



## Shaping the global AI landscape

*Pages 4–5*

### **DIGITAL POLICY SNAPSHOT**

AI governance, content policy, and digital rights dominated headlines in October.

*Pages 2-3*

### **MISINFORMATION IN THE MIDDLE EAST**

Misinformation about the conflict threatens to crowd out the truth. What are tech companies doing to counter it?

*Page 6*

### **IGF 2023**

IGF 2023 discussions presented through ten questions our team derived from hundreds of sessions.

*Page 7*

### **UPCOMING: UNCTAD eWEEK 2023**

Participants will gather in December to discuss how to shape the future of the digital economy.

*Page 8*

## Snapshot: What's making waves in digital policy?

### Geopolitics

The US Department of Commerce (DoC) Bureau of Industry and Security (BIS) announced a [tightening of export restrictions](#) on advanced semiconductors to China and other nations subject to arms embargoes. This decision [has elicited a strong reaction](#) from China, labelling the measures as 'unilateral bullying' and an abuse of export control mechanisms.

Further complicating the US-China tech landscape, there are discussions within the US government about imposing restrictions on Chinese companies' access to cloud services. If implemented, this move could have significant consequences for both nations, particularly impacting major players like Amazon Web Services and Microsoft. Finally, Canada [has banned Chinese and Russian](#) software from devices issued by the government, citing security concerns.

### AI governance

In other developments, a [leaked draft text](#) suggests that Southeast Asian countries, under the umbrella of the Association of Southeast Asian Nations (ASEAN), are adopting a business-friendly approach to AI regulation. The draft guide to AI ethics and governance asks companies to consider cultural differences and doesn't prescribe categories of unacceptable risk. Meanwhile, [Germany has introduced an AI action plan](#) intending to increase AI advancement on national and European scales, to compete with the predominant AI forces of the USA and China.

Read more on AI governance on pages 4-5.

### Security

The heads of security agencies from the USA, the UK, Australia, Canada, and New Zealand, collectively known as the Five Eyes, [have publicly cautioned](#) about China's widespread espionage campaign to steal commercial secrets. The European Commission has [announced](#) a comprehensive review of security risks in vital technology domains, including

semiconductors, AI, quantum technologies, and biotechnologies. ChatGPT faced outages on 8 November, [believed to be a result](#) of a distributed denial-of-service (DDoS) attack. Hacktivist group Anonymous Sudan [claimed responsibility](#). Finally, Microsoft's latest [Digital Defense Report](#) revealed a global increase in cyberattacks, with government-sponsored spying and influence operations on the rise.

### Infrastructure

The US Federal Communications Commission (FCC) [voted to initiate the process](#) of restoring net neutrality rules. Initially adopted in 2015, these rules were repealed under the previous administration but are now poised for reinstatement.

Access Now, the Internet Society, and 22 other organisations and experts [have jointly sent a letter to the Telecom Regulatory Authority of India \(TRAI\) opposing the enforcement of discriminatory network costs or licensing regimes for online platforms](#).

### Internet economy

Alphabet's Google [reportedly](#) paid a substantial sum of USD 26.3 billion to other companies in 2021 to ensure its search engine remained the default on web browsers and mobile phones. This was revealed during the US Department of Justice's (DoJ) antitrust trial. For similar anticompetitive actions, the Japan Fair Trade Commission (JFTC) has opened an [antimonopoly](#) investigation into Google's web search dominance.

The European Central Bank (ECB) [has decided to commence a two-year preparation phase](#) starting 1 November 2023, to finalise regulations and select private-sector partners before the possible launch of a digital version of the euro. The next step will be the possible implementation after a green light from policymakers. In parallel, the European Data Protection Board (EDPB) [has called for enhanced privacy safeguards](#) in the European Commission's proposed digital euro legislation.

## Digital rights

The council presidency and the European Parliament have reached a [provisional agreement on a new framework for a European digital identity \(eID\) to provide all Europeans](#) with a trusted and secure digital identity. Under the new agreement, member states will provide citizens and businesses with digital wallets that link their national digital identities with other personal attributes, such as driver's licences and diplomas.

