Geneva Internet Platform
DigitalWatch
dig.watch

Issue 52, July & August 2020
Newsletter

US-China tech dispute wages on

TRENDS

Tech disputes between the USA and China continue, privacy remains in focus, and tech companies face antitrust investigations.

Pages 2–3

PRIVACY SHIELD

What does the invalidation of the EU-US Privacy Shield mean for cross-border data transfers?

Page 6

ANTITRUST

The four Big Tech companies are in the spotlight again over their market position and anticompetitive practices.

Page 7

DIGITAL FINANCE

Access to digital finance can support sustainable development. But several barriers and risks need to be tackled first.

Pages 8–9

The top digital policy trends in July & August

Each month we analyse hundreds of unfolding developments to identify key trends in digital policy and their underlying issues. These were the trends in July and August.

1. The US-China tech dispute wages on

The month of August saw the tech dispute between the USA and China take new forms, as US authorities launched new actions against Chinese tech companies.

On 6 August, President Trump issued two executive orders targeted at the video-sharing mobile app TikTok (owned by Chinese company ByteDance) and the social media, messaging, and e-payment app WeChat (owned by Tencent). The orders present the two apps as national security threats, arguing, among other points, that the user data they collect might be handed over to the Chinese government. Transactions between these companies and anyone subject to US jurisdiction are banned starting 45 days after the date of the orders. But the orders are not clear on the types of transactions referred to; these are to be determined by the Secretary of Commerce.

A week later, a third order required ByteDance to sell its US assets and remove the data of all US users within 90 days. It stated that the US authorities had 'credible evidence' that the Chinese tech giant could take action to imperil national security. The main bidders for the acquisition of ByteDance assets are Microsoft and Oracle. President Trump has also suggested that, if the transaction occurs, a portion of the sale price goes to the US Treasury, although the legality of such a request is unclear.

China reacted strongly to the three orders, accusing the USA of 'political manipulation and suppression'. In the USA, the orders are being challenged in court by TikTok, TikTok employees, and WeChat users. At this stage, their exact implications are difficult to assess. Questions have been raised as to the legality of a ban prohibiting individuals from using a certain app, especially when there could be freedom of speech implications (i.e., would banning TikTok infringe on users' ability to express themselves?). Then, if the US government requires Apple and Google to remove TikTok and WeChat from their app stores, would the companies simply follow the request or try to resist it and avoid setting a dangerous precedent (e.g. other governments banning apps provided by US companies)? The case of WeChat is even more interesting. In China, WeChat is extensively used by iPhone owners; if the order prohibits Apple from hosting the app, would Chinese users switch to another app or another phone? A poll among 800 000 WeChat users found that 750 000 of them would rather buy a new phone than stop using WeChat.

In parallel with the TikTok and WeChat controversies, the US administration also took new actions against Huawei, as the Department of Commerce (DoC) further restricted the company's access to US technology. Moreover, the Department of State announced the expansion of a programme called the Clean Network aimed at 'protecting America's critical telecommunications and technology infrastructure'. The programme envisions new action lines focused, among others, on ensuring that Chinese carriers are not connected with US telecom networks, and removing untrusted applications from US mobile app stores. Targeted explicitly at Chinese companies, the programme has been criticised over its potential to 'fracture the Internet into pieces'.

While all these US administration actions have the same geostrategic framework, each has a specific focus. In the case of Huawei, the focus is on telecom infrastructure (mainly 5G). Targeting WeChat means targeting an app which is used by US companies to conduct businesses with Chinese users and by the Chinese diaspora to communicate with their families. For TikTok, the key elements are data (given the app's wide use in the USA) and the fact that the app is a competitor for US companies. If the TikTok controversy seemed the easiest to 'unplug', this might be complicated by new Chinese export control rules that could require ByteDance to get a licence from the Chinese government before being able to sell TikTok. A WeChat ban could create significant communication disruptions for millions of people and negatively impact US businesses. Huawei is about future strategic developments. It remains to be seen how each of these cases will unfold.

2. Privacy-related court cases and investigations on the rise

The way in which tech companies handle user data is often at the core of heated debates. Almost every month we see new privacy cases being filed in courts

and new investigations being launched by data protection authorities (DPAs). This has also been the case in July and August.

