GENEVA INTERNET PLATFORM
digwatch
NEWSLETTER

Issue 64 – November 2021

Facebook facing faces

CONTENT

Social media platforms struggle with removing harmful content. In the hot seat: Facebook.

Page 1

PRIVACY SHIELD III

We look into the challenges that need to be solved to achieve an EU-US agreement on personal data transfers.

Pages 6-7

RANSOMWARE

31 countries + the EU huddled on anti-ransomware efforts.

Pages 8-9

METAVERSE

The newest hype: What is it and what are its challenges?

Page 10

Ongoing issues in digital policy

1. Dealing with harmful content online

Content moderation was the talk of the globe in October, with many social media platforms running into content moderation and regulatory struggles. Microsoft will pull LinkedIn out of China later this year because of pressure to comply with the Chinese government's requirements for internet platforms. Twitter's internal research has discovered that its algorithms amplify right-wing content – however, the company does not know why this is the case and will continue looking into it. But no other platform had it as rough as Facebook.

Facebook's ex-employee turned whistle-blower Francis Haugen testified in front of the US Congress that Facebook cares more about profits than users. She accused Facebook of harming children's mental health and amplifying division, extremism, and polarisation among its users. Haugen's testimony was corroborated by another whistle-blower, who at the moment of writing is still anonymous. In front of the UK parliament, Haugen cautioned that time is running out to regulate social media companies that use AI for content moderation.

A consortium of news agencies obtained redacted versions of Haugen's leaked documents. Dubbed 'The Facebook Papers', the documents show that the company has been struggling to combat vaccine misinformation and to moderate content in languages other than English. They also indicate that Facebook devoted markedly fewer resources to moderation in markets outside of the USA – only 13% of the budget for combating misinformation was directed beyond US borders, where 90% of its users are located. Additionally, the documents allege that Facebook ignored Instagram's harmful impact on teens' mental health and took limited action to stop sex trafficking via the platform. Its algorithms are fueling divisiveness, and its strategies are insufficient to curb posts inciting violence in countries at risk of conflict.

Spurred on by the revelations around Facebook (soon to be Meta), regulators everywhere are gearing up for a showdown with social media platforms. TikTok, Snapchat, and YouTube were questioned about how children are steered towards specific content on their platforms by the US Congress. Facebook, Google, Twitter, and TikTok also testified about combating harmful content to the UK parliament. India is seeking information from Facebook about the algorithms that Facebook uses for content moderation.

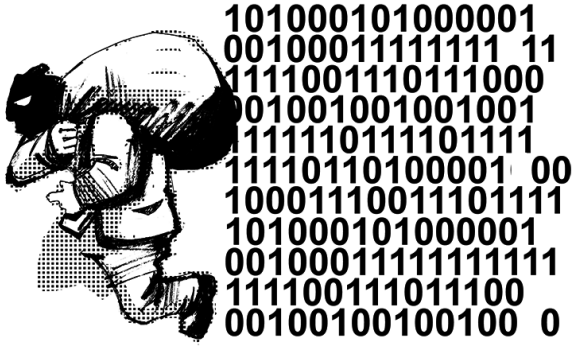
Is legislation the solution? The UK and Singapore certainly think so: the former will speed up its Online Safety Bill, and the latter passed a law to tackle 'foreign interference', which allows authorities to block content they consider hostile.

Interestingly, tech giants seem to agree: Twitter has stressed that criminality is determined by government bodies rather than the private sector. In its position paper on 'Protecting the Open Internet', Twitter called for regulations to clearly define the different categories of content that require moderation, especially when the content is lawful but 'a government believes there's a need to intervene'. Reacting to Haugens' testimony before the US Congress, Facebook CEO Mark Zuckerberg wrote 'the right body to assess tradeoffs between social equities is our democratically elected Congress.' He urged Congress to update internet regulations.

2. Countering ransomware

'We are observing the golden era of ransomware... it has become a national security priority...and some argue that it has not yet reached the peak of its impact,' the European Union Agency for Cybersecurity (ENISA) annual report about cyber threats cautioned.

