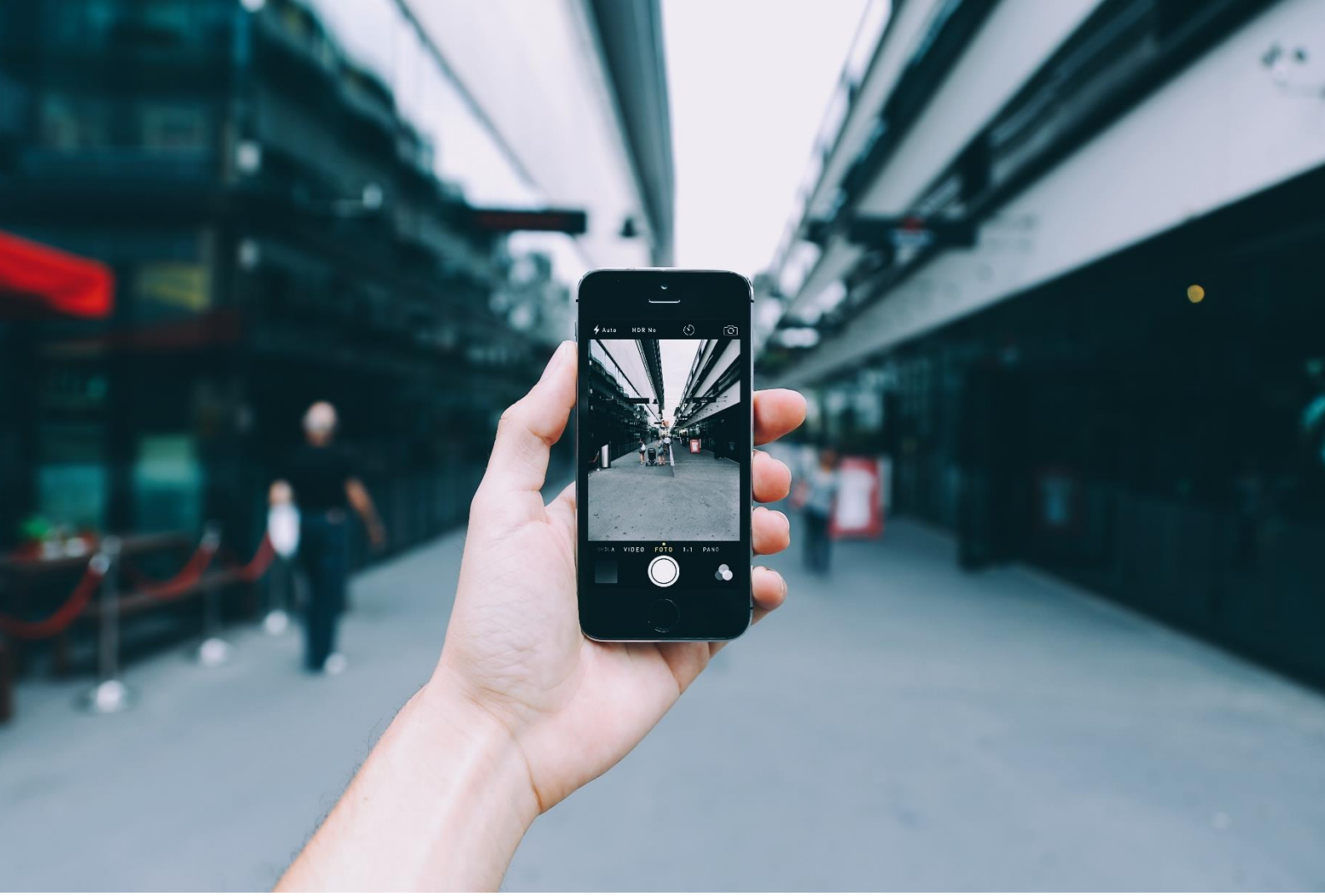
We will also see a proliferation of threats — ranging from denial-of-service and ransomware to data theft — and their preparators, whether criminals, hacktivists or nation states. Cyber action will continue to be a low-intensity, low-risk operational methodology for nation states: Chinese theft of sensitive data from the Office of Personnel Management in the US resulted in the loss of security clearance information, personal details and fingerprints of millions of people. It will also continue to be used as a precursor to kinetic attacks, as we have seen with the Russian government-affiliated attacks on Ukrainian government and military targets.

