Geneva Internet Platform
DigitalWatch
dig.watch

Issue 56, January 2021

# Newsletter

# In the cards for 2021

## PREDICTIONS

In just 10 keywords, we look ahead at what's in store for digital policy in 2021.

*Pages 2–3-4-5*

## BAROMETER

What's hot, what's cold, and what's warming up? Content policy, the internet economy, and cybersecurity top the list.

*Page 6-7*

## PRESIDENT BIDEN

The new administration's digital policy approach may not differ too much from his predecessor's. Here's why.

*Page 8*

## ELECTIONS

The positive contributions of technology are far from negligible, but so are the challenges. We look at what's at stake.

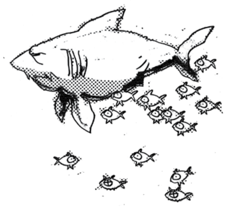
*Page 9*

# 10 keywords for 2021: Our digital policy predictions

**The idea of predicting digital policy trends through keywords started last year with our Dictionary of Digital Predictions for the 2020s. It proved to be successful (and accurate). A simple term can capture many complex topics and bring together issues typically discussed in siloed spaces. Plus, in a world in which we are bombarded with information on digital politics (and pandemics), a handful of keywords to guide us through 2021 are a welcome tonic.**

**Here are our ten keywords for 2021, in alphabetical order.**

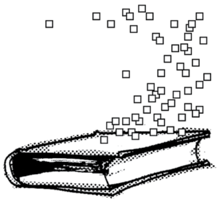
## **Big Tech** /bɪɡ tɛk/



Big Tech has become synonymous with might and power. Economic strength? The four main tech giants – Google, Amazon, Facebook, and Apple – have a total annual revenue surpassing the GDP of Norway and France put together. Market dominance? The USA, the EU, China, Japan, India, and numerous other players are arguing that Big Tech has systematically squashed any rising stars that have threatened their position. Legislation? Last year's campaign in California in favour of Proposition 22 – the newly passed ballot measure allowing companies to continue treating workers as independent contractors – cost the companies over US$180 million. (Harmful content? That too; it's further down the list.)

Ongoing investigations into market practices, most of which were initiated just last year, point to two main solutions: splitting up the giant tech companies (reminiscent of the Baby Bells of the 1980s) or imposing regulatory obligations coupled with mega-fines for non-observance. Both solutions are insufficient on their own. Allowing companies to amass their wealth through (approved) acquisitions and then splitting them up is futile if they are then allowed to re-merge. Enacting new local or regional regulations (or updating current ones) just adds to the current patchwork of laws, creating more uncertainty. Rather, multi-pronged measures may be required.

## **Cybernorms** /ˈsʌɪbə nɔːms/



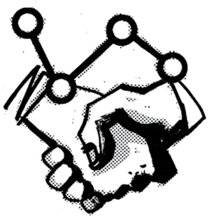
The unprecedented espionage campaign against US institutions – known as the SolarWinds breach – identified by security firm FireEye in December 2020 and thought to be likely of Russian origin, will undoubtedly be one of the toughest issues that newly-elected US President Joe Biden will have to face.

It is also expected that the USA will take  a leading role in cybersecurity negotiations. Since the stakes of cyberattacks are getting higher, Russian-US cooperation on international information security is likely to resume in some form. This could mark a turning point for global negotiations as well.

The UN Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) are both expected to finalise their reports in 2021, with the OEWG's mandate extended to 2025. Despite calls for both groups to include a Programme of Action in their reports, with the aim of ending the confusing work-in-parallel, expectations are modest. Nonetheless, the groups serve an important function: they provide countries with a collaborative space in which to talk, rather than fight.

In 2021, the Paris Call for Trust and Security in Cyberspace will move into the operationalisation of its principles; the Global Forum on Cyber Expertise is strengthening its support of particular projects and match-making activities; while the Geneva Dialogue on Responsible Behaviour in Cyberspace and the Organisation for Economic Co-operation and Development (OECD) will focus on the security of digital products and services and on increased cooperation between policymakers and the corporate sector.