The European Parliament's Internal Market and Consumer Protection Committee [has passed a report](#) warning of the addictive nature of certain digital services, advocating tighter regulations to combat addictive design in digital platforms. On a similar note, the [European data regulator has ordered the Irish data regulator](#) to impose a permanent ban on Meta's behavioural advertising across Facebook and Instagram.

Key political groups in the European Parliament [have reached a consensus](#) on draft legislation compelling internet platforms to detect and report child sexual abuse material (CSAM) to prevent its dissemination on the internet.

## Content policy

Meta, the parent company of Facebook and Instagram, [is confronting a legal battle](#) initiated by over 30 US states. The lawsuit claims that Meta intentionally and knowingly used addictive features while concealing the potential risks of social media use, violating consumer protection laws, and breaching privacy regulations concerning children under 13.

The EU [has formally requested](#) details on anti-disinformation measures from Meta and TikTok. Against the backdrop of the Middle East conflict, the EU emphasises the risks associated with the widespread dissemination of illegal content and disinformation.

The [UK's Online Safety Act](#), imposing new responsibilities on social media companies, has come into effect. This law aims to enhance online safety and holds social media platforms accountable for their content moderation practices.

## Development

The Gaza Strip has faced three internet blackouts [since the start of the conflict](#), prompting Elon Musk's SpaceX's Starlink to [offer internet access](#) to internationally recognised aid organisations in Gaza. Meanwhile, environmental NGOs [are urging](#) the EU to take action on electronic waste, calling for a revision of the Waste Electrical and Electronic Equipment Directive (WEEE Directive), per the European Environmental Bureau's communication.

## THE TALK OF THE TOWN – GENEVA

As agreed during the regular session of the [ITU Council](#) in July 2023, [an additional session](#) dedicated to confirming logistical issues and organisational planning for 2024–2026 was held in October 2023. It was preceded by the cluster of [Council Working Group \(CWG\) and Expert Group \(EG\) meetings](#) where the list of chairs and vice-chairs were appointed until the 2026 Plenipotentiary Conference. The next cluster of CWG and EG meetings will take place from 24 January to 2 February 2024.

The [3rd Geneva Science and Diplomacy Anticipator \(GESDA\) Summit](#) saw the launch of the [Open Quantum Institute \(OQI\)](#), a partnership among the Swiss Federal Department of Foreign Affairs (FDFA), CERN and UBS. The OQI aims to make high-performance quantum computers accessible to all users devoted to finding solutions for and accelerating progress in attaining sustainable development goals (SDGs). The OQI will be hosted at CERN beginning in March 2024 and facilitate the exploration of the technology's use cases in health, energy, climate protection, and more.

## Shaping the global AI landscape

Month in, month out, we spent most of 2023 reading and writing about AI governance. October is no exception. As the world grapples with the complexities of this technology, the following initiatives showcase efforts to navigate its ethical, safety, and regulatory challenges on both national and international fronts.

***Biden's executive order on AI.*** The [order](#) represents the most substantial effort by the US government to regulate AI to date. Unveiled with anticipation, the order provides actionable directives where possible and calls for bipartisan legislation where necessary, particularly in data privacy.

One standout feature is the emphasis on AI safety and security. Developers of the most potent AI systems are now mandated to share safety test results and critical information with the US government. Additionally, AI systems utilised in critical infrastructure sectors are subjected to rigorous safety standards, reflecting a proactive approach to mitigating potential risks associated with AI deployment.

Unlike some emerging AI laws, such as the EU's AI Act, Biden's order takes a sectoral approach. It directs specific federal agencies to focus on AI applications within their domains. For instance, the Department of Health and Human Services is tasked with advancing responsible AI use in healthcare, while the DoC is directed to develop guidelines for content authentication and watermarking to label AI-generated content clearly. The DoJ is instructed to address algorithmic discrimination, showcasing a nuanced and tailored approach to AI governance.

Beyond regulations, the executive order aims to bolster the US's technological edge. It facilitates the entry of highly skilled workers into the country, recognising their pivotal role in advancing AI capabilities. The order also prioritises AI research through funding initiatives, increased access to AI resources and data, and the establishment of new research structures.