As we saw with the leak of Shadow Brokers material, which was repurposed for use by criminals and the North Korean government, the continued proliferation of cyber weapons by nation-state actors will continue to aid less sophisticated actors in acquiring advanced tools, with corresponding effects on other targets. Last year alone, Facebook announced that hackers accessed the accounts of up to 50 million users, and the Under Armour data breach affected an estimated 150 million users.

As cyberattacks continue to grow in scale and scope, governments will face increasing pressure to protect their own infrastructure and establish a framework for industry. As such, we should expect the continued proliferation of norms in 2019. Late last year, the UN General Assembly established a short-term UN Group of Governmental Experts (UNGGE) and an Open-Ended Working Group (OEWG) to study the normative behaviour of states in cyber conflict and to discuss cybersecurity in the international arena. The working group will aim to build consensus for norms that will guide the establishment of legal concepts within cyber space. In addition, the UN Global Commission for Stability in Cyberspace will continue to build on its proposed norms, offering a more multistakeholder perspective on how normative behaviours can be created and enforced.

The outcome of these groups, though, will depend on the commitment by individual states to follow the international principles and overcome policy challenges, such as:

- Selecting which norms they want to promote and adopt at the national level, which will impact the way that states deal with private infrastructure in their cyber operations.
- Ensuring appropriate protection of civilian critical infrastructure between military and intelligence resources while coordinating with industry.
- Foster public trust within laws and regulation without creating secondary effects such as weakened encryption of content censorship.



Smart Cities in Asia Get Smarter

Seha Yatim, Policy Analyst

“Smart cities” was one of the buzz phrases of the year 2018. Local and national governments have been keen to develop their own smart cities to enjoy the promised savings, greater efficiency in resource deployment, potential reductions in congestion and improved sustainability, not to mention the prestige.

Within ASEAN, members states are already ahead of the curve. They launched the ASEAN Smart Cities Network last year and are expected to meet in Tokyo this year as part of a joint initiative by Japan and Singapore. Japan is collaborating with ASEAN to pursue smart cities projects by partnering with Society 5.0, the ASEAN-Japan Innovation Network, and the Japan-ASEAN Science, Technology and Innovation for Sustainable Development Goals Bridging Initiative among others.

Asian governments are also rushing to sign agreements with the private sector. Indonesia is working with Dassault Systèmes to develop the Padang Pariaman Smart City Implementation Project; private sector firms from Japan and China will begin building a smart city in Thailand, Sunway and NEC will be collaborating on developing smart city solutions for the Iskandar region in Malaysia; and the list goes on.

As the pursuit of smart cities grows in the region, here are some trends that we will see in 2019.

1. **Rise in policies that support the smart cities environment**

Smart cities depend on vast amounts of data and connected devices. This year, governments are drumming up support for two policy areas necessary to support smart cities: policies that enable the constituent technologies and policies that protect citizens' rights. Enabling policies and others that encourage the development of new technologies mooted around Asia include the use of (anonymised) data for research, the protection of IP rights, or regulatory sandboxes that allow new product testing without regulation. On the other side, policy-makers will also need to carefully consider grey policy areas. For example, increased use of surveillance drones and security robots within smart cities will require guidelines that balance national security and individual privacy.

2. **Growth in applications that focus on people-centricity**

Smart cities often come with wholesale redevelopment of an area; usually, this is the most visible, most talked about, and the part of the plan most likely to cause backlash. In 2019, smart cities will likely respond by trending towards genuine consultation with local inhabitants and adaptive design.