## **Data flows** /ˈdeɪtə fləʊs/



Five years have passed since the Court of Justice of the EU ruled in favour of privacy activist Max Schrems, invalidating the Safe Harbour regime. The framework's successor, the EU-US Privacy Shield, was struck down by the same court in July 2020. The underlying issue remains the same: whether the data of EU citizens processed in the USA is protected as adequately as in the EU.

The invalidation of these frameworks sent companies scrambling to find legal alternatives to processing EU citizens' data. In 2021, one of the main issues will be to find a more permanent solution – one that can quell any outstanding doubts in the minds of governments and civil society.

Other jurisdictions will continue to update local laws on user data protection. The EU's General Data Protection Regulation (GDPR), which came into effect in 2018, is arguably the world's most coveted piece of legislation on data protection, as it affords citizens with strong protections and prescribes hefty fines for non-observance. Its gold standard status will continue to influence legal reform in other countries.

When it comes to the flow of non-personal data, the debate is much more polarised. There are countries that believe data is like the oil of the digital economy and needs to flow freely across borders, while others would rather see local data housed within their own borders. These opposing positions will continue to influence negotiations on digital commerce and trade. It will not be easy.

## **Future of work** /ˈfjuːtʃə ɒv wɜːk/

In recent years, the main debates around the future of work have revolved around two key issues: the impact of artificial intelligence (AI) and automation on the job market, and the status of 'platform workers' (typically, those driving taxis or delivering food or supplies ordered via an app). COVID-19 added a third: how the job sector is adjusting to the new normal, and how it will continue to do so post-pandemic.

The degree of disruption that automation and AI will bring is a moot point, but the certainty that this technological progress will significantly affect the world of work will continue to fuel calls for reformed educational and training systems and better regulations and safety nets to protect workers.

As for the status of workers, jurisdictions and courts are still split. There are those who see this type of work as precarious due to the absence of social security, leave, and other protections normally afforded to regular employees. Then there are those who agree with the platforms' idea that the gig economy is an important source of flexible work arrangements.

The post-COVID outlook foresees online work to remain a reality for many. This will likely be the case even after physical distancing restrictions are lifted, as companies have already started introducing more flexible work arrangements allowing employees to choose where they work from (many of whom are choosing either a hybrid or an entirely remote way of working).

All of this calls for adequate regulations (such as the proposed right to disconnect, in Europe) that uphold labour rights in this rather different environment.

## **Harmful content** /ˈhɑːmfʊl kənˈtɛnt/

The relative ease through which harmful content can be spread online has made it even more pervasive. Given their ability to root out harmful content, tech platforms have borne the brunt of the sharp criticism that has come from all directions. Platforms are being criticised for not doing enough or not reacting fast enough. Their bold decision to permanently ban Trump from social media was also criticised. European leaders thought that such decisions, impacting one's freedom of expression, should not be left in the hands of private companies. Judging solely by the reactions to the Capitol Hill attacks, the regulation of harmful content and the associated responsibility of platforms will be fiercely debated this year.

In the USA, Section 230 of the 1996 Communications Decency Act hangs in the balance. There is enough bipartisan support to expect changes to the liability regime of digital platforms for user content posted online. *More on page 8.*

In the EU, the process is more advanced, with the draft Digital Services Act and the draft Digital Markets Act having been released in December 2020. That's not to say that the proposals will not be as hotly debated. However, the EU's track record of enacting tough legislation (GDPR) and of holding tech companies to account on issues of privacy, data protection, and market behaviours does promise a strict framework.

