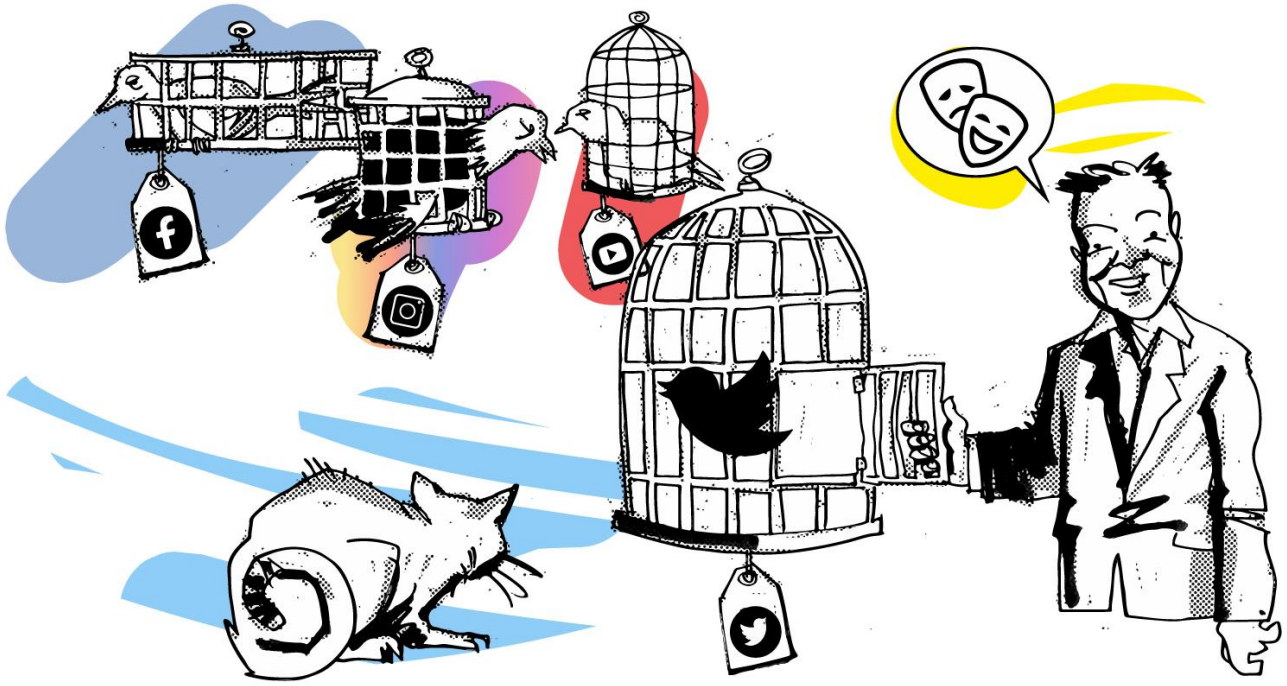
digwatch GENEVA INTERNET PLATFORM

NEWSLETTER

Issue 69, **May 2022**



Can Elon Musk save social media?

Pages 6–7

TRENDING

Content policy, the pause or end of USA-Russia cyber detente, and discussions in the OEWG on cyber.

Pages 2-3

DSA

A political agreement on the Digital Services Act (DSA) has been reached. We look at its implications for content policing in the EU and elsewhere.

Pages 8-9

E-COMMERCE WEEK

UNCTAD's e-commerce week 2022 put data governance in the spotlight, discussing data and digitalisation for development.

Pages 8–9

GENEVA

Many policy discussions take place in Geneva every month. Continue reading for the latest news from International Geneva.

Pages 11

Top digital policy trends

1. Content policy and the liability of internet intermediaries

Billionaire Elon Musk has acquired Twitter for $44 million. He has been tweeting up a storm about his plans for the platform, especially in terms of content moderation. *Read more about Musk's plans for Twitter on pages 6 and 7.*

EU regulators have warned Musk that his moderation plans will have to be in line with the Digital Services Act (DSA), the most important update in the regulation of intermediary liability in the EU in the last 20 years. Officials from the European Parliament, the French presidency of the Council of the EU, and the Commission have reached a political agreement on the DSA, opening the way for its formal adoption at the end of June. The regulation will come into force 15 months later. *Read more about the DSA on pages 8 and 9.*

The agreement on the DSA is not the only piece of news on platform liability coming from the EU this month. The Court of Justice of the European Union (CJEU) ended the EU's three-year legal battle with Poland over Art. 17 of the Copyright Directive (C-401/19 Poland v Parliament and Council). The court ruled that 'online content-sharing service providers are de facto required to carry out a prior review of the content that users wish to upload to their platforms.'