For example, local privacy rules will dictate how smart cities can run on a basic level. Wayfinding and smart mapping apps depend on whether transport agencies can or are willing to share data, while the sensor-equipped smart districts like Google's Sidewalk Toronto or South Korea's Songdo could fall afoul of consent laws. Moreover, governments should seek the involvement of civil society to create tailored solutions and improve the chances of success. In London, a city often highly-rated in smart cities indexes, launched the 'Smart London Plan' in 2013 to increase citizens' participation through improving digital inclusion and access to open data.

3. **More governments will take up a leadership role**

Smart cities projects are long-term projects reliant on a vision, leadership, and commitment from national leaders. Without these qualities, projects labelled "smart city" may come to be seen as delivering buzzwords rather than meaningful innovation or improvements to quality of life.

For bigger countries, this will require collaboration between municipal governments and the central government to ensure similar initiatives and effective project management across government levels. With the amount of resources and commitment needed, governments will likely play a larger role in 2019. Japan is a prime example; taking a whole-of-government approach while collaborating with key Japanese technology firms through the Japan Smart Community Alliance (JSCA) and sharing their policies on smart-

energy, disaster, spatial and other planning initiatives. As a result, Japan is becoming a leading smart city hub, and other countries are likely to look to their example this year.

4. **Greater support for start-ups and innovation**

To create an environment conducive to smart cities, governments have to support start-ups and encourage innovation. Governments have increasingly looked to start-ups and private providers to help boost smart cities with Deloitte finding that only 16% of cities are able to self-fund the infrastructure they need for smart cities.

Policy-makers can create opportunities through grants, rebates, subsidies or competitions. For example, the collaboration between the Cyber Security Agency of Singapore and TNB Ventures invited start-ups to join an innovation call and pitch their ideas. In addition, government can look to educational institutions for digital talent. In Indonesia, the Digital Talent Scholarship programme expects to train 20 000 people by 2019 on artificial intelligence, robotics, cybersecurity, and big data, among others. Encouraging exchange between academia and the public and private sectors will drive the development of local smart cities initiatives.

5. **Careful measurements for smart cities initiatives**

With the huge investment poured into smart cities, ensuring there is some measure of success is crucial. 2019's projects should focus on indicators that evaluate the impact of smart cities on sustainability (CO2 emissions), transport (efficiency of public transportation), governance (citizen participation), digitalisation (Internet access and smartphone penetration), and security. In countries like Indonesia or Thailand, measurements are essential to track the success across the different municipalities. Clear, consistent measurements may also make it easier to pull in future investors who would be looking for indicators to identify which cities to work with.

Buzz to business

Smart cities reaching the lofty goals they set themselves will depend on policy-makers' commitment to establishing favourable governance frameworks, and 2019 shows signs of them doing that. In Asia, this requires up-to-date policies for new technologies and the participation of civil society and private firms — from big tech companies to local start-ups. Regional governments can take example from Japan's approach as it starts to reap the benefits, while partnerships in Indonesia and Malaysia are laying the ground for future work.

Digital Identity: A New Impetus for Stronger Management

Renuka Rajaratnam, Public Policy Manager

A crucial but less-noticed factor in the reduction of poverty has been the spread of formal identification among previously undocumented people. A concrete ID grants people in poverty access to social services such as sanitation, education, and medical care, as well as being a prerequisite for access to bank accounts, business licences, and financial services. As many of these services expand online, digital ID is an urgent necessity to guarantee continuous and secure access.

Recognising this, in 2017, the World Bank launched the Identification for Development (ID4D) initiative to realise the creation of “inclusive and responsible digital identification systems as a sustainable development priority.” Less developed countries have slowly made progress in transitioning from paper-based to digital identification, with several countries announcing plans to create digital identity systems and six Asian governments already expected to roll out digital IDs over 2019 and beyond.

In 2019, as this process accelerates, success depends on whether a market for digital identity systems can overcome growing challenges and the memory of some high-profile failures.