# Predictions

## **Inequality** /ɪnɪˈkwɒlɪti/

In 2020, COVID-19 made it more obvious that digital inequalities continue to exist in different forms, and know no boundaries. While internet access is taken for granted in developed countries, the persistent digital divide combined with a raging pandemic served to exacerbate existing inequalities in the offline space. For instance, data shows that many more children worldwide were kept out of the education system last year compared to previous years; some children lacked access to a computer (even in developed countries), while others simply had no internet connection.

Calls for prioritising universal connectivity will have to be met with more concrete and sustained actions if we are to truly create a fairer and more inclusive (digital) economy and society. Beyond accelerating infrastructure roll-out in uncovered areas, more efforts will have to be dedicated to addressing issues such as affordability, digital skills, and equal opportunity for women and gender minorities.

One of the main issues is how to most effectively fund such efforts. Seeking innovative funding models is a challenge for governments, international organisations, and the private sector. Developing and least developed countries also need more support to build the enabling environments (i.e. policies, regulations, and institutions) to help them catch up with the rest of the world and take advantage of technology.

## **In-(ter-)dependence** /ɪntədɪˈpɛndəns/

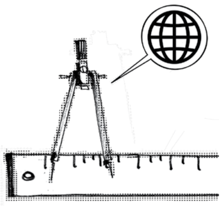
The ongoing trade war between the USA and China is a battle for market stakes (more on this further down). The race for tech supremacy is a quest for power. States engaging in strategic cyber warfare do so to disrupt the efforts of others.

It also invites trade alliances to form, such as what we have been seeing between the USA and the EU (and between other countries), and what has been floated in other quarters. At the foundation of these alliances is the notion of like-mindedness.

Interdependence – particularly shared global values and cooperation – is on the other side of the coin. It was emphasised in the final report of the UN Secretary-General's High-level Panel on Digital Cooperation. States can still be sovereign, but the benefits of technology – the so-called digital dividends – can be borderless and enjoyed by everyone.

Containing the risks and maximising the benefits of digitalisation will require an agile management of the emerging age of digital interdependence. In steering this process, the UN Secretary-General's roadmap is the first concrete step in implementing the vision of interdependence as described in the High-level Panel's report.

## **Standards** /ˈstændəds/



Standards are commonly accepted benchmarks that provide technical specifications or define processes. In the digital field, important standard-setting bodies include the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (ITU), and the Internet Engineering Task Force (IETF).

Chinese companies (such as Huawei) are increasingly involved in the standardisation process. Their increased participation can have positive consequences for global interoperability and the safety of products and services.

Some Western countries, however, are worried about a new proposal made by China to replace the existing internet protocol (IP) – a set of standards that specifies how data moves around on the internet. The 'New IP' would see a different way in which computers or devices are identified for data to reach them. A change to the current IP would mean a change of the internet's core architecture.

China's proposal and growing influence in standardisation has inspired counter-proposals. One of them is to create the Technology-12 (T-12), an alliance of democratic countries and technological leaders that would seek to 'regain the initiative in global technology competition'. The EU has also proposed a transatlantic agenda for consideration by the Biden Administration, through which it is inviting the USA to collaborate in a series of technology-related areas, including adopting a coordinated approach to standard-setting.

The significance of all this is that the debate around China's proposed New IP will intensify this year. Standards can easily be reduced to being solely a tool for gaining political and market dominance. A more balanced assessment of these developments is needed. Standardisation is far too important to be left at the mercy of trade disputes or races for tech supremacy.

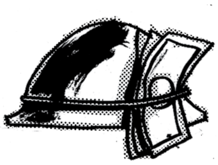
## **Taxation** /tækˈseɪʃ(ə)n/

Governments yearning to fill their coffers with digital taxes – targeting Big Tech – are growing impatient. France has already introduced a 3% digital tax; Spain's new digital tax just came into force; and other countries, such as Austria, Indonesia, Kenya, Malaysia, and Mexico have enacted some form of digital tax or another.