***G7's guiding principles.*** Simultaneously, the G7 nations released their [guiding principles for advanced AI](#), accompanied by a detailed code of conduct for organisations developing AI.



Image credit: Politico

These principles, totalling 11, centre around risk-based responsibility. The G7 encourages developers to implement reliable content authentication mechanisms, signalling a commitment to ensuring transparency in AI-generated content.

A notable similarity with the EU's AI Act is the risk-based approach, placing responsibility on AI developers to assess and manage the risks associated with their systems. The EU promptly welcomed these principles, citing their potential to complement the legally binding rules under the EU AI Act internationally.

While building on the existing Organisation for Economic Co-operation and Development AI Principles (OECD) [principles](#), the G7 principles go a step further in certain aspects. They encourage developers to deploy reliable content authentication and provenance mechanisms, such as watermarking, to enable users to identify AI-generated content. However, the G7's approach preserves a degree of flexibility, allowing jurisdictions to adopt the code in ways that align with their individual approaches.

Differing viewpoints on AI regulation among G7 countries are acknowledged, ranging from strict enforcement to more innovation-friendly guidelines. However, some provisions, such as

those related to privacy and copyright, are criticised for their vagueness, raising questions about their potential to drive tangible change.

**China's Global AI Governance Initiative (GAIGI).** China [unveiled its GAIGI during the Third Belt and Road Forum](#), marking a significant stride in shaping the trajectory of AI on a global scale. China's GAIGI is expected to bring together 155 countries participating in the Belt and Road Initiative, establishing one of the largest global AI governance forums.

This strategic initiative [focuses on five aspects](#), including ensuring AI development aligns with human progress, promoting mutual benefit, and opposing ideological divisions. It also establishes a testing and assessment system to evaluate and mitigate AI-related risks, similar to the risk-based approach of the EU's upcoming AI Act. Additionally, the GAIGI supports consensus-based frameworks and provides vital support to developing nations in building their AI capacities.

China's proactive approach to regulating its homegrown AI industry has granted it a first-mover advantage. Despite its deeply ideological approach, China's interim measures on generative AI, effective since August this year, were a world first. This advantage positions China as a significant influencer in shaping global standards for AI regulation.

**AI Safety Summit at Bletchley Park.** The [UK's much-anticipated summit](#) resulted in a landmark commitment among leading AI countries and companies to test frontier AI models before public release.

The [Bletchley Declaration](#) identifies the dangers of current AI, including bias, threats to privacy, and deceptive content generation. While addressing these immediate concerns, the focus shifted to frontier AI – advanced models that exceed current capabilities – and their potential for serious harm. Signatories include Australia, Canada, China, France, Germany, India, Korea, Singapore, the UK, and the USA for a total of 28 countries plus the EU.

Governments will now play a more active role in testing AI models. [The AI Safety Institute](#), a new global hub established in the UK, will collaborate with leading AI institutions to assess the safety of emerging AI technologies before and after their public release. This marks a significant departure from the traditional model, where AI companies were solely responsible for ensuring the safety of their models.

The summit resulted in an agreement to form an international advisory panel on AI risk, inspired by [the Intergovernmental Panel on Climate Change \(IPCC\)](#). Each signatory country will nominate a representative to support a larger group of leading AI academics, producing State of the Science reports. This collaborative approach aims to foster international consensus on AI risk.

**UN's High-Level Advisory Body on AI.** The UN has taken a unique approach by [launching a High-Level Advisory Body on AI](#), comprising 39 members. Led by UN Tech Envoy Amandeep Singh Gill, the body will publish its first recommendations by the end of this year, with final recommendations expected next year. These recommendations will be discussed during the UN's Summit of the Future in September 2024.

Unlike previous initiatives that introduced new principles, the UN's advisory body focuses on assessing existing governance initiatives worldwide, identifying gaps, and proposing solutions. The tech envoy envisions the UN as the platform for governments to discuss and refine AI governance frameworks.

**OECD's updated AI definition.** The OECD [has officially revised its definition of AI](#), to read: *An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that [can] influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.* It is anticipated that this definition will be incorporated into the EU's upcoming AI regulation.