The reason ransomware is prospering is that it has largely been uncontested, stated Sir Jeremy Fleming, the UK's cyber head. It is lawful to 'go after' criminal actors under international law, Fleming stated, but it is also not so easy: 'There's a lot of things here that need to go fall into place to make that happen, and we're quite a long way off really addressing the profit



model which is making this just so easy for criminals to exploit.'

The Netherlands and Australia are in favour of more defensive approaches. Ben Knapen, the Dutch foreign affairs minister, noted that diplomatic and legal channels take precedence but that Dutch intelligence services can respond to a ransomware attack threatening national security. The Defense Cyber Command can even carry out a counter-attack, but only as a last resort, stressed Knapen. Australia is planning to take a different but no less interesting approach. Under the new draft Critical Infrastructure Bill, the Australian Signals Directorate (ASD) would be able to take over control of critical infrastructure in the event of a ransomware attack. A coalition of companies has called for changes, requesting a statutorily-prescribed mechanism for judicial review and oversight and extending the window for mandatory reporting of an incident.

All three aforementioned countries also participated in the US-led Counter Ransomware Initiative, which gathered 31 countries and the EU and culminated in commitments on fighting ransomware transnationally. *Read more about the initiative on pages 8–9.*

On a positive note, the good guys notched a big win this month: The notorious ransomware group REvil, responsible for hacking Kaseya and JBS, was hacked and forced offline in a multi-country operation. The group may rebrand, as ransomware groups often do, but theories abound that it has lost the trust of the cybercrime community. These developments will likely make other ransomware groups pause and think.

3. Facial recognition: privacy in the crosshairs

All the way back in our July/August 2019 newsletter, we explained that the main concerns around facial recognition technology (FRT) were privacy, bias, and discrimination. This month, privacy concerns took centre stage.

Privacy advocates are concerned that Moscow's metro facial recognition payment system could be used by security agencies to surveil citizens. The system does, admittedly, sound powerful: it can recognise travellers even if they are wearing masks or glasses. The authorities, on the other hand, are pleased that Moscow now employs one of the largest use of FRT worldwide.

Scottish citizens were not happy to learn that their data from the NHS Scotland Covid Status app was being shared with tech companies, including the AI facial recognition firm iProov. More discontent arose throughout the UK upon learning that nine Scottish schools are using FRT to take payments for students' lunches. The system's cameras check against encrypted faceprint templates of the student's faces stored on servers at the schools. The UK Information Commissioner's Office has now stepped in, urging a less invasive alternative for payment.

A Finnish police unit was reprimanded by the country's Deputy Data Protection Ombudsman for the illegal processing of facial data. The unit experimented with identifying possible victims of child sexual abuse using the Clearview AI software. Clearview AI, whose facial recognition software has been under scrutiny for scraping data indiscriminately, has doubled down and scraped another 10 billion photographs from people's public social media accounts for its database.

Speaking of the private sector, in an unprecedented case, the South Korean government handed over 170 million photographs collected at Incheon International Airport to private sector AI developers, without the subjects' consent.

The old debate on whether to ban or legislate FRT will continue to rage on, especially if we look at the reactions of the EU and the USA over the past month. The EU parliament has called for a ban on automated recognition in public spaces of human features such as gait, fingertips, DNA, voice, and other biometric and behavioural signals. The parliament further called for a ban on private facial recognition databases (like the Clearview AI system), predictive policing based on behavioural data, and AI-enabled mass-scale scoring of individuals.

On the other side of the pond, the US White House Office of Science and Technology Policy (OSTP) is requesting information about technologies, including FRT, used to identify people and infer their attributes. According to the OSTP, 'In the 21st century, we need a "bill of rights" to guard against the powerful technologies we have created.' Before crafting a pivotal piece of legislation, it is clear the USA is looking to understand the technology better.

Digital policy developments that made headlines

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

low relevance

Global digital governance architecture

The European Commission published its 2022 work plan, which includes advancing 'A Europe fit for the digital age'.