The EU also seems determined to implement some form of digital taxation very soon. In January 2021, the European Commission launched a public consultation on a new digital levy, aimed to 'ensure fair taxation in the digital economy while at the same time contributing to Europe's recovery'. Although the Commission notes that the levy will be designed in a way that is consistent with the OECD's ongoing work, it doesn't necessarily mean that the EU will also wait indefinitely.

None of this is ideal. The longer-term solution is to establish a global digital tax framework. But at the OECD, where most hopes for a global tax lie, things have been taking long. Hopefully, they will come to a close this year, as the OECD has now signalled that it expects to conclude its current work by mid-2021.

## **Trade wars** /treɪd wɔː(r)s/



It was a tumultuous year for US-China relations. Throughout 2020, the USA took several measures to limit the presence of Chinese tech companies in the country over fears that they posed security threats – allegations which China denied. The main target was Huawei, which faced a series of bans and trade sanctions. These ranged from restricting its access to US technology to prohibiting US companies from using federal funds to purchase Huawei (and ZTE) equipment. At the international level, the USA has tried (and in some cases succeeded) to convince its allies to impose similar restrictions on Huawei. The TikTok and WeChat mobile apps were also targeted by bans. China's reaction was to threaten retaliatory measures. The bans have been challenged in court (and not implemented so far), while the status of TikTok's sale seems uncertain.

With a new US administration in place, there is now the question of the future of the US-China tech dispute. The US strategic and whole-of-government approach towards China, announced in 2020, took on a more confrontational stance than in the past. We can expect this approach to intensify in the year(s) to come, but we may also witness a change in rhetoric.

The USA may also push for stronger alliances to contain China's growing digital power. These include: the EU-US tech alliance proposed by the EU, with no direct reference to China; a Technology Alliance between the US and nine other countries (Australia, Canada, France, Germany, Italy, Japan, the Netherlands, South Korea, and the UK, proposed by the Centre for New American Security); and a Digital Trade Zone (proposed by the Council of Foreign Relations).

On its side, China is promoting its interests through investment and trade alliances, filling the gap left by the US withdrawal from the world over the past four years. After almost a decade of negotiations, the Regional Comprehensive Economic Partnership (RCEP) agreement was signed in November 2020. It covers approximately 30% of the global population and GDP, and brings in two key US allies in Asia – Japan and Singapore – closer to China. The RCEP will also serve as a platform for investment in infrastructure and communications through China's Belt and Road Initiative, strengthening ties among its participants.

China has also reached a deal with the EU – the Comprehensive Agreement on Investment (CAI) – in December 2020. This shows that both parties will continue to pragmatically invest in the economic ties between them, in spite of US pressure to isolate China. It remains to be seen whether these ongoing attempts to contain China are a wise choice for the future of the global digital economy, and of the internet as a global network.

# Digital policy developments in January

The digital policy landscape is filled with new developments emerging practically every day. Our aim is to decode, contextualise, and analyse ongoing developments, offering a digestible yet authoritative update. There's more detail in each update on the *Digital Watch* observatory.

decreasing relevance

## Global IG architecture

The Internet Governance Forum launched the Policy Network on Environment and Digitalisation intersessional programme.

same relevance

## Sustainable development

Egypt allocated US$3.18 million to support the Digital Egypt Builders initiative. Ethiopia developed a national digital skills action plan.

Hong Kong launched a new digital ID platform. Barbados intends to accelerate the roll-out of digital ID cards.

The World Economic Forum's Global Risks Report 2021 listed digital inequality among the greatest risks of the next decade.

increasing relevance

## Security

The Zambian government approved a national cybersecurity policy. Darkmarket, the largest illegal marketplace on the darkweb, was taken offline.

US authorities stated that the SolarWind cyberattacks are 'likely Russian in origin' and 'an intelligence gathering effort'. The International Organization for Standardization published international standards on the security of biometric systems.

increasing relevance

## E-commerce & internet economy

The German parliament approved a law intended to make the digital market fairer.