In April, social media platforms were active in combating what is considered Russian propaganda vis-à-vis the Ukraine war. YouTube took down a recording of a briefing given by Russian Foreign Ministry spokeswoman Maria Zakharova and Twitter disabled the account of the Russian television channel RT for violating their rules. Facebook reported that it disrupted several covert influence operations aimed at Ukrainians and set up a corporate fact-checker and an operations centre with Russian and Ukrainian speakers that monitors war-related topics on the platform.

Russian authorities are cracking down on social media platforms for spreading what they consider fake news and for not complying with the ground law. Russia's telecoms regulator, Roskomnadzor, announced it will start labelling Google as a 'violator of Russian law' and prohibit it from advertising. Twitter was fined 3 million roubles for failing to remove content prohibited in Russia, such as Nazi symbolism and instructions for homemade bombs. Meta Platforms Inc and TikTok were fined 4 million roubles and 2 million roubles, respectively, for failing to delete 'LGBT propaganda' posts. Meta, who was designated as a terrorist organisation by a Moscow court last month for allowing calls for violence against Russian soldiers, appealed against the ban on its activities.

While intermediaries and Russia continue their tug-of-information-war, the UN Human Rights Council adopted a resolution underlining that governments have the primary role in countering false narratives. The resolution, officially sponsored by Ukraine, Japan, Latvia, Lithuania, Poland, the UK, and the USA, calls on states to refrain from spreading or harbouring disinformation campaigns and to ensure that any responses to tackling disinformation comply with international human rights law.

2. US-Russian cyber detente is off

The USA has pulled out of cyber bilateral dialogue with Russia, effectively ending a period of cyber detente, which started after the 16 June 2021 summit of the presidents in Geneva. This period saw a significant softening of cyber tensions between the USA and Russia: a bilateral cyber dialogue was established; major cyberattacks similar to those affecting the Colonial Pipeline, JBS, and so on were absent; and successes in legal enforcement were achieved, such as the arrest of REvil hackers. On the multilateral level, both countries were involved in various global negotiations from the UN Open-Ended Working Group (OEWG) to the UN Cybercrime Ad Hoc Committee. The fact that they were talking to each other meant a lot within tense global relations. However, the Ukraine war, which can rightfully be called an earthquake in global geopolitics, has paused, or ended, the cyber detente.

Shortly after this US move, Five Eyes cybersecurity authorities issued a warning against Russia-backed cyberattacks on critical infrastructure in Ukraine and beyond. On the

other hand, Russia claimed that cyberattacks against its information resources by Ukraine are West-supported, noting 'Ukrainian special ICT operations centres trained by US and other NATO experts', and warned the consequences for 'inspirers and operators' of the 'cyber aggression' will be severe.

This fraying of good bilateral relations between two major cyber powers will inevitably shake up cyberspace, making it more dangerous and unstable in the coming period. While it is impossible to say whether the detente is over forever or if it will pick up again, it is indubitable that the political will to restart it will be absent for some time.

Yet, singular constructive developments are possible. A shining example is the US Treasury Department exempting telecommunications services from its latest sanctions against Russia, allowing the sale or supply of 'services, software, hardware, or technology incident to the exchange of communications over the Internet'. This is likely a concession to the calls from civil society activists to keep the internet on for Russian citizens and activists.

3. UN open-ended working group on cyber continues discussions

The second substantive session of the OEWG was overtaken by an organisational issue of how non-governmental stakeholders should participate. These undecided modes of multistakeholder participation were an obstacle to adopting the programme of work of the second session, resulting in discussions proceeding in an informal mode.