G7 trade ministers agreed on principles to govern digital trade, covering open digital markets; cross border data flows; safeguards for workers, consumers, and businesses; digital trading systems; and fair and inclusive global governance.

G20 Leaders endorsed the OECD agreement on global tax rules.

low relevance

Sustainable development

ASEAN and the USA issued Leaders' Statement on Digital Development, committing to cooperate in cybersecurity, digital infrastructure, and the digital economy.

The European Commission launched an expert group to develop guidelines on disinformation and digital literacy for educators.

increasing relevance

Security

Ransomware gang REvil was hacked and forced offline by a multinational effort. UK, Australia, and the Netherlands detailed national ransomware plans. *Read more on pages 2 and 3.*

The international Counter Ransomware Initiative held its first meeting. *Read more on pages 8 and 9.*

ENISA report on cybersecurity threats assessed ransomware as the top threat in Europe and cryptocurrency the main pay-out method for threat actors.

Russia and the USA cosponsored a resolution on cybersecurity at the UN General Assembly, emphasising the adoption of the voluntary norms of responsible behaviour.

increasing relevance

E-commerce and the internet economy

A total of 136 countries have agreed on the OECD's new global corporate tax rules, which will affect big tech companies.

The International Chamber of Commerce published new global rules for digital trade transactions.

Amazon was accused of using seller data to copy products and manipulating search results to benefit those products.

Nigeria has launched eNaira, the African continent's first digital currency.

same relevance

Infrastructure

Facebook, WhatsApp, and Instagram suffered worldwide outages due to a faulty configuration of Border Gateway Protocol (BGP) settings.

Planned subsea cables include Africa-Europe cable by Google, Europe-US cable by Facebook, and 100% green Canada-Norway cable by Erikson.

same relevance

Digital rights

The European Commission launched an expert group to develop guidelines on disinformation and digital literacy for educators.

Eswatini and Sudan shut off internet access. Indonesian constitutional court ruled that internet blocks amid social unrest in 2019 were lawful.

Rwanda and Botswana enacted data protection laws. Brazil's Senate included protection of personal data as a fundamental right in the country's constitution.

---

increasing relevance

Content policy

Microsoft will pull LinkedIn from the Chinese market due to the challenging regulatory environment. China's regulator will build a 'civilised internet' by reshaping online behaviour and using the internet to promote socialist values.

Twitter's research shows its algorithms amplify content by the political right wing.

Facebook whistle-blower Frances Haugen testified on Facebook's products and practices before the US Congress and the UK parliament. A consortium of 17 American news organisations started the Facebook Papers Project, publishing internal Facebook documents obtained by Haugen.

Twitter called for legislation on content moderation. Facebook urged the US Congress to update internet regulations.

Lawmakers in the USA and UK questioned social media platforms on protecting children from harmful content.

---

low relevance

Jurisdictional and legal issues

Portuguese bill aiming to give platform drivers rights as employees and not as contractors is waiting for Parliamentary approval.

Google and Facebook colluded to undermine Apple's privacy protections.

---

increasing relevance

New technologies (IoT, AI, etc.)

UNCTAD15 conference concluded policies are critical to harnessing frontier technologies for good.

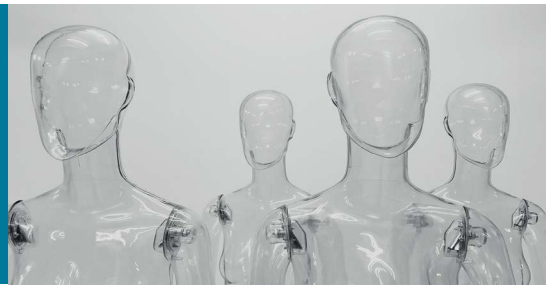
The EU parliament called for a ban on facial recognition in public spaces. The USA will develop a 'bill of rights for an AI-powered world'.

NATO's AI strategy outlines how AI can be applied to defence and security. The UN launched the AI for Road Safety initiative to reduce road traffic deaths and injuries.