What are the policy considerations?

Attempts to expand digital ID schemes in 2019 will need to balance the security of critical information with concerns on privacy, individual rights and freedom.

Cybersecurity

Digital ID requires several strands of highly sensitive information, naturally raising concerns about data breaches and cyberattacks. This will intensify as the digital identity market moves towards greater interoperability in 2019, characterised by federated identity management and the use of distributed ledger technologies (for example blockchain) to secure digital identity.

Technologies to safeguard digital identities have been developed but are struggling to expand beyond national borders, at least in part due to diverse languages and cultural variations. It will be critical for safeguarding technologies to overcome these barriers as several current systems have lacked sufficient security. For example, India's Aadhaar — the largest national digital ID system in the world — has suffered major security breaches that made confidential information widely available.

Digital trust and privacy

The use of new technologies to enhance the security of digital ID systems will further test the boundaries of trust in digital systems. Digital ID systems intrinsically allow tracking and study of peoples' online and offline behaviour patterns, as well as the sale of this information for commercial or political use, making users inherently suspicious of the technology. For instance, national digital ID systems used for surveillance are already a reality in parts of China and raise ethical issues around individual freedom and privacy.

Similarly, efforts to secure these systems will also have to contend with the need to retain transparency. For example, distributed ledger technologies are gaining popularity but also obscure the operations of these systems. This could further erode trust in these systems and raise concerns about how and where data is accessed, processed, and stored.

Accessibility

Although digital ID systems make it much easier to obtain services, run businesses, and participate in government, registration can be a higher-bar than previous paper-based systems and marginalised populations risk being 'locked out' of services even more than they were before. Verification of digital identity requires electricity and connectivity, not always available, while the reliance on biometrics risks excluding people who cannot

provide commonly used forms of data; for example because of illnesses or professions likely to degrade fingerprints.

Unless policy-makers plan to address these issues, 2019's digital ID systems will face challenges in adoption, trust, and use.

Solutions for 2019

The key to managing the tension between the immense benefits and the pitfalls of digital ID systems will lie in ensuring regulations remain adequate and relevant for new technologies through consistent multi-stakeholder engagements and capacity-building efforts.

For instance, governments can look to international standards being developed, like the US Department of Commerce's National Institute of Standards and Technology (NIST)'s technical standard around digital identity systems. The standard should allow for easier enrolment and proof of identity that meet both the authentication and life cycle requirements that government institutions need as party of a digital legal identity.

In addition, it will be critical to monitor in the next year how governments and business implement data protection and cybersecurity laws released or amended in 2018. Regulations and implementation guidelines may need to be updated to better facilitate authentication of digital identities. Gaps between policy and practice both in the public and private sectors will need to be eliminated through capacity building and training. This will continue to ensure that basic levels of cybersecurity and data protection are met.

Digital ID offer great potential in terms of facilitating access to basic services and improving efficiency of businesses. In 2019, it will be essential to protect this potential from mismanagement or misuse.

The Thriving AI Ecosystem

Hussein Abul-Enein, Policy Analyst

2018 was undoubtedly the year of artificial intelligence (AI). It dominated the tech sector, from literature and conferences to national strategies across the globe, including the UAE, Mexico, France, Germany. In 2019, we should expect the global AI ecosystem to expand further.

Countries will likely jump on the AI bandwagon and develop their own strategies, either for fear of missing out or in an honest bid to reap the benefits of the technology. For example, following in the footsteps of South Africa, Ghana announced the drafting of a comprehensive AI policy, with planned engagement with both the public and private sectors. Or Egypt, who despite its foreign debt and political turmoil is mimicking the Saudis and Emiratis by utilising advanced technologies such as AI, blockchain and cloud computing in government. We can also expect some initiatives from Brazil, Bahrain, Nigeria, Kenya and Oman.

As new players join the AI revolution, countries with existing strategies are expected to double down on their commitments. The UAE will expand its AI council, China and the US are both taking steps in coupling expansive private investment with a governance framework, while Paris and Berlin will focus on building their "ethical AI" model.