For a start, international data transfers and their privacy implications made the headlines as the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield which had been governing the transatlantic data flows since 2016. Developed by the European Commission and the US DoC, the Privacy Shield functioned as a tool for companies to self-certify their adherence to EU data protection standards when transferring personal data from the EU to the USA. Now, the CJEU has ruled that the mechanism does not offer sufficient protection of privacy rights.

The court ruling does not mean that EU-US data transfers can no longer happen, but it does mean that companies face a high compliance burden and must switch to alternative data protection safeguards. *Read more on page 6.*

Beyond the Privacy Shield debates, tech companies have continued to be scrutinised for their privacy practices. In Belgium, the DPA fined Google €600 000 for failing to delete links to articles deemed harmful to a person's reputation under the EU's right to be forgotten. In the USA, Twitter is being investigated by the Federal Trade Commission over misusing personal data: between 2013 and 2019, the company used data provided by users for security purposes to target them with ads. Facebook-owned Instagram is facing a lawsuit in California, accused of collecting the biometric data of up to 100 000 million users without their consent. And the French DPA has launched an investigation into TikTok's compliance with the EU General Data Protection Regulation (GDPR).

These and other similar cases demonstrate that authorities and users alike continue to place an increased importance on how tech companies treat personal data. What seems to remain unclear is the companies' willingness to improve their compliance with privacy regulations, even when faced with fines and court cases.

3. Antitrust: Tech companies in the spotlight (again)

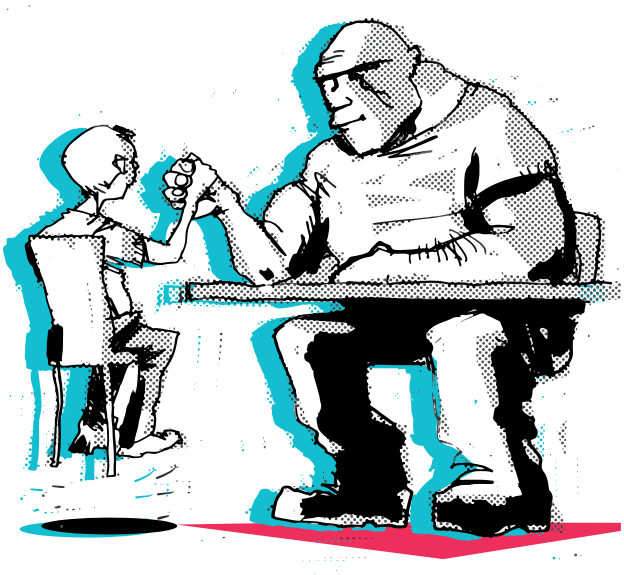
The four Big Tech companies – Apple, Amazon, Google, and Facebook – have been in the spotlight again over antitrust issues. They are facing numerous investigations in the USA, some of which may soon result in formal action.

In July, the four CEOs appeared before Congress for questioning by the House Judiciary Antitrust Committee, one of the players investigating Big Tech. This marked the first time that all four CEOs were questioned during the same hearing. *Read more on page 7.*

Beyond the USA, Big Tech faces other woes. The European Commission, which has so far fined the companies billions of euro, has announced new inquiries. These include an investigation into Google's planned acquisition of Fitbit and a sector inquiry into the Internet of Things (IoT) market for consumers. Meanwhile, Telegram's antitrust complaint against Apple adds more pressure to ongoing investigations on the company's App Store.

Elsewhere, the Australian Competition and Consumer Commission has proposed a draft code allowing media outlets to bargain with digital platforms like Google and Facebook over payments for including news in their services, while the UK Competition and Markets Authority's market study into online platforms and the digital advertising market explains that 'competition is not working well in these markets, leading to substantial harm for consumers and society as a whole'.

The action undertaken by regulators in the USA compared to that in the EU and other regions varies considerably. The view of the dominance of Big Tech and the need to review existing laws and enforcement practices, however, is across the board. The tougher question is to agree on what type of action is needed.



Digital policy developments in July and August

The digital policy landscape is filled with new initiatives, evolving regulatory frameworks, and new legislation and court judgments. In the *Digital Watch* observatory – available at **dig.watch** – we decode, contextualise, and analyse ongoing developments, offering a digestible yet authoritative update on the complex world of digital policy. The monthly barometer tracks and compares the issues to reveal new trends and to allow them to be understood relative to those of previous months. The following is a summarised version; read more about each development by clicking the blue icons, or by visiting the Updates section on the observatory.

decreasing relevance

Global IG architecture

The Internet Governance Forum (IGF) outlined plans for its 15th annual meeting, to be held entirely online.

same relevance

Sustainable development

The UN launched a 2030 Connect online platform to promote science, technology, and innovation for sustainable development. The African Union launched the African E-Commerce Platform.