A quick summary of the discussions. As expected, the Ukraine war heavily impacted the group's discussion on threats, with the majority of participants calling on Russia to stop cyberattacks on Ukraine's information resources and cease fake news campaigns. Russia, on the other hand, brought up two new threats to states in cyberspace: disconnecting a country from the internet and cutting it off from the international payment system.

The ground the OEWG is standing on has started to shake, as the usefulness of the previously agreed-upon framework is being called into question. Some countries, such as Australia and the USA, want to move forward with the implementation of current norms, while others, such as Russia, Cuba, Iran, and Syria, believe that these norms are insufficient and should be discussed further. A heated debate ensued over the need for a new legally binding document, with Belarus, Iran, Syria, and Russia all calling for one.

The future of regular institutional dialogue looks as murky as ever. There is no consensus on whether the OEWG should remain the only negotiating platform for cyber issues or whether a Programme of Action (PoA) should be established.

There is, however, room for progress based on agreed confidence-building measures (CBMs) and capacity building. There is a general agreement that a global directory of Points of Contact (PoCs) should be created and turned into an active, operational, and regularly tested network. Countries expressed support for the Cybersecurity Capacity Maturity Model for Nations (CMM) which would allow developing countries to better set priorities for capacity building. There are also calls to increase international coordination through existing organisations such as the Global Forum on Cyber Expertise (GFCE) and the United Nations Institute for Disarmament Research (UNIDIR). A new mechanism that would allow compiling lessons learned and publishing comparative studies on different regional capacity-building programmes was suggested.

For a more detailed analysis, read our blog post. For a detailed rundown of who said what, read our event reports.

The agreement on the modes of multistakeholder engagement. The first sign of a willingness to compromise came shortly after the session ended. On 22 April, the OEWG reached an agreement on modalities for the participation of stakeholders as suggested by the Chair. NGOs with and without ECOSOC status should inform the OEWG Secretariat of their interest to participate. If no objections from states are raised, NGOs will be invited to participate as observers in the formal sessions, make oral statements during a dedicated stakeholder session, and submit written inputs to be posted on the OEWG's website.

Digital policy developments that made headlines

The digital policy landscape changes daily, so here are all the main developments from April. We've decoded them into bite-sized authoritative updates. There's more detail in each update on the Digital Watch observatory.

Increasing relevance

Global digital governance architecture

Over 60 countries and territories issued a Declaration for the Future of the Internet.

The Secretariat of the Internet Governance Forum launched the call for session proposals for IGF 2022.

Same relevance

Sustainable development

The UN launched new targets for universal meaningful connectivity.

The UAE Cabinet approved a new Digital Economy Strategy and established a Council for Digital Economy.

The European Parliament voted in favour of a common charger for portable electronic devices.

Increasing relevance

Security

Microsoft announced it had managed to disrupt Russian cyberattacks against Ukraine. China denied claims that it launched cyberattacks on Ukraine.

The US State Department launched the Bureau of Cyberspace and Digital Policy.

The US Department of Homeland Security initiated investigations against TikTok over hosting child sexual abuse material. Apple announced it is rolling out a child safety feature that alerts kids about nudity in photos.

Increasing relevance

E-commerce and the internet economy

The crypto industry cautioned the EU about privacy risks from new anti-money laundering rules. The web 3.0 community is raising similar concerns.

The Central African Republic passed a law accepting cryptocurrencies as legal tender. In Panama, the parliament approved a bill regulating the use of crypto-assets as payment systems.

The criminal court of Paris fined food delivery company Deliveroo for abusing the contractor status of its drivers.

Same relevance

Digital rights

Google introduced a 'reject all' button for tracking cookies for users in Europe.

Ranking Digital Rights' 2022 Big Tech Scorecard shows 'incremental progress' when it comes to internet platforms aligning their policies and practices with human rights standards.

Access to internet platforms was restricted in Sri Lanka as the government declared a state of emergency; services were reportedly restored after 16 hours.

Increased relevance

Content policy

The UN Human Rights Council adopted a resolution on tackling disinformation.

Russian telecoms regulator Roskomnadzor ordered Wikipedia to remove 'false information'. The UK announced new sanctions on Russian media.

Increased relevance

Jurisdiction and legal issues

A US court ruled that scraping publicly accessible data does not violate US computer hacking rules.