Facebook will hire 10,000 people in the EU to build the metaverse. *Read more about the concept on page 10.*

#ICYMI:

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression presented her report to the UN General Assembly, calling for stronger efforts to close the gender digital divide and ensure that digital spaces are safe for 'women and non-binary people'.



Third time's a charm?

The discussion on personal data transfers between the EU and the USA is taking place now for the third time. Both countries recognise the importance of succeeding – for their bilateral relations and for positioning themselves as global leaders in digital policymaking. We look into the challenges that need to be solved to achieve a viable agreement.

For years now, the USA and the EU have been trying to establish a mechanism for the transfer of the personal data of EU citizens to the USA and satisfy the requirements of EU privacy legislation. The first framework, Safe Harbor, was struck down by the Court of Justice of the European Union (CJEU) in 2015 in the so-called Schrems I case. The second framework, the EU-US Privacy Shield, was invalidated in July 2020 in the so-called Schrems II case and was done so without a transition period, taking effect immediately.

The reasons for invalidating both Safe Harbor and Privacy Shield are strikingly similar and are at the heart of ongoing negotiations between the two governments. With the **different approaches to data protection regulations in the EU and the USA – which are literally an ocean apart – such negotiations are not an easy feat**. The EU takes a hardline regulatory approach, with the General Data Protection Regulation (GDPR) as the main vehicle for the protection of personal data. The USA takes a sectoral approach to privacy regulation and does not maintain a singular, comprehensive data protection law regulating the processing of personal data on the federal level.

The main issue is that in order for the personal data of EU citizens to flow into the USA without additional safeguards, **the USA is required to provide a level of personal data protection adequate to the one set in the EU's GDPR.** Such flows have important impacts on trade and the development of technologies such as cloud computing and AI.

Specifically, the new agreement on the transfer of personal data from the EU to the US must address **limiting the reach of US surveillance and establishing a new mechanism for redress.**

Limiting the reach of US surveillance

According to the CJEU, Sec. 702 of the US Foreign Intelligence Surveillance Act, which permits the US government to conduct targeted surveillance of foreign persons located outside the USA and US Executive Order 12333, concerning surveillance authorities for the US intelligence community, do not satisfy the requirements set by the EU. **EU regulation requires that data is collected and processed for specific, justifiable purposes using methods that are not disproportionately invasive of fundamental human rights** (necessity and proportionality principles).

Establishment of a new mechanism for redress

CJEU also decided that there is a lack of a redress mechanism for EU citizens in the USA.

EU citizens should be able to learn whether US agencies have collected or processed their data and seek legal remedies before US courts if their data was collected or processed in a way that violates the principles of necessity and proportionality. The previous effort of establishing a Privacy Shield Ombudsperson at the US Department of State was not deemed sufficient.

Potential solutions

In August 2020 – right after the Schrems II judgement – the US Department of Commerce and the European Commission announced that they started discussions on an enhanced EU-US Privacy Shield framework. In March 2021, the US Congressional Research Service released an informational report that summarised potential solutions such as:

- An Executive Order limiting bulk intelligence collection and providing additional redress mechanisms
- A diplomatic agreement for a new framework to replace the Privacy Shield or a data transfer treaty
- Legislation that limited bulk intelligence collection or created a cause of action for non-US persons in the event of unlawful collection

EU Justice Commissioner Didier Reynders, who is in charge of negotiations from the EU side, has remarked positively on many innovative proposals that are on the table.

Smooth sailing or rough seas

The pace of the negotiations is dependent on how many concerns can be addressed through the executive branch of the US government, which would be faster than going through Congress. Should Congress need to vote on legislative changes, especially with respect to changing the judiciary system to establish an adequate redress mechanism, it would take more time. Another question is how far the USA might go to satisfy the EU's court decision.