The UN's Sustainable Development Goals (SDGs) Report 2020 showed that the world is off track to meet the SDGs by 2030. The 2020 UN E-Government Survey highlighted the persistent digital divide.

The European Commission launched a European Skills Agenda.

increasing relevance

Security

The EU imposed its first-ever cyber sanctions.

Twitter accounts of high-profile individuals were hacked. A cyber-attack caused extensive damage to an Iranian nuclear facility.

The Intelligence and Security Committee in the UK Parliament published a report on Russian influence and cyber operations. European law enforcement agencies shut down an encrypted communication platform used by criminals. An Interpol report assessed the impact of COVID-19 on cybercrime. The Australian government published its Cybersecurity Strategy 2020.

increasing relevance

E-commerce & Internet economy

The General Court of the EU annulled the 2016 decision of the European Commission regarding the Irish tax ruling in favour of Apple.

Apple, Amazon, Google, and Facebook testified before US Congress in an antitrust hearing. The European Commission announced an investigation into the acquisition of Fitbit by Google. Telegram filed an antitrust complaint to the EU against Apple's App Store. Online sellers in India filed an antitrust case against Amazon.

Australia started consultations on a news media bargaining code.

The Organisation for Economic Co-operation and Development (OECD) released a global tax reporting framework for digital platforms in the sharing and gig economy. Facebook agreed to pay France €106 million to settle a dispute on revenue tax.

increasing relevance

Digital rights

The Belgian DPA fined Google €600 000 in a right-to-be-forgotten case. UK and Australian DPAs launched a joint investigation into Clearview AI. The French DPA started an investigation into TikTok over privacy concerns. A lawsuit was filed in the USA against Facebook's Instagram over alleged illegal collection of biometric data.

Internet access restrictions were reported in Ethiopia, Mali, Iran, Somalia, and Belarus.

Facebook and Twitter took action against posts by US President Trump and his campaign over false COVID-19 claims. TikTok announced new policies to tackle misinformation ahead of US elections. Twitter announced new labels for government and state-affiliated media accounts. Attorneys general in 20 US states asked Facebook to take more measures against online harassment, discrimination, and misinformation.

increasing relevance

Jurisdiction & legal issues

The CJEU invalidated the EU-US Privacy Shield.

The US President issued executive orders to 'address the threats' posed by TikTok and WeChat.

Turkey adopted a controversial law regulating social media.

The CJEU ruled that YouTube is not required to share certain personal information of users who upload films illegally on its platform.

The Court of Justice of the Economic Community of West African States asked Nigeria to amend or repeal its cybercrime law.

A UK court ruled that the use of facial recognition technology (FRT) by the South Wales Police was unlawful. Amazon, Google, and Microsoft were sued over using photos to train FRT systems.

same relevance

Infrastructure

Google announced a subsea cable connecting the USA, the UK, and Spain.

The UK decided to ban Huawei from its 5G networks.

Bangladesh ordered Internet service providers to stop offering free access to social media services.

The European Commission launched an antitrust inquiry into IoT for consumers. The UK published proposals for regulating the security of consumer IoT devices.

same relevance

New technologies (IoT, AI, etc.)

Saudi Arabia adopted an AI strategy. The US Intelligence Community released a set of principles for AI ethics. New Zealand launched an Algorithm Charter for government agencies. The UK Information Commissioner's Office published guidance on AI and data protection.

The USA announced a blueprint for a national quantum Internet. Japan revealed plans to develop a quantum cryptography communication network.

EU-US Privacy Shield invalidated: What does it mean?

In a long-awaited decision, the CJEU delivered its judgment in Case C-311/18 — Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (the so-called Schrems II) invalidating the Privacy Shield and confirming that data protection rights in the EU are human rights.

Back to the negotiating table

The issue of personal data transfers from the EU to the USA has been in the spotlight for many years. The predecessor of the Privacy Shield, the 2000 Safe Harbour Framework, was invalidated by the CJEU in 2015 (Schrems I case). On 16 July 2020, the CJEU invalidated the Privacy Shield Framework for the same reasons: the lack of limitations on surveillance by the US intelligence community and a lack of judicial remedies for EU citizens in the USA in the event of personal data breaches.