Mexico's Supreme Court ruled that the government-backed cell phone registry with biometric data is unconstitutional.

Decreasing relevance

Infrastructure

Google announced plans to build a subsea cable connecting Canada and Asia.

Increasing relevance

New technologies

The Council of Europe's Committee on AI held its inaugural meeting. The Central Cyberspace Administration of China announced it will inspect algorithms used by internet companies to verify compliance with regulations.

NATO approved the Charter of the Defence Innovation Accelerator for the North Atlantic to leverage advanced technologies for solving defence and security challenges. The USA and India agreed to establish a Defense Artificial Intelligence Dialogue.

Australia's government launched a public consultation to collect input for the development of a national quantum technologies strategy. The USA signed cooperation agreements on quantum information science and technology with Finland and Sweden. A bill on quantum-resistant cryptography was introduced in the US House of Representatives.

Can Elon Musk save social media?

The Twitter Board of Directors unanimously accepted billionaire Elon Musk's $44 billion takeover bid on 25 April after a rollercoaster of events. For the first time since 2013, Twitter will become a privately held company, and the content policy of the social media platform will most likely be affected.

Way back on 14 March, Elon Musk bought a 9.2% share of Twitter and became its largest shareholder. The public would not find that out until 4 April when Twitter published a note about the sale. The same note said that Musk was joining Twitter's board of directors. However, this would have prevented him from becoming the owner, either alone or as a member of a group, of more than 14.9% of Twitter's stock.

In an (at that time) odd twist of events, Musk decided not to join Twitter's board of directors. A few days later, he made an offer to buy Twitter for $54.20 per share. The takeover became hostile, unusual for a tech takeover, because the board rejected his offer. Twitter adopted a 'poison pill' defence; poison pills allow existing shareholders the right to purchase additional shares at a discount, diluting the ownership interest of a new, hostile party. In this case, Twitter adopted a limited duration shareholder rights plan which would 'reduce the likelihood that any entity, person or group gains control of Twitter through open market accumulation without paying all shareholders an appropriate control premium or without providing the Board sufficient time to make informed judgments and take actions that are in the best interests of shareholders'.

On 25 April, Twitter unexpectedly accepted Musk's bid. The agreement between the parties is that Twitter will be 'acquired by an entity wholly owned by Elon Musk'. Twitter will become a privately held company after the transaction, estimated to be worth $44 billion, is completed.

Why did Twitter's board change its mind? Rumour has it that Twitter did not want Musk to go directly to the shareholders in a so-called tender offer if the company's board did not accept his bid. Musk also campaigned on Twitter for a deal, and the company likely was not keen to be dragged through the mud. The board was forced to take Musk seriously when he secured $46.5 billion in financing, especially in the absence of other buyers.

What are Musk's plans for the platform?

Musk has mentioned many changes, such as introducing an edit button, allowing long-form tweets, encrypting direct messages on Twitter, and creating an ad-free Twitter. It is hard to guess which of these goals he will pursue. We're taking the goals he mentioned in the press release about the acquisition of the company at face value.

The press release quotes him as saying: 'Free speech is the bedrock of a functioning democracy, and Twitter is the digital town square where matters vital to the future of humanity are debated.' He added: 'I also want to make Twitter better than ever by enhancing the product with new features, making the algorithms open source to increase trust, defeating the spambots, and authenticating all humans. Twitter has tremendous potential – I look forward to working with the company and the community of users to unlock it.'

Free speech. Musk has repeatedly underlined his free speech vision for Twitter. At the TED2022 conference, Musk stated that he thinks Twitter should not regulate content beyond what is required by the laws of the countries in which it operates.

He also hinted that he would be against lifetime banning, noting: 'I think time outs are better than permanent bans.' However, Twitter already has a graded approach that includes deleting tweets or temporarily locking account(s) in the case of a first offence. Subsequent platform manipulation offences result in permanent suspension. The company's policy does, however, note that accounts will be permanently suspended at the first detection of a serious violation of platform manipulation.

The use of Twitter will always be free for casual users, but commercial and government users may be charged a small fee, Musk tweeted. What fee that might be, and if Twitter would differentiate between fees for smaller and

bigger companies, is still unknown. Reports also say that Musk intends to 'charge a fee when a third-party website wants to quote or embed a tweet from verified individuals or organizations'. Critics say this is against the right of free speech, as quoting a tweet amounts to fair use under copyright law.