The UK competition authority launched an investigation into Google's proposals to remove third party cookies from its Chrome browser. Amazon sued the European Commission for allowing the Italian competition authority to pursue an independent case against the company.

The European Commission launched a public consultation on an EU-wide digital levy. Spain's new digital tax came into force on 16 January. The European Parliament called for EU legislation to grant workers the right to digitally disconnect outside working hours.

same relevance

## Infrastructure

The breakdown of two undersea cables disrupted internet services in Vietnam. The Supreme Administrative Court of Sweden dismissed an appeal by Huawei against its exclusion from the country's 5G spectrum auction.

The US National Telecommunications and Information Administration released a 5G implementation strategy. Alphabet shut down its Loon subsidiary dedicated to providing internet from floating balloons.

# Observatory

## Digital rights

same relevance

WhatsApp's plans to update its privacy policy triggered an investigation in Turkey, a call from India to withdraw the plan, and an announcement from Pakistan about introducing new data protection legislation. The company decided to delay the new policy until 15 May.

The Norwegian data protection authority is to impose a €9.6 million fine on dating app Grindr over sharing personal data without users' consent.

TikTok faces potential legal action in the UK for violating children's privacy law. The Italian data protection authority imposed a temporary block on access to TikTok for users whose age could not be verified.

The Ugandan government ordered service providers to block internet access ahead of presidential elections.

## Content policy

increasing relevance

Twitter and Facebook permanently suspended former US President Trump's accounts while still in office, generating mixed reactions. YouTube suspended Trump's channel indefinitely.

Facebook shut down accounts of Ugandan officials before elections. Twitter locked out China's US embassy account for violating its policy against dehumanisation.

Apple and Facebook suspended social network Parler from their app stores for failing to moderate content that incites violence. Amazon removed the network from its hosting service. Apple and Google were sued to remove Telegram from their app stores for allegedly being used to encourage violence and extremism.

Twitter launched a community-driven approach to help address misinformation.

## Jurisdiction & legal issues

same relevance

Google and French press publishers reached an agreement on payments for news re-use. Facebook asked the Australian government to postpone by six months the implementation of the news media bargaining code. Google said it would stop making Google Search available in Australia if the code is approved as proposed.

President Trump issued an executive order banning eight Chinese apps before leaving office.

The UK High Court ruled that security and intelligence services can no longer rely on general warrants for bulk computer hacking.

## New technologies (IoT, AI, etc.)

increasing relevance

The US White House established a National AI Initiative Office. Algeria launched a national AI strategy. The European Parliament adopted a resolution on civil and military uses of AI. The UK competition authority launched a public consultation on algorithms' impact on competition and consumers.

The US Secretary of State approved the creation of a Bureau of Cyberspace Security and Emerging Technologies.

The Council of Europe called for strict regulation of facial recognition technology. Civil society organisations called on the Commission to ensure that the upcoming AI legislative proposal prevents the use of AI that violates human rights.

# Digital policy priorities of the Biden Administration

**US President Joe Biden inherits a wide range of digital policy issues: reigning in Big Tech, cybersecurity in the wake of SolarWinds hack, and dealing with China, to name a few. While the administration is new, the digital policy approach may not differ too much from his predecessor.**

Within a few days of taking office, President Biden issued a slew of executive orders addressing some of the most pressing issues in the USA: COVID-19, the economy, racial equity, and climate change. Digital issues are not far behind, although an official statement on priorities in the digital policy sphere has not been published yet.

## Getting the (cyber) house in order

Cybersecurity was not a priority policy field under President Trump, who terminated the White House Cybersecurity Coordinator position, reduced cyber diplomacy at the US State Department, and after his electoral defeat, fired Chris Krebs, director of the Cybersecurity and Infrastructure Security Agency (CISA) at the US Department of Homeland Security via tweet.