The Schrems II judgement has left the EU and the USA with the uneasy task of negotiating – for the third time – a framework for transatlantic data transfers that fully comply with EU data protection regulations and the judgement. It is expected that the negotiations will have to address the lack of US federal data protection regulations and the need for the US judicial system to allow EU citizens to claim their data protection rights. They may also reopen discussions on the US Clarifying Lawful Overseas Use of Data Act (which allows US law enforcement to access data on servers of US-based companies, regardless of where the servers are).

Implications beyond EU-US relations

The Schrems II judgement has shed light on how to evaluate whether EU standards for personal data protection are met in other countries – such as rule of law, respect for human rights, adequate safeguards in national security and defence laws, the presence of an independent authority enforcing of data protection rules, and effective court remedies for EU citizens.

The task of evaluating the adequacy of personal data protection in third countries has now been transferred to the data exporters (EU companies transferring data out) and the data importers (third country companies receiving data). As described by the German state of Baden-Wuerttemberg's DPA in its guidance, EU companies are to undertake a review of where the personal data of EU citizens is transferred, and whether such third countries provide adequate protection. The German DPA has acknowledged that the Schrems II ruling is 'imposing an extreme burden on the companies'.

Standard contractual clauses

The CJEU confirmed that companies may use standard contractual clauses to transfer the personal data of EU citizens. However, it urged them to provide 'additional safeguards' for these transfers. Such safeguards have not been clarified by the CJEU, but the European Data Protection Board (EDPB) has indicated that it is developing guidance in this regard. Solutions could include the encryption of personal data or the introduction of data localisation rules. With respect to the US transfers, however, the CJEU's decision means that even the approved personal data transfer mechanisms are not appropriate, since US laws do not provide essential equivalency with EU standards.

What next?

The Schrems II judgement has caused quite a shake-up in personal data transfers. The EDPB is now looking into reevaluating adequacy decisions of the European Commission related to other countries, as well as interpreting the Schrems II judgement and providing guidance to authorities and companies on how to proceed. The first enforcement decisions of the judgement by national DPAs will also create a blueprint for moving forward.

Even though the Schrems II judgement and relevant authorities (such as the EDPB and the Berlin Commissioner for Data Protection and Freedom of Information) call for an immediate suspension of personal data transfers out of the EU to third countries not providing adequate levels of protection, the reality remains that data transfers are still taking place. The proposed approaches for clarifying the conditions for personal data transfers outside the EU (e.g. EU-US negotiations on a new mechanism, use of standard contractual clauses with evaluations of third countries' legal systems by companies, or awaiting enforcement decisions by DPAs) are neither fast nor simple, and the next weeks and months will show how this issue will be resolved.

Read more on the implications of the Privacy Shield invalidation.

Antitrust: Big Tech under scrutiny

The four Big Tech companies – Apple, Amazon, Google, and Facebook – were in the spotlight again. In July, they appeared before US Congress as part of an investigation into the dominance of tech companies. For the first time, they faced collective scrutiny.

Have the four Big Tech companies grown too much? Are they exerting too much influence on the economy and on democracy? These are some of the questions that have been brewing in Washington's mind in the past few years.

Leading the House Judiciary Antitrust Subcommittee's hearing, chairman David Cicilline explained that 'simply put, they have too much power'. They each control a key segment of the market, they surveill companies to assess potential competitive threats, and they abuse their dominant position.

The CEOs have a different – but shared – opinion. Punctuated by personal stories of humble beginnings, the CEOs' strikingly similar written statements delivered eight key messages:

1. We create jobs.
2. We invest heavily in the USA.
3. We help small businesses.
4. We care for our consumers and society.
5. We compete with big global players.
6. We nurture American values.
7. We solidify America's digital leadership globally.
8. Therefore, big is not bad.

Main differences in the statements reflected the companies' relations with China. Apple, which relies on China for its supply chain and a large user base, is careful to avoid any reference to the country. Facebook, which has no operations in China, is the most critical.

The CEO's statements hardly answered the questions posed by the House Judiciary. The committee wanted to determine how dominant the Big Tech's position is. But more than that, it sought the CEOs' testimony on perceived antitrust behaviour, giving them the chance to reply. Harm is not only measured through prices; certain practices, such as lost competition due to questionable behaviour, are just as bad.