Another one of Musk's plans is to expand the use of Twitter: 'Right now it's sort of niche. I want a much bigger percentage of the country to be on it, engaging in dialogue', Reuters quoted him as saying at the MET gala. Apparently, Musk envisions the platform 'as broadly inclusive as possible, where ideally most of America is on it and talking'. Does this mean that Twitter will become America's digital town square, not a global agora?

Open-source algorithms. Musk suggested that the algorithm that promotes and demotes posts should be posted on GitHub. This would reveal the maths behind the posts that appear on a user's Twitter feed, thus increasing trust in Twitter. However, a Twitter source told Wired that 'there is no 'master algorithm' for Twitter. Additionally, too much transparency may help those who want to game the system.

Defeating spambots. Musk's plan to 'defeat the spam bots or die trying!' seems to be authenticating humans. This would also stop the anonymity of contributions, which could endanger many people protected by said anonymity, especially those living under authoritarian regimes.

Reflection: Musk's Twitter experiment could be a success even if it fails

Executive Director of DiploFoundation and Head of the Geneva Internet Platform (GIP) Jovan Kurbalija reflected on Musk's Twitter experiment, estimating that it could be a success even if it fails.

If Elon Musk is successful in fixing Twitter, he believes Musk will have solved one of the most difficult policy issues of modern times. He would succeed in creating a welcoming environment for debate while also containing hate speech, trolling, and other platform misuses.

If Elon Musk fails to fix Twitter, he will still help to clarify the conversation about platform regulation. The current situation, in which social media platforms arbitrate public debate by allowing their own version of reality is, according to Kurbalija, untenable. Assigning such power to tech platforms goes against the visceral vibrancy of modern society, which expects to speak out loud (or be read on Twitter).

Whatever happens with Musk's Twitter reform, Kurbalija concludes, discussions on upholding freedom of expression, and addressing the risks of misinformation, truth policing, and platform responsibility for the content they host, will advance significantly.

Digital Services Act

The political agreement on the DSA was reached at the end of April, drawing attention to the intermediary liability and content regulation by the EU and its effects in other countries. We have a look at selected parts of this agreement and its implications for the road ahead.

The discussion on the major piece of the EU legislation has concluded with the European Commission announcing that the European Parliament and the EU member states had reached a political agreement on the DSA, a landmark regulation on the accountability of online platforms regarding illegal and harmful content. We wrote in our February newsletter about the key provisions of the DSA and the Digital Markets Act (DMA), two pieces of EU legislation seeking to redefine the role of digital platforms.

The DSA overhauls the intermediary responsibility regime in the EU and is expected to have effects beyond its borders, similar to the effects of the General Data Protection Regulation (GDPR).

The DSA applies to service providers (online intermediary services, hosting, caching service providers, and others), online platform providers (online marketplaces, app stores, and social media platforms), as well as very large online platforms (with more than 45 million active monthly users) that offer their services within the EU. While the transparency, accountability, and due diligence obligations apply to all entities under the DSA, the scope of the obligations increases with the size of the entity, with very large online platforms having the most extensive obligations.

The final text of the DSA is currently in the hands of technical negotiators to translate the political agreement into the final version of the legislation. The published framework, however, provides an insight into the modifications agreed by the negotiators at the European Council and the European Parliament. Some of the modifications include:

- The European Commission and EU member states will have access to very large online platforms algorithms on request and within a reasonable time to monitor and assess compliance with the DSA. This is particularly relevant for the recommender algorithms, such as Netflix's show recommendations or Instagram's newsfeed, where users should also be offered a recommender system 'not based on profiling'.

- Online search engines were added to the scope of the DSA as a new category of intermediary, but are not subject to strict removal obligations of content flagged as illegal. According to the Center for Democracy and Technology (CDT), the compromise reached provides scope for "a case-by-case assessment of the responsibilities of Google and the likes for illegal content, which is left to be clarified by a legal review".

- While the definition of illegal content is left to EU or national legislation, content targeting victims of cyber violence (such as revenge porn) must be removed immediately. Other content flagged as illegal shall be removed 'swiftly'.