The Biden Administration has made cybersecurity a priority, as it inherits the aftermath of the SolarWinds attack, the largest cybersecurity failure in recent times. On Inauguration Day, White House Press Secretary Jen Psaki confirmed to reporters that President Biden asked the intelligence community 'for its full assessment of the SolarWinds cyber breach, and Russian interference in the 2020 election'. Currently, the nomination for the new director of CISA is underway.

Early involvement in cybersecurity provides hope for the revival of the Cyber Diplomacy Act, which would establish the Office of International Cyberspace Policy led by an official with the rank and status of ambassador that would coordinate all aspects of international diplomacy related to cybersecurity policy issues.

## Reigning in Big Tech

After the 6 January attack on the US Capitol, there have been renewed and urgent calls to restrain the power of Big Tech. The Biden Administration is expected to address misinformation and the liability of platforms regarding the content they host, as well as antitrust issues.

Section 230 of the Communication Decency Act (1996), which limits the liability of platforms for content posted online, will most likely not survive 2021 in its current form. There are calls to change the liability regime of platforms for user content posted online from both Republicans and Democrats, albeit for different reasons. The most radical approach – revoking Section 230 entirely – is one of the few clear positions President Biden has expressed. Others call for amending the current Section 230 and other laws to achieve a balance between freedom of speech and platform liability.

In antitrust matters, the Biden Administration is expected to build on ongoing government investigations of Google, Facebook, Apple, and Amazon and pursue antitrust lawsuits filed against Google and Facebook, as well as introduce antitrust cases against Amazon and Apple.

## Restoring global standing

One of the priorities of President Biden is 'restoring US standing in the world and rebuilding democratic alliances across the globe'. Apart from mending relations with the EU and other allies, the Biden Administration will have to tackle the question of how to address globally important technologies from countries that do not share the values of Western democracies.

President Biden seems to have similar concerns about the ambitions of China in tech and other areas to the previous presidential administration, but so far has only confirmed to aim for a more consistent and coherent policy in these issues. While Trump was focused on the trade deficit with China, Biden said to the *New York Times* that his 'goal would be to pursue trade policies that actually produce progress on China's abusive practices – that's stealing intellectual property, dumping products, illegal subsidies to corporations' and forcing 'tech transfers' from American companies to their Chinese counterparts.

The Biden Administration also seems to be following the footsteps of the previous administration in supporting American manufacturing (Buy American Executive Order from 25 January 2021) by limiting the procurement of goods and services by the federal government to US-made products and US-based services.

# Elections in the digital age

**In today's digital age, when the use of technology spans the entire electoral process – from political advertising and voter registration to vote counting – there's growing attention to the integrity of voting and privacy of voter data.**

In 2020, over 70 presidential and parliamentary elections took place worldwide. Voters across the globe are expected to 'take to the polls' in some 80 elections in 2021. The positive contributions of technology are far from negligible. They give a voice to marginalised groups, and extend their reach to diasporas. There are also serious challenges.

## E-voting popularity

Despite its advantages, the take-up of e-voting (using electronic voting machines rather than paper ballots) has been rather conservative, with only a small number of countries using it.

In Europe, Estonia was the first country to allow e-voting in the 2005 general elections and has since been considered as the most advanced actor in this domain. Whereas initiatives to introduce e-voting have been established in Germany, Norway, and Switzerland, efforts are still far from being realised.

Globally, e-voting has been adopted in only 33 countries, many of which are in Asia (12 countries) and in the Americas (10 countries). E-voting is the least popular in Africa, used only by the Democratic Republic of Congo and Namibia.

## Inseparable: Cybersecurity and data protection

The major challenge in digitalising elections is to ensure that technology remains concealed from those attempting to disrupt the security of the election process and transparent enough to the voters to instill trust.

Technological advances nowadays allow end-to-end encryption to ensure that votes cannot be tampered with before or after they arrive on the server, as well as verifiable decryption that facilitates voter anonymity when votes are counted.