Displaying considerable knowledge about the complex market in which tech companies operate, representatives grilled the CEOs on several issues and allegations – most of which the CEOs did not deny.

For instance, Google was questioned on the Yelp case as one example of anti-competitive behaviour, in which Google reportedly threatened to delist Yelp from its searches after the latter complained that Google stole its restaurant reviews.

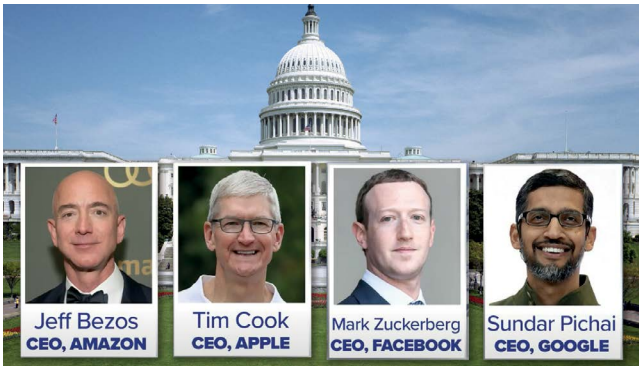
Amazon was grilled about the Quidsi case – in which Amazon reportedly dropped the prices of baby products to drive a competitor out of the market – and the issue of counterfeit goods where the platform 'acts like it's not responsible' even though it profits from the sales.

Facebook was accused of using copy-acquire-kill tactics, in which it allegedly uses data to spy on other companies, and then threatens potential competitors with consequences if they do not agree to be acquired. Apple was questioned about its App Store practices, referring to the 30% flat commission it charges app developers.

The hearing confirmed that there is clear consensus that something needs to be done. What is yet unclear is which action to take.

One of the key questions is whether the current antitrust laws need to be updated to effectively regulate tech companies that have grown extremely large. Other courses of action include opening up the merger review process to public comment, and breaking up the biggest monopolies.

What the hearings have provided, together with a months-long collection of documents, is mounting evidence of antitrust behaviour. The next potential step is to see whether the companies – all of them or any of them – will be taken to court.



Digital finance in the spotlight

This summer, digital finance came into focus as a renewed attempt to accelerate achievement of the SDGs. The UN Secretary-General's Digital Task Force (DFTF) issued a report summarising current trends and new possibilities in digital finance. The report anchors inclusive finance in the wider context of digital policies related to the digital divide, cyber vulnerabilities, data protection, and market concentration.

The DFTF was mandated to recommend and catalyse ways to harness digitalisation to accelerate financing of the SDGs. Its report titled *People's Money: Harnessing Digitalization to Finance a Sustainable Future* addresses some of the key barriers and risks to digital finance and proposes a set of recommendations on how to overcome the underlying setbacks and secure the financing of sustainable development. *Read our overview of the report.*

The DFTF report is anchored in the fast pandemic-driven changes in the economic and social landscape of the modern world. In a just-in-time reflection, it focuses on how the COVID-19 crisis has altered the way we access financial services. According to the findings of VeriTran, the use of digital wallets has increased globally by 180% since the outbreak. While this transition was easy for those with access to financial services and institutions, the situation was somewhat different for the 1.7 billion underserved.