Meanwhile, Canada and Tel Aviv will concentrate their efforts to attract AI researchers and start-ups, respectively.

With governments and industry pushing hard to instigate and direct their own AI sectors, it will be critical for international institutions to frame development through best practice guidelines. Taking an example from the Asilomar Principles — endorsed by Apple, Facebook, and Google — and Intel's Public Policy Principles For AI, the OECD is set to release its own set of precepts to encourage the ethical development of emerging machine learning technologies. Similarly, the ITU may publish a similar list at the upcoming AI For Good Global Summit. The Fourth Industrial Revolution will thrive if governments, business, and academia pool their resources and initiate discussions on the inevitable ethical and societal concerns that will rise from the widespread use of AI.

Still, the AI governance framework is nascent and we have yet to see any universally-accepted best practice principles. Neither the United Nations nor its Economic and Social Council have implemented an AI Resolution, or even a ministerial declaration. During the Plenipotentiary Conference in Autumn 2018, member states failed to pass an ITU resolution after 16 straight hours of discussions. The effort was commendable, but the failure revealed pivotal differences in national approaches. For example, the Arab and African groups keen on deregulation rallied against their European counterparts focused on building an ethical model for AI uptake.

Unless a consensus can be reached in the UN or any other international body, countries will continue to push their own strategies to leverage AI. While some countries are visualising AI development as a zero-sum game, the outcome of all this competition will be the steady development of a global AI ecosystem. As stakeholders naturally converge, the question is which working model will be adopted, whether it's Europe's ethics-led development or unregulated private innovation.

Intelligent Healthcare

Anne-Shannon Baxter, Policy Analyst

Artificial intelligence (AI) in healthcare has the ability to revolutionise healthcare delivery but has yet to live up to its hype due to structural obstacles. That could change in 2019 with the promotion of AI through policies that encourage innovation. With more than half of the world's population lacking access to the healthcare services they need, according to the World Health Organisation (WHO), governments and industry can leverage AI to provide tailored, cost-effective, high quality and more accessible healthcare.

AI-based solutions are already reducing the cost of healthcare and freeing up time for patient interaction and treatment by automating administrative tasks such as writing chart notes, prescriptions, and voice-to-text transcriptions. Virtual nursing assistants — apps which provide basic medical information based on the patient's symptoms — can 'filter out' less serious conditions to local doctors and pharmacies, reducing hospital visits and the risk of exposure to illnesses at hospitals.

These efficiency savings, while necessary and helpful, are not the healthcare revolution anticipated by many in the medical world. In the future, AI could play an important role in early detection and diagnosis of illnesses, by using cognitive technology (such as machine learning and advanced analytics) to store and combine scientific data with

personalised medical information. For example, AI can suggest the most optimal surgical approaches based on individual patient records, as well as medical research and data on past surgeries.

The technology is developing but several obstacles remain. Privacy regulations on medical data limit what can information can be used, while the low case numbers of many conditions prevent bulk analysis. For example, Google's acquisition and subsequent relocation of DeepMind Health raised concerns over the transfer of UK residents' data to the US. Also, accusations of bias in AI algorithms, differing resource levels, and different medical cultures limit the extent of usability of AI-based solutions.

Therefore, to use AI to help achieve the WHO's triple billion targets — an additional one billion people receiving universal healthcare, one billion people better protected from health emergencies, and one billion people experiencing better health — the WHO, in partnership with the International Telecommunication Union (ITU), has launched a Focus Group on Artificial Intelligence in Health (FG-AI4H). The group's objective is to establish a standardised assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions.

Over the coming year, the Focus Group hopes to develop international standards for collecting, aggregating, analysing, and developing AI models for various stakeholders in the health system including patients, healthcare providers, insurers, and health authorities. While the Focus Group has noted that it does not intend to specify the algorithms themselves, it does represent an opportunity for those developing AI systems to have them evaluated and benchmarked. If proven successful, these AI systems could be adopted in countries around the world.