- The agreement includes stronger protection of minors with platforms being obliged to take specific measures to protect them, including a complete ban on targeted advertising.

- Online platforms are prohibited from using dark patterns to manipulate users' choices. The European Commission is expected to issue guidance on the types of practices that constitute dark patterns under the DSA.

- Spurred by the current geopolitical situation, the agreement on DSA has added special measures in times of crisis. The European Commission may require very large online platforms to 'limit any urgent threats' for three months in the case of a public security or health crisis. This addition raised concerns of civil society stating that the European Commission would have the power to unilaterally

declare a state of emergency thus undermining democratic processes and the rule of law. We await the final wording of the DSA to see how the mechanism for times of crisis is set up and whether the concerns of civil society are addressed.

With respect to the enforcement of DSA, the draft certainly reflects lessons learned from the enforcement shortcomings of the GDPR. EU member states will have primary responsibility for overseeing compliance with and enforcement of the DSA, supported by a new European Board for Digital Services. For very large online platforms, the European Commission will undertake centralised supervision and enforcement.

Looking at what comes next, after the DSA text is finalised, it will be sent for approval to the European Parliament and EU member states, becoming enforceable in the first quarter of 2024. It is expected that the DSA and the DMA will come into force at the same time.

While the EU is described as leading in regulatory dominance, EU initiatives to rein in tech companies are not isolated. Other countries are also proceeding in their efforts to regulate intermediary liability and online platforms in general. China introduced its new platform policies last year, reshaping its tech sector to such an extent that it now seeks to ease the regulatory impact and stimulate its growth. In the USA, discussions on regulating online content and speech are well underway, even beyond Section 230 of the Communication Decency Act. Currently, the US Senate is discussing the drafts of the Platform Accountability and Transparency Act (PATA), the Digital Services Oversight and Safety Act (DSOSA), the Social Media NUDGE Act, and the Kids Online Safety Act. It remains to be seen how the global regulatory landscape will look when the DSA (and the DMA) become enforceable and how the diverse national regulations will reflect in discussions on an international level.

The GIP webinar Unpacking EU regulations on digital markets and services (DMA & DSA)'

1. Discussed the economic, ethical, and political challenges of the development of large digital platforms and intermediate services.
2. Analysed the legislative work carried out by European institutions.
3. Discussed the challenges linked to the implementation of these regulations in the global arena.

Our speakers were Mr Henri Verdier, Ambassador for Digital Affairs, Ministry for Europe and Foreign Affairs of France; Mr Prabhat Agarwal, Head of Digital Services and Platforms Unit, Directorate-General for Communications Networks, Content and Technology, European Commission; Dr Jovan Kurbalija, Head, Geneva Internet Platform (GIP); and Ms Marilia Maciel, Head of Digital Commerce and Internet Policy, Geneva Internet Platform (GIP).

Missed the event? Watch the recording.