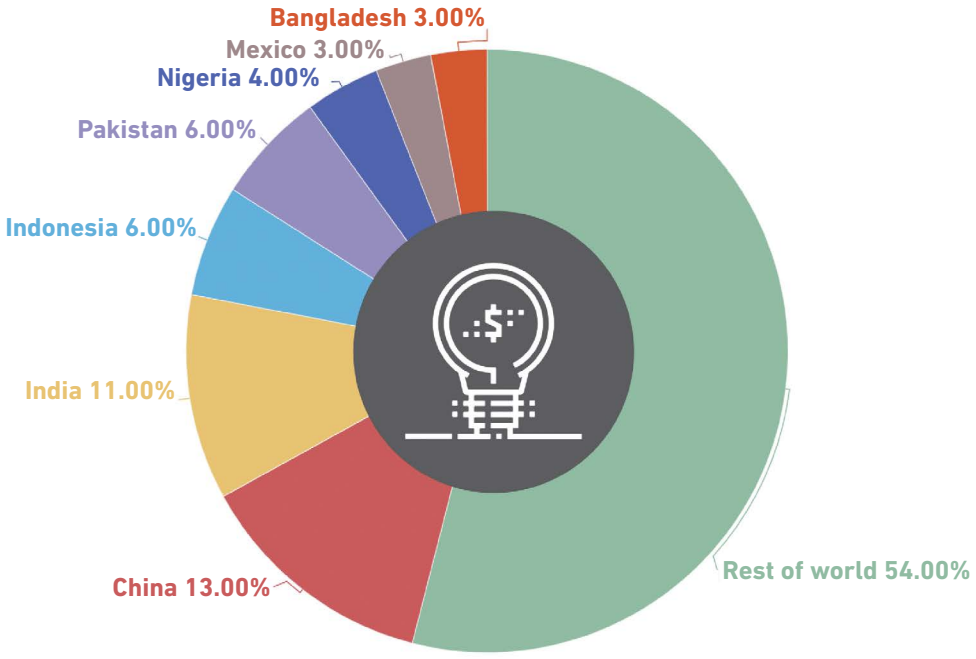
Digital finance in a nutshell

Digital finance centres on the idea that individuals and companies can access payments, savings, and credit products through digital infrastructure including the Internet and mobile devices, without ever entering a bank branch. Digital finance can essentially foster financial inclusion by allowing millions of unbanked to access financial services.

Identifying the unbanked

The majority of unbanked individuals are from developing countries in sub-Saharan Africa and South Asia. Moreover, nearly half of all unbanked adults live in seven economies.

Distribution of unbanked adults



Source: Global Findex database (2017)

This divide becomes even more apparent when placed in the context of gender. Roughly 56% of unbanked individuals are women. Despite some success stories (for instance, the penetration of mobile money services such as Orange money that help increase the financial inclusion of the underrepresented), the lack of access to official IDs, along with lower levels of mobile phone ownership, digital literacy, and financial capability are cited as the main obstacles faced by women accessing digital financial services.

With regard to other vulnerable groups including indigenous people, older people, and refugees and the internally displaced, isolation, the insufficient engagement of the private sector, as well as inadequate access to ICTs are also identified as significant challenges to digital financial inclusion. Similar setbacks are faced by an estimated 80% of people with disabilities in low- and middle-income countries who lack access to adequate assistive technologies.

Unveiling the potential of digital technology

Digital technology has the potential to foster financial inclusion. In India, for instance, the government has used biometric identification to promote access to digital financial services (e.g. by connecting ID cards with mobile phones and financial service accounts). This has resulted in a significant increase of financially included individuals (from 54% in 2014 to 81% in 2018). A rise in the number of banked individuals has also been observed in Mexico, where Banco Azteca increased its customer base from 0 to 8 million in 5 years by connecting electronic banking to large retail chains.

Although digital technologies, in particular mobile-based assistive technologies, still remain at the early stages of development and have limited financial support, they are being recognised as a means to increase the financial inclusion of people with disabilities. Strides are being made, for instance, in the domain of voice-assisted banking.

FinTech or TechFin?

Jack Ma, the founder of Alibaba, argues that we should use the term TechFin instead of FinTech, since technology is more important in achieving inclusive finance. This linguistic subtleness reflects a wider discussion on whether tech companies or banks will be leaders in the future of financial developments.

If developing countries succeed in making use of digital technologies and other tools to increase access to digital financing, this can act as an enabler of social and economic development. This point was equally emphasised by the DFTF in recognising digital finance as a 'key step' in the formalisation of two-thirds of the global informal workforce; mobile money accounts provide the underserved with access to finance, social safety nets, and the formalisation of small savings and microinsurance.

Understanding the risks of digital finance

As highlighted by the DFTF, digital finance also comes with a number of challenges. Attention is particularly drawn to cybersecurity risks which, according to surveys conducted by the International Monetary Fund (IMF) in 2018, can cause significant damage to financial institutions ranging from USD 100 billion to USD 350 billion. Money laundering, fraud, and financing of terrorism are equally regarded as threats that increasingly involve digital currency and crowdfunding platforms.

At the citizen level, privacy violations such as identity and data theft in the context of mobile-phone scams oftentimes result from the lack of digital financial literacy competences.

Acting on digital finance

Realising the opportunities and fallback of digital finance, in recent years, a noticeable rise in action on the matter has been seen at both national and international levels. To illustrate, the EU has undertaken an initiative to develop a new digital finance strategy that seeks to improve access to and efficiency of financial services, but also help overcome risks and barriers associated with digital finance through financial oversight mechanisms.