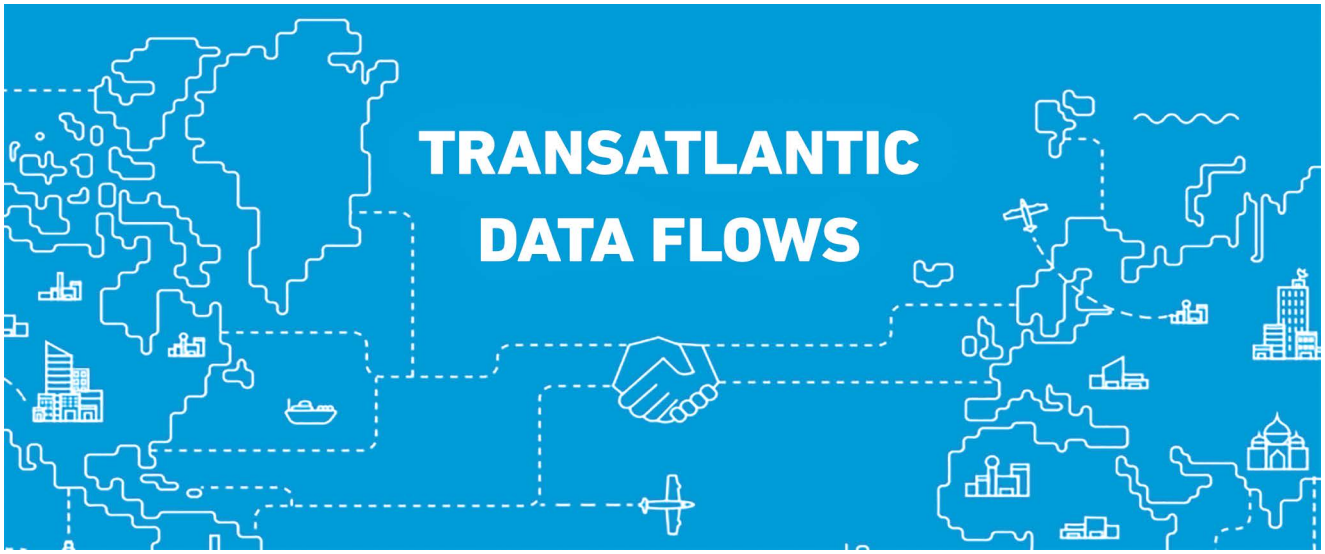
The EU and the USA must also take into account a more developed and mature regulatory global private data protection landscape since they negotiated the Privacy Shield last time. As many as 17 countries – including China – have now adopted laws based on the GDPR, the G20's Osaka Track was established, and the G7 reinforced its support to the principle of 'data free flow with trust', as well as ongoing scrutiny and guidance by data protection authorities worldwide.

In bilateral discussions, the negotiations on the enhanced Privacy Shield added complexity to the Trade and Technology Council (TTC) negotiations. While Working Group 5 of the TTC on data governance and technology platforms is tasked to 'exchange information on our respective approaches to data governance and technology platform governance, seeking consistency and interoperability where feasible', negotiations related to personal data transfers were explicitly excluded from the TTC agenda and run in parallel.

According to Politico, EU and US officials are **hopeful that an agreement on the new enhanced Privacy Shield will be reached by the end of 2021**. This should include creating legal oversight of US intelligence agencies by independent judges who could rule on whether data collection of the personal data of EU citizens is lawful and proportionate. It remains to be seen how much stamina Max Schrems still has to challenge these arrangements and whether this new mechanism will face and withhold the scrutiny of the CJEU.

On the global level, a new cloud on the horizon is **the new Chinese Private Information Protection Act,** which has extraterritorial effects. It will **inevitably bring to light the same issues of personal data protection of the EU citizens** as currently discussed with the USA. In addition, China is starting to call for a legal system that creates and defines data property rights, thus allowing data to be traded. China's debate around public ownership of data also indicates that the government is willing to go well beyond limited data collection to obtain data from individuals and companies that can be used without much restriction in 'public interest', as well as exert control over what personal data is exported.

The work of the data protection agencies on establishing global principles for personal data transfers is also noteworthy. The Global Privacy Assembly, a platform of more than 130 data protection and privacy authorities worldwide, has just issued its Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes, thus shaping global discourse from the position of enforcement.