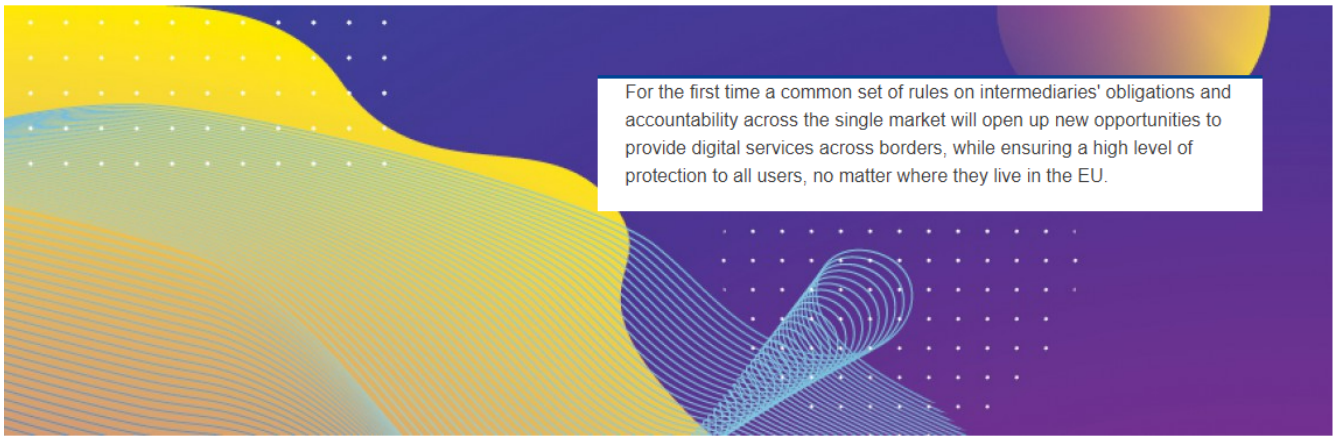


Image credit: European Commission

UNCTAD e-commerce week 2022: data governance under the spotlight

The UNCTAD e-commerce week took place from 25 to 29 April in a hybrid format. The overarching theme of the event – Data and digitalisation for development – set the stage for a timely discussion on the role of data and the distribution of wealth in the digital economy.

Global data flows are one of the key elements that bind the world economy. They are key to boosting productivity, fostering new products and processes, and creating new markets in the context of data-driven innovation. Data has also transformed production and distribution, thanks to continuous flows of data across value-chains and jurisdictions.

In economic terms, data has become a new form of capital for twenty-first-century knowledge economies. Nevertheless, data capital is increasingly concentrated in two countries, the USA and China, where a significant proportion of large digital platforms are based. UNCTAD's 2021 Digital Economy report provided an overview of this concentration, and the obstacles it creates for the meaningful inclusion of developing countries in the digital economy and for achieving the sustainable development goals (SDGs). The report was widely referred to during e-commerce week, and set the backstage for discussions therein.

This year's event enabled valuable information sharing among participants, as well as the cross-regional exchange of good practices. Sessions touched on a diverse range of topics, such as the role of standards in digital transformation, the implementation of online dispute resolution systems, and how data can be used to support local online marketplaces. It also provided an opportunity to take current discussions on data flows a few steps further, by allowing a diverse group of participants to engage in problem-shaping and agenda-setting, which are key elements for tackling data governance in a coordinated manner at the global level. In this respect, two topics stood out: the urgency of tackling the growing data divide among countries and regions, and the future governance of data flows.

Data governance is a multilayered challenge. It can be distilled from the sessions that more effort needs to be put into research to enhance understanding of the unique nature of data, as well as the structure, players, incentives, and obstacles in the data market. Concrete mechanisms to promote access to data and data sharing need to be devised and tested, from data sandboxes to data cooperatives. Emerging conceptual frameworks to promote access to data, such as the ideas of 'community data' and 'trustworthy data spaces' need to be further discussed, compared, and contrasted, to identify potential synergies. Most developed and developing countries are equally seeking to use data as a way to achieve socially relevant policy objectives.

In this scenario, it is important to enhance the opportunities for developing countries to influence the rules that will govern data, voicing their development-oriented priorities on the global stage. Capacity building will continue to be paramount to promoting data equity and avoiding future regulatory fragmentation.

The Geneva Internet Platform and Diplo reported from selected sessions at the UNCTAD e-commerce week. Visit our dedicated page on the Digital Watch website to read the reports.

Do not miss the opportunity to enrol in our upcoming course Data governance in the digital economy. The course will cover this issue holistically, from technical, economic, legal, policy, and geopolitical perspectives.

Policy updates from International Geneva

Many policy discussions take place in Geneva every month. In this space, we update you with all that's been happening in the past few weeks. For other event reports, visit the Past Events section on the GIP Digital Watch observatory.

The WIPO conversation on intellectual property and frontier technologies | 5-6 April 2022

The conference addressed how frontier technologies, such as AI, big data analytics, and blockchain can be used to address the growing challenges facing intellectual property offices (IPOs) in order to make IP efficient and accessible for everyone and everywhere. The fifth session encouraged information sharing across all stakeholders from IPOs to private enterprises and the sharing of diverse views from IP professionals, innovators, creators, and individuals.