The widespread adoption of AI could benefit health systems in developing countries that face structural challenges, such as shortages of staff and supplies, accessibility barriers, and lack of awareness on certain health issues. A standardised framework of AI-based solutions can facilitate the uptake of AI and help bridge these gaps.

Some governments are already investing in AI in the health sector. The UK government, for example, is encouraging AI uptake in its National Health Service (NHS), and local trials are being held in several London suburbs for the 'C the Signs' tool, which helps doctors recommend cancer investigations or referrals based on the presented symptoms. Governments can continue to promote the development of AI in healthcare by creating thoughtful policies that foster innovation, including:

- Increase investment in ICT infrastructure to enable stakeholders to develop AI solutions.
- Encourage the reduction of algorithmic bias to ensure discrimination and prejudice are removed from AI solutions.

- Develop data privacy regulation that protects data without hindering cross-border data transfer.
- Expand datasets through government investment in statistical agencies that can publish accessible data.
- Encourage data sharing platforms by funding academic and scientific research institutions in order to increase the data pool used by stakeholders.
- Ensure intellectual property regulation properly protects against infringement of algorithms.
- Develop international standards to ensure data portability and interoperability across borders.

WTO Reform Gathers Steam

Logan Finucan, Public Policy Manager

After being overshadowed by headline-grabbing national confrontations over trade last year, reform of the World Trade Organization (WTO) will cease to be a sleeper issue in 2019.

Despite the sudden focus on trade issues thrusting national grievances into the spotlight, several countries have been quietly laying the groundwork for a thorough shakeup of the organisation for a long time.

In 2019, we expect increasingly high-profile discussions of how to change how the organisation deals with dispute settlement, negotiation processes, and issues between members. The US, EU, Canada, and Japan (as well as others) have floated possible changes on a slew of issues — several more recent proposals prompted by Chinese trade practices, including notification of subsidies, definition of state-owned enterprises, forced tech transfer, data issues, local content requirements, and overcapacity-generating subsidies.

The US has also indicated it would like a clearer delineation in the rules between "market" and "non-market" economies — affecting how the General Agreement on Tariffs and Trade (GATT) rules on anti-dumping apply — which will be strenuously resisted by China.

Why now?

The new US hostility towards the WTO has brought matters to a head, with US Trade Representative (USTR) Robert Lighthizer (a long-documented critic of WTO dispute settlement processes) one of the driving forces behind the project. In 2017, they began blocking new appointments to the WTO's dispute settlement body, bringing that arm of the institution to the brink of collapse. Deputy USTR Dennis Shea, who has a built a reputation of bluntly confronting China at usually staid WTO meetings, has said "the biggest challenge is dealing with China, whose non-market economy is simply incompatible with WTO norms."

Despite clashing on other trade issues, the US, EU and Japan have been coordinating trilaterally on how to hem in Chinese trade practices through new WTO rules, building on long held irritation towards the failure of economies like China to comply with notification or transparency notifications, making new negotiations difficult, and towards the Appellate Body, a group of seven judges who are widely perceived to have gone beyond interpreting existing rules to trying to establish new ones.

Why does it matter?

Much of the world and nearly USD 20 trillion in international trade are bound by trade rules structured by the WTO. If a reform package cannot be struck, there is every possibility a Trump administration may take the US out of the organisation. A US withdrawal may not totally shred that framework, but it would cripple it. If the US doesn't leave but continues to block Appellate Body appointments, the dispute-settlement mechanism will cease to function entirely after two judge terms expire this year, leaving 2019's disputes in the hands of bilateral negotiations.