The international counter-ransomware initiative

Ministers and representatives of 31 countries and the EU gathered virtually to discuss accelerating international cooperation to counter ransomware.

The first meeting of the Counter-Ransomware Coalition Initiative was hosted by the White House on 13–14 October, after its announcement during President Joe Biden's statement on cybersecurity awareness month. Happening less than 2 weeks after the announcement shows either impressive enthusiasm from allies and partners or long-laid groundwork for the summit, in which case it is the lack of foreshadowing whispers and rumours about the initiative that is impressive.

What was discussed?

The agenda was disclosed on the first day of the meeting by a senior official of the Biden administration. The discussions were divided into four broad topics: network resilience, countering illicit finance, disruption and other law enforcement efforts, and diplomatic engagement. These discussions were chaired by India, the UK, Australia, and Germany, respectively.

What are the outcomes?

The emphatic takeaway was that 'it takes a network to fight a network': A network of countries needs to connect elements across diplomacy, law enforcement, financial regulators, and infrastructure – first nationally and then globally – to be able to fight ransomware networks successfully.

The participants agreed on complementary efforts to reduce the risk of ransomware.

How were the participants chosen?

According to Anne Neuberger, deputy assistant to the president and deputy national security advisor for cyber and emerging technology, the White House invited countries that **'have virtual currency exchanges in their countries, have a leading CERT, or who can really bring things to the fight in the first**

An overview of the networking efforts agreed upon at the summit

Resilience:
(a) Promoting basic cyber hygiene
(b) Incident information sharing between ransomware victims and law enforcement and cyber emergency response teams
(c) Sharing lessons learned and best practices for development of policies to address ransom payments
(d) Engaging with the private sector to promote incident info sharing
(e) Actively involving senior leaders in cybersecurity decision-making

Countering illicit finance:
(a) Ensuring national anti-money laundering frameworks prevent an environment in which malicious actors can find platforms to move illicit proceeds
(b) Enhancing national authorities' capacity to regulate, supervise, investigate, and take action against virtual asset exploitation
(c) Enhancing information sharing about ransomware-related information through cooperation with the virtual asset industry

Diplomatic engagement:
(a) Coordinating a response to states whenever they do not address the activities of cybercriminals to meaningfully reduce safe havens
(b) Coordinating capacity building by sharing approaches, available resources and programs, and ensuring capacity building complements other counter-ransomware efforts

Disruption and other law enforcement efforts:
(a) Countering cybercriminal activity emanating from within their own territory
(b) Exchanging information and providing requested assistance to combat ransomware activity targeting infrastructure and financial institutions
(c) Taking national action against actors responsible for ransomware targeting critical infrastructure

wave' and can 'determine where cooperation is working, where additional cooperation is needed'.

Who was not invited?

It was underlined that this is not solely a US initiative, but the country was the one to dole out invitations. Surprising no one, yet gaining quite some news coverage, **Russia did not receive an invitation**.

US officials explained multiple times over the days that followed the summit that the USA and Russia have been discussing ransomware in a bilateral format since the Biden-Putin Geneva summit in June. Russian officials have consistently stressed that the USA puts too much focus on ransomware in these bilateral talks and that other topics such as critical infrastructure and election interference should be covered as well.

The USA, on the other hand, might consider Russia an unreliable partner in countering ransomware: the Russian government did take 'some steps' on cybercrime data shared bilaterally by the USA, but follow-up actions are needed.

Read more about the US-Russian cyber discussions in the cyber detente monthly barometer, published on the 16th of every month.

But Russia is not precluded from any future events, and neither is any other country the USA did not invite this time.

The initiative's future

This summit, according to a White House senior official, was only the first of many; the USA plans to invite more countries to participate. However, it has been stated that the involvement of too many countries may not be conducive to getting practical results. It will be interesting to see at what point the USA will stop inviting new participants.