The GIP reported from the Sharing Session: IPO AI tools and beyond. Presenters addressed four broad themes. First, AI could both improve and complicate an applicant's experience with patent filing platforms. IPOs need to investigate how to optimise the user journey. Second, AI could enhance the efficiency of IP administration in the same way it helps users. Third, there are certain human rights and organisational concerns among IPOs that adopt frontier technologies in their workflow. IPOs must ensure a smooth transition by looking into how AI impacts the work of their employees. Lastly, AI and frontier technologies might prove fruitful in battling intellectual property rights (IPR) infringements. Read our full session report.

14th Geneva Summit for Human Rights and Democracy | 6 April 2022

The Geneva Summit for Human Rights and Democracy was held in connection with the main annual session of the United Nations Human Rights Council, when foreign ministers gather in Geneva to force critical issues onto the international agenda. The Summit paid particular attention to urgent human rights situations that require global attention.

The Geneva Summit was sponsored by a coalition of 25 human rights NGOs from around the world. The 14th Session focused on the rights of political prisoners, the fight for freedom of expression in specific countries, as well as the fight against corruption.

Upcoming

What to watch for: Global digital policy events in April

12 MAY, International conference and opening for signature of the Second Additional Protocol to the Convention on Cybercrime (Strasbourg, France)

The Council of Europe Convention on Cybercrime will be strengthened with the Second Additional Protocol when member states sign off on enhanced cooperation and disclosure of electronic evidence on 12 May in Strasbourg. The Convention is the most relevant international criminal justice treaty on cybercrime and electronic evidence. The Protocol provides a legal basis for disclosure of domain name registration information and for direct cooperation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate cooperation in emergencies, mutual assistance tools, as well as personal data protection safeguards.

15–16 MAY, EU-US Trade and Technology Council Second Ministerial Meeting (France)

Following the inaugural meeting of the EU-US TTC that took place in September 2021 in Pittsburgh, the Second Ministerial Meeting will be held in Europe. The Council will come together on 15 and 16 May in France; the meeting will build on the progress made so far. According to the joint statement, high on the agenda are concrete actions regarding third-country cooperation, AI and emerging technologies, supply chain security, sustainability and energy security, conformity assessment and mutual recognition agreements, and stakeholder engagement.

16-20 MAY, Annual UN/CEFACT Forum (online)

The 38th United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Forum will take place virtually between 16 and 20 May. Experts from the public and private sectors globally will come together to discuss trade facilitation recommendations and e-business standards. Some of the central topics are private sector participation in national trade facilitation bodies, cross-border trade in agricultural goods, open banking and open finance, sustainable tourism, and the SDGs. Participation is open and registration is mandatory.

24 MAY, DC Blockchain Summit (Washington, DC, USA)

The DC Blockchain Summit is a one-day gathering of the most influential people working in the field of public policy action for digital asset and blockchain innovations. On 24 May, policymakers, entrepreneurs, business leaders, investors, representatives of federal and state agencies, and members of the United States Chamber of Digital Commerce will come together to discuss blockchain regulation, stablecoins, crypto, and current and future blockchain policy.

24–25 MAY, EU Cyber Act Conference (Brussels, Belgium)

The 2022 International Conference on the EU Cybersecurity Act will take place in Brussels and focus on the EU Cybersecurity Act, currently in the works. The Act will eventually create a broad-based, independent European body of cybersecurity Legislation as part of the 'single digital market' ambition. This year's conference will focus on the potential effects on current schemes and regulatory mandates, as well as new potential candidate schemes for key industry verticals such as internet of things (IoT), cloud, communications, payments, automotive, and more.

About this issue: Issue 69 of the Digital Watch newsletter, published on 11 May 2022 by the Geneva Internet Platform and DiploFoundation
Contributors: Boris Begović, Andrijana Gavrilović (Editor), Pavlina Ittelson, Jovan Kurbalija, Marco Lotti, Jana Mišić, Anamarija Pavlović, and Sorina Teleanu
Design: Diplo's CreativeLab | Get in touch: digitalwatch@diplomacy.edu
On the cover: *Can Elon Musk save social media?* Credit: Vladimir Veljasević DiploFoundation (2022)

The Geneva Internet Platform is an initiative of:

GENEVA INTERNET PLATFORM digwatch
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
REPUBLIQUE ET CANTON DE GENEVE
DiPLO www.diplomacy.edu