Yet, the risks of vote manipulation require trust in electoral technology, especially when it involves online components, under a lot of pressure. In 2017, for instance, voter registration information during the presidential elections in Kenya was used to send out text messages and invite Kenyans to vote for political candidates. The Cambridge Analytica scandal, where the Facebook data of an estimated 87 million people was used for profiling and advertising during elections, is another example of failure to ensure data protection and privacy.

## AI: Friend or foe?

The prediction of voting trends and 'candidate-voter' matching are two examples of potential assistive use of AI. The YourVoteMatters platform, tested in the 2019 European Parliament elections, relies on AI algorithms to match voters with the best corresponding candidates. AI tools are also being used to fight disinformation on social media.

In contrast, AI can be misused for generating deepfakes and spreading disinformation. In Gabon, claims that a video of President Ali Bongo communicating his improved state of health was a deepfake triggered a coup attempt.

## Social media campaigning

With more than 4.41 billion users – or roughly 53% of the world's population – social media is a powerful communication tool. Estimates suggest that around US$7 billion was spent on political digital advertising in 2020 in the USA alone.

Unfortunately, social media is also rife with fake news during election time. In order to curb its spread, social networking companies are increasingly taking action. In the lead-up to the 2020 US presidential election, Twitter attached warning labels to posts – or deleted tweets entirely – while messaging apps WhatsApp and Facebook Messenger limited the number of messages which could be forwarded. YouTube decided to remove videos that contained misleading or erroneous claims of election fraud.

With so much at stake, the use (and misuse) of technology in the electoral process cannot be taken lightly. Flaws in the system, no matter how unintentional, undermine voters' trust. The question is, how high should we set the bar?

*Read more about Elections in the Digital Age on our dedicated space.*

# Policy discussions in Geneva

**Numerous policy discussions take place in Geneva every month. The following updates cover January's main events. For event reports, visit the Past Events section on the *GIP Digital Watch* observatory.**

### *CENSORSHIP – Twitter and Facebook make the law. But by what right?* | 28 January 2021

The online roundtable, organised by the Club de la Presse Suisse, discussed the recent measures taken by Facebook and Twitter, resulting in the ban of former US President Donald Trump's accounts from social media platforms. Although currently permitted by the US legal framework, speakers agreed that such measures created a dangerous precedent for freedom of expression and for political responsibility of social media platforms, and called for a debate on the need to create a common public space online that is not owned by private companies.

### *ITU Council Working Group (CWG) on Child Online Protection* | 26 January 2021

CWG Child Online Protection (COP) focused its 17th meeting on discussions around the ITU Child online protection initiative and the implementation of the 2020 Child online protection guidelines. The agenda also included contributions from member states on issues such as the promotion of the healthy use of technology by children and the challenges in using encryption protocols on the internet. The CWG-COP maintains an ongoing online public consultation inviting children and young adults between 15–24 years of age to help identify solutions to online safety challenges. The results of the consultation will inform the policy and programme recommendations issued by the group.

### *ITU Council Working Group on International Internet-related Public Policy Issues* | 27–28 January 2021

The 15th meeting of CWG-Internet – held in a virtual format – started with discussions around the secretariat report on the range of ITU initiatives related to the implementation of Resolutions 101 (internet protocol-based networks), 102 (the ITU's role in internet public policy issues), 133 (the role of states in the management of internationalised domain names), 180 (deployment of internet protocol version 6 (IPv6)), and 206 (over-the-top services). Also discussed were the results of an open consultation held by the group in December 2020 on expanding internet connectivity, as well as several contributions from member states on topics such as child safety online, trust and security on the internet, and cyber resilience.