It is also interesting to note that 20 of the 31 participants are signatories and 8 others are observers to the Budapest Convention on Cybercrime. The outliers are India, Lithuania, South Korea, and the United Arab Emirates. This leads us to question whether this new initiative could translate into a common position or draft at the UN Cybercrime Ad Hoc Committee. This UN committee is tasked to draft a new cybercrime treaty, and it is uncertain how that will interplay with the Budapest Convention on Cybercrime.

The newest hype in tech: The metaverse

Once Facebook announced it will rebrand to reflect the company's new focus on building the metaverse, hype around this concept reached a new high. What is the metaverse and what are its challenges?

The original metaverse

The latest buzzword in the tech world has actually been around for almost 30 years. It originated in Neal Stephenson's 1992 dystopian novel *Snow Crash*. Here is how he described his protagonists' experience in the metaverse:

So Hiro's not actually here at all. He's in a computer-generated universe that his computer is drawing onto his goggles and pumping into his earphones.

Attributes of the metaverse

A popular essay on the metaverse by venture capitalist Matthew Ball identifies its core attributes. The metaverse will be:

- Persistent – it will continue indefinitely
- Synchronous and live
- Without any cap to concurrent users – everyone can be a part of the metaverse at the same time
- A fully functioning economy – users will be able to create, own, invest, sell, and be rewarded for work
- An experience that spans both the digital and physical worlds, private and public networks/experiences, and open and closed platforms
- A place with unprecedented interoperability of data, digital items and assets, and content
- Populated by content and experiences created and operated by a wide range of contributors

Leading companies' vision of the metaverse

Facebook CEO Mark Zuckerberg called the metaverse 'a persistent, synchronous environment where we can be together'. Nvidia CEO Jensen Huang described it as 'a virtual world that is shared by a lot of people. It has real design. It has a real economy. You have a real avatar. That avatar belongs to you and is you. It could be a photoreal avatar of you, or a character.' Epic Games CEO Tim Sweeney characterised it as 'a kind of online playground where users could join friends to play a multiplayer game like Epic's Fortnite one moment, watch a movie via Netflix the next.' For Roblox, the metaverse is 'a platform for immersive co-experiences, where people can come together within millions of 3D experiences to learn, work, play, create, and socialise.' For Microsoft, the metaverse is a convergence of physical and digital worlds.

If you are still having trouble wrapping your brain around it, here is an example from popular culture you could use as a frame of reference: the Matrix.

The challenges

The main technological challenges will be interoperability and standards. Companies will have to adhere to a common set of standards to make their metaverses interoperable. Facebook and Epic Games already spoke out in favour of this.

The main issue around content creation may be intellectual property. In some jurisdictions (e.g. the USA, the UK) intellectual property rights cannot be awarded to AI, as AI-created works lack the element of human intervention. If an avatar creates something in the metaverse, will it be attributed to the person the avatar is representing?

The metaverse will also have many privacy and security issues because users' biometric and location data, as well as banking information, will be available to the metaverse provider(s).

Perhaps the biggest issues are about our condition as human beings. Whom do we trust to run and govern the metaverse – is it tech companies, or do we expect countries to have digital twins of their governance structures in the metaverse? Will we be able to trust that someone's avatar was not hacked before we interact with them? Can we be sure they are, in fact, human? How will we prove our own identity to others?

Food for thought

Will we get lost in the metaverse? Stephenson's characters went to the metaverse to escape their dystopian world; will we do the same? Could the metaverse become the real-life version of Robert Nozick's experience machine, where we choose pleasure in the virtual world over the challenges of life in the physical world?

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.

Digitalisation powering environmental protection 14 October 2021

The discussion was part of the 'Reflections on Digital Future' event series discussing how we can shape our digital future while ensuring human rights are adhered to and championed. This event considered the impact of new technologies for environmental protection and climate action. For example, AI can strengthen climate predictions, enable smarter decision-making for decarbonising industries, and anticipate the effects of extreme weather. Panellists asked how can we truly benefit from the technology's environmental solutions and use the digital revolution to advance environmental stewardship? How can we appropriately harness digital opportunities while limiting the adverse effects of digitalisation on the environment? How can we build strong partnerships among regions to support a digital transition that powers environmental protection across the globe?