More recently, Singapore has established the Asian Institute of Digital Finance, whose role will be to promote new tech-driven financial services and encourage education in related fields. Malaysia and Indonesia have agreed to 'establish a collaborative framework to develop a fintech ecosystem in both market'. In Geneva, the Building Bridges summit (October 2019) started linking financial and development communities with the aim to establish Geneva as a hub for sustainable finance. Geneva, as host of many digital policy organisations, can play an important role in connecting digital finance with trade, security, and standardisation processes in the digital realm.

Policy discussions in Geneva

The COVID-19 crisis has pushed several discussions, negotiations, and processes online; in other cases, meetings have been postponed. Geneva-based organisations have adjusted quickly to the new online reality. The global focus on health and humanitarian issues has increased the relevance of Geneva dynamics for global governance. The following updates cover the main discussions of the past two months. For event reports, visit the Past Events section on the *Digital Watch* observatory.

World Summit on the Information Society Forum 2020 | 22 June–10 September 2020

Held entirely online, the WSIS Forum continued in July and August with a series of virtual sessions exploring diverse digital policy topics. Among them were several high-level policy sessions which discussed bridging digital divides and fostering inclusiveness and access to information for all; gender mainstreaming and ICTs; the role of ICT applications and services in promoting sustainable development; mechanisms for building confidence and security in the use of ICTs; the role of ICT and the digital economy in trade/financing for development; and capacity building and e-learning.

Human Rights Council: 44th Regular Session | 30 June–17 July 2020

This session of the Human Rights Council (HRC) featured discussions on a wide range of issues, from the rights to education and freedom of expression, to the rights of women and children. Included in the agenda was a panel discussion on the impacts, opportunities, and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights; the discussion built on the 2019 HRC Resolution on New and emerging digital technologies and human rights. Two advanced reports with direct relevance to digital policy were presented during the session: a report of the United Nations High Commissioner for Human Rights on the *Impact of new technologies on the promotion and protection of human rights in the context of assemblies* and a report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance on *Racial discrimination and emerging digital technologies: a human rights analysis*. The report on *Disease pandemics and the freedom of opinion and expression* presented by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also touched on issues related to Internet access, seen as 'a critical element for health-care policy and practice, public information and even the right to life'.

WIPO Conversation on Intellectual Property and Artificial Intelligence: Second Session | 7–9 July 2020

Held online, this session brought together over 2000 participants (representing member states of the World Intellectual Property Organization (WIPO), academics, and scientific and private organisations) to discuss the impact of AI on intellectual property (IP) policy. Continuing a debate that started in September 2019, the session allowed for an in-depth discussion on the revised Issue Paper on IP Policy and AI, which explores questions and issues arising for IP policy as a consequence of the increasing use of AI as a general-purpose technology. Specific issues discussed included IP protection for AI-generated and AI-assisted works and inventions; patentability, disclosure, and guidelines for AI inventions; and copyright in AI training data. These debates will feed into a third session of the Conversation on IP and AI, to be held in November 2020.

The main global digital policy events in September

Here we take a look ahead at the digital policy calendar to highlight the main discussions taking place in the next few weeks across the globe. For more details and for the proceedings of some events – including summary reports and digests from individual sessions – please check in regularly at the *Digital Watch* observatory.

7–10 SEP
WSIS Forum 2020: Final Week (online)

The 2020 WSIS Forum will culminate with a final week which will include policy statements, interactive high-level dialogues, a WSIS Prize ceremony, a ministerial roundtable, as well as a series of WSIS Action Line facilitation meetings. Session reports from the final week will be available on the *Digital Watch* observatory.

14 SEP–6 OCT
Human Rights Council – 45th Regular Session (Geneva)

The Human Rights Council will consider the annual report of the United Nations High Commissioner for Human Rights, and reports of the Office of the High Commissioner and the Secretary-General. It will also discuss the promotion and protection of human rights; human rights situations in several countries; and combating racism, racial discrimination, xenophobia, and related forms of intolerance, among others.