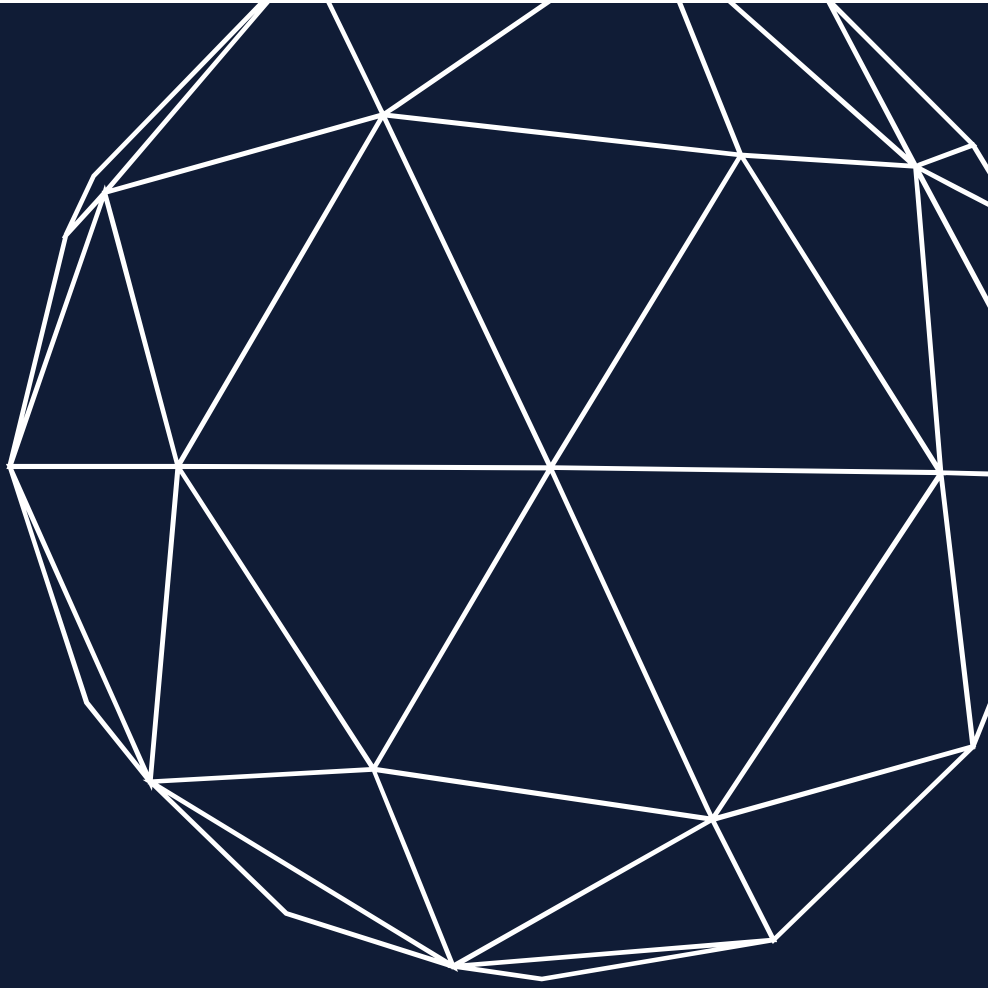
What's next?

US-China trade talks, currently within a self-imposed 90-day window to produce some outcome, is the next major front to watch for movement on the WTO issue. Agreement on changes to WTO rules could be an element of a negotiated settlement; at least indicating whether the US wants to achieve deep reform or just paper over the trade war in 2019.

Prompted by the unfolding disputes, other countries are being proactive. Europe has been out in front, constructively engaging with specific proposals. A small group of friends-of-the-system who met in Ottawa last October — pointedly excluding China and the US — are continuing to explore paths forward, meeting again in Davos in January.

Another group, led by Japan, Australia, and Singapore, is quietly spear-heading discussions for new rules that protect corporate data against over-bearing state intrusion.

Other high-level multilateral engagements in 2019, like the June G20 summit in Osaka and the August G7 summit in France, will opportunities to further advance these issues in preparation for the WTO ministerial meeting in 2020.



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

www.accesspartnership.com
AccessAlerts
AccessPartnership