The series is organised by the EU Delegation to the UN in Geneva, the Permanent Mission of Switzerland to the UN in Geneva, the Permanent Mission of Slovenia to the UN in Geneva (currently holding the Presidency of the Council of the EU), and GIP, in partnership with the International Research Centre for Artificial Intelligence.

Digital trust 2025 15 October 2021

Panellists addressed how the lack of digital trust manifests itself today and whether this lack of trust is justified or exaggerated. The discussion also considered which lessons can be learned from other sectors on how to build the necessary trust for our digital future. The conference was organised by the Graduate Institute's Centre for Trade and Economic Integration and EPFL's Centre for Digital Trust.

Legal and Governance tour | 12 Tours to Navigate Digital Geneva 28 October 2021

The event discussed the invisible thread that unites the digital ecosystem: digital governance. Panellists unpacked current developments regarding the UN envoy on technology, the future of the Internet Governance Forum, AI governance, and other processes that gravitate around Geneva.

What to watch for: Upcoming global policy events

Let's look ahead at the global digital policy calendar. Here's what will take place next month around the globe. For even more events, visit the Events section on the *Digital Watch* observatory.

November

11–12 NOVEMBER, 2nd GPAI Summit (Paris, France)

The second annual summit of the Global Partnership on AI (GPAI) showcases results from the ten working group studies, and lays the foundation for developing responsible AI and adopting trustworthy AI.

22–24 NOVEMBER, African Internet Governance Forum (online)

The 10th meeting of the African Internet Governance Forum (AfIGF) will be held on 22–24 November. The AfIGF gathers stakeholders from across the continent, such as ministers, policy and regulatory heads, civil society, industry, and others.

23–25 NOVEMBER, EU Open Data Days: Shaping our future with open data (online)

The first-ever EU Open Data Days will take place online on 23–25 November under the auspices of the Publications Office of the EU. The event looks to exhibit data visualisation for the EU public sector, when nine teams from across Europe and beyond will compete in a Datathon by working on innovative, open data-based applications.

29 NOVEMBER–1 DECEMBER, UN Forum on Business and Human Rights (online)

The UN Guiding Principles on Business and Human Rights marks its 10th anniversary this year, which will form the central theme of the 2021 Forum. This milestone provides an opportunity to look back at progress and challenges to date and, more importantly, to inspire a renewed push for scaled-up global implementation by states and businesses in the decade ahead. This year's theme is 'The next decade of business and human rights: Increasing the pace and scale of action to implement the Guiding Principles on Business and Human Rights'.

29 NOVEMBER–3 DECEMBER, European Big Data Value Forum (online and Ljubljana, Slovenia)

Being an associated Slovenian EU Presidency event, the first day of the European Big Data Value Forum (EBDVF) 2021 is hosted in Ljubljana. The rest of the EBDVF will be organised fully online, with multiple sessions, workshops, tutorials, and non-commercial speeches. This year's theme is 'Digital Transformation powered by Data and AI'.

30 NOVEMBER–2 DECEMBER, GFCE Annual Meeting 2021 (online)

The Global Forum on Cyber Expertise (GFCE) will convene its annual meeting on 30 November–2 December and gather more than 140 members and partners from all regions of the world, aiming to strengthen cyber capacity and expertise globally.

30 NOVEMBER–3 DECEMBER, WTO 12th (Geneva, Switzerland) (online)

The WTO Ministerial Conference, attended by trade ministers and other senior officials from the organisation's 164 members, is the highest decision-making body of the WTO. It will be co-hosted by Kazakhstan and chaired by Kazakhstan's Minister of Trade and Integration, Bakhyt Sultanov.

December

About this issue

Issue 64 of the *Digital Watch* newsletter, published on 3 November 2021 by the Geneva Internet Platform and DiploFoundation | Contributors: Andrijana Gavrilović, Pavlina Ittelson, Marco Lotti, Jana Mišić | Editing and design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić | Get in touch: digitalwatch@diplomacy.edu

On the cover

Facebook facing faces. Credit: Vladimir Veljasević

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