15–30 SEP
75th Session of the UN General Assembly (UNGA 75) (New York)

The UNGA will mark its 75th anniversary on 21 September with a high-level meeting themed 'The Future We Want, the UN We Need: Reaffirming our Collective Commitment to Multilateralism – confronting COVID-19 through effective multilateral action'. The General Debate will be held under this theme on 22–26 September and on 29 September, and will focus on the most vulnerable, as well as on ensuring that partnerships to achieve the 2030 Agenda adapt to the crisis. An analysis of the digital issues covered by the speeches will be available on the *Digital Watch* observatory.

21–25 SEP
SEEDIG 6 (online)

Held for the sixth consecutive year, the annual meeting of the South Eastern European Dialogue on Internet Governance (SEEDIG) will discuss some of the most pressing Internet and digital policy issues in South Eastern Europe and the neighbouring area (SEE+), from digitalisation and the digital economy, to online privacy and cybercrime. The discussions will be organised around four main tracks: Internet infrastructure, digitalisation, trust and security, and advanced technologies. In addition to the main sessions, the programme will also feature a series of SEEtalks, an innovation track, and an 'Online Living Library'.

27–30 SEP
APrIGF 2020 (online)

Originally planned to be held in Kathmandu, Nepal, APrIGF will move online to tackle four sub-themes: cybersecurity, safety and trust; digital inclusion, gender equality and diversity; human rights and ethics; and innovation and development. Some of the issues on the agenda are cybernorms, online child abuse, women's safety online, encryption, techical capacity buidling, access to information, digital gender divide, digital rights, and online education.

30 SEP–1 OCT
AI Summit 2020 (online)

The 2020 edition POLITICO's AI Summit is themed 'Can Europe keep up with its digital legacy and be a global AI rule-maker?'. It includes sessions on the AI global state of play, AI boundaries, Europe's place in the future AI world, Europe's digital legacy and competitiveness, strategies for AI implementation, and access needs.

September is the diplomatic 'New Year'

Traditionally, the diplomatic year starts in September when heads of states gather in New York for the UN General Assembly's annual debate. It's also a time when negotiations resume in conference rooms worldwide. This year, however, things are quite different. Head of the Geneva Internet Platform (GIP), Prof. Jovan Kurbalija, explains.

DW: How is this year different for diplomacy?

Prof. Kurbalija: COVID-19 has changed a few things. Instead of the habitual meetings as part of the high-level segment of the UN General Debate, state representatives will deliver their statements by video. Like our lives, diplomacy is also changing fast.

DW: What can we expect in the field of digital policy?

Prof. Kurbalija: *How*, *where*, and *who* will govern the digital space will come into sharper focus in the next few months. The UN Secretary-General's Roadmap for Digital Cooperation provides a framework and a space for a holistic approach to digital governance.

DW: What other issues should we keep an eye on?

Prof. Kurbalija: Emerging issues include the interplay between the environment and digital governance; digital standards as shapers of the digital world; shifts in geopolitics, especially with players such as China, the USA, and the EU; issues related to taxation, competition, and the digital economy, which are now maturing; and of course, the way digital technology is being used to fight the spread of COVID-19.

DW: How is the GIP approaching the coming months?

Prof. Kurbalija: At Diplo and the GIP, we are starting this 'new' diplomatic and academic year by continuing our work on the transformations in diplomacy. Online learning and diplomacy, which have been our modus operandi for many years, are even more prominent. In addition, we're digging deeper into AI and putting it to good use. At a time when Zoom meetings and online learning have become part of the daily routine for many, we will be focusing on launching more creative, engaging, and effective ways of learning and meeting online. Here's what we plan to launch in the coming weeks:

- A new version of the ***Digital Watch*** **observatory**, together with **a weekly newsletter** and **an updated barometer**.
- An AI-powered **Speech Generator for cybersecurity**.
- A **pilot Data Sandbox** that will help identify patterns in data on COVID-19, the SDGs, and other pressing digital policy issues.
- The new **Geneva Digital Atlas**, which will be a useful guide for navigating digital issues, actors, and processes in International Geneva.

For more updates, subscribe to the GIP newsletter

About this issue
Issue no. 52 of the *Digital Watch* newsletter, published on 3 September 2020 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđelković, Stephanie Borg Psaila, Andrijana Gavrilović, Pavlina Ittelson, Jovan Kurbalija, Nataša Perućica, 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
US-China tech dispute wages on. Credit: Vladimir Veljasević

Geneva Internet Platform DigitalWatch

The Geneva Internet Platform is an initiative of:
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
République et Canton de Genève
DiPLO www.diplomacy.edu