### *ITU Council Working Group on WSIS and SDGs* | 28–29 January 2021

At its 36th meeting, the ITU Council Working Group on the World Summit on the Information Society (WSIS) and sustainable development goals (SDGs) started with taking stock of several activities related to the WSIS process and SDGs, including the outcomes of the IGF 2020 meeting, the 2020 UN General Assembly Resolution on ICT for sustainable development, and the UN Secretary-General Roadmap for Digital Cooperation. The ITU's activities related to the WSIS process were reviewed, and a discussion was held on the overall review of the implementation of the WSIS outcomes. Group members were also briefed on ITU activities related to the implementation of the 2030 Agenda for Sustainable Development.

Upcoming

# The main global digital policy events in February

**Let's look ahead at the global digital policy calendar. Here's what will take place in the next few weeks across the globe. For more details and event updates, check in regularly on our online space dedicated to digital policy events.**

February

### 8–10 FEBRUARY
**Dutch Digital Conference 2021 (online)**

The third edition of the Dutch Digital Conference will feature discussions on the six priorities of the Dutch Digitization Strategy, plus side sessions and events. The programme will be divided into six themes: AI, data sharing and access, digital inclusion and skills, digital government, digital connectivity, and digital resilience. The conference is organised by the Dutch government in collaboration with Noorden Digitaal and Platform for the Information Society.

### 18 FEBRUARY
**6th Geneva Engage Awards (online)**

Every year, the Geneva Engage Awards recognise actors in International Geneva in their social media outreach and online engagement. There are three categories – International Organisations, Non-governmental Organisations and Associations, and Permanent Representations to the UN in Geneva – with a fourth being introduced this year for online meetings. A new award, which will be in recognition of innovative and effective approaches to conducting remote meetings, will serve to encourage even more creative and engaging ways of holding online meetings. The awards are an initiative of the Geneva Internet Platform.

### 22–26 FEBRUARY (tbc)
**First IGF 2021 Open Consultations and Face-to-Face MAG Meeting (online)**

The first meeting of the 2021 IGF preparatory cycle will take place online. On the agenda: stocktaking last year's IGF; how to implement proposals for improving the IGF; how to implement the UN Secretary-General's Roadmap for Digital Cooperation; updates on intersessional workstreams; the main thematic tracks and programme for IGF 2021; and approving the Multistakeholder Advisory Group (MAG) working groups.

### 22 FEBRUARY–23 MARCH
**Human Rights Council 46th session (online and Geneva, Switzerland)**

The agenda of this 46th session includes: a high-level panel discussion on human rights on the fight against racism and discrimination 20 years after the adoption of the Durban Declaration and Plan of Action; an annual discussion on the rights of the child; a biennial high-level panel on the death penalty; an annual debate on rights of persons with disabilities; and a debate on racial discrimination. The session will also consider different reports.

March

# Introducing our weekly read

**The digital policy field is highly complex and full of developments. It never slows down.**

This is why, for the past four months, we've been publishing a new digest – a weekly interlude with bite-sized updates. The digest summarises the week's developments that have made the headlines. It's published every Friday, and is delivered straight to our subscribers' inbox.

Want to know what to expect? Click here to read the latest issue, and subscribe to receive it regularly.

## *Take our survey!*

We are constantly striving to make our newsletters better and more useful.
Your opinion matters: Take 30 seconds **to answer our questionnaire.**

**About this issue**
Issue no. 56 of the *Digital Watch* newsletter, published on 2 February 2021 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Andjelković, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Pavlina Ittelson, Marco Lotti, Marilia Maciel, Nataša Peručica, Vladimir Radunović, Sorina Teleanu | Design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić, Diplo's CreativeLab. | Get in touch: digitalwatch@diplomacy.edu

**Go deeper with more resources**
Wherever you see the blue icon click on it in the digital version to access the source or additional resources.

**On the cover**
*In the cards for 2021.* Credit: Vladimir Veljašević

Geneva Internet Platform
DigitalWatch

The Geneva Internet Platform is an initiative of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO
www.diplomacy.edu