## Misinformation crowding out the truth in the Middle East

It is said that a lie can travel halfway around the world while the truth is still putting on its shoes. It is also said it was Mark Twain who coined it – which, ironically, is [untrue](#).

Misinformation is as old as humanity and decades old in its current recognisable form, but social media has amplified its speed and scale. An MIT report from 2018 found that [lies spread six times faster than the truth](#) – on Twitter, that is. Different platforms amplify misinformation differently – depending on [how many mechanisms for the virality](#) of posts the platform has in place.

Yet all social media platforms have struggled with misinformation in recent days, as people have been grappling with the violence unfolding in Israel and Gaza, social media platforms have become inundated with graphic images and videos of the conflict – and images and videos that have nothing to do with it.

**What's happening?** Miscalcaptioned imagery, altered documents, and old videos taken out of context are circulating online. This makes it hard for anyone looking for information about the conflict to parse falsehood from truth.



**Shaping perceptions.** Misleading claims are not confined to the conflict zone; they also impact global perceptions and contribute to the polarisation of opinions. Individuals, influenced by biases and emotions, take sides based on information that often lacks accuracy or context.

False narratives on platforms like X (formerly known as Twitter) can influence political agendas, with instances of fake memos circulating about military aid and allegations of fund transfers. Even supposedly reliable verified accounts contribute significantly to the dissemination of misinformation.

**What tech companies are doing.** Meta has [established](#) a special operations centre staffed with experts, including fluent Hebrew and Arabic speakers. It is working with fact-checkers, using their ratings to downrank false content in the feed to reduce its visibility. TikTok's measures are somewhat similar. The company [established](#) a command centre for its safety team, added moderators proficient in Arabic and Hebrew, and enhanced automated detection systems. X [removed](#) hundreds of Hamas-linked accounts and removed or flagged thousands of pieces of content. Google and Apple reportedly [disabled](#) live traffic data for online maps for Israel and Gaza. Social messaging platform Telegram [blocked](#) Hamas channels on Android due to violations of Google's app store guidelines.

**The EU reacts.** The EU ordered [X](#), [Alphabet](#), [Meta](#), and [TikTok](#) to remove fake content. European Commissioner Thierry Breton reminded them of their obligations under the new Digital Services Act (DSA), giving X, Meta, and TikTok 24 hours to respond. X confirmed removing Hamas-linked accounts, but the EU sent a [formal request for information](#), marking the beginning of an [investigation into compliance with the DSA](#).

**Complicating matters.** However, earlier this year, Meta, Amazon, Alphabet, and Twitter laid off many team members [focusing on misinformation](#). This was part of a post-COVID-19-induced restructuring aimed at improving financial efficiency.

The situation underscores the need for robust measures, including effective fact-checking, regulatory oversight, and platform accountability, to mitigate the impact of misinformation on public perception and global discourse.

## IGF 2023

The Internet Governance Forum (IGF) 2023 addressed pressing issues amid global tensions, including the Middle East conflict. With a record-breaking 300 sessions, 15 days of video content, and 1,240 speakers, debates covered topics from the Global Digital Compact (GDC) and AI policy to data governance and narrowing the digital divide.



The following ten questions are derived from [detailed reports from hundreds of workshops and sessions at the IGF 2023](#).

**1. How can AI be governed?** Sessions explored national and international AI governance options, emphasising transparency and questioning the regulation of AI applications or capabilities.

**2. What will be the future of the IGF in the context of the Global Digital Compact (GDC) and the WSIS+20 Review Process?** The future of the IGF is closely tied to the GDC and the WSIS+20 Review Process. The 2025 review may decide the IGF's fate, and negotiations on the GDC, expected in 2024, will also impact the IGF's trajectory.

**3. How can we use the IGF's wealth of data for an AI-supported, human-centred future?** The IGF's 18 years of data is considered a public good. Discussions explored using AI to gain insights, enhance multistakeholder participation, and visually represent discussions through knowledge graphs.

**4. How can risks of internet fragmentation be mitigated?** Multidimensional approaches and inclusive dialogue were proposed to prevent unintended consequences.

**5. What challenges arise from the negotiations on the UN treaty on cybercrime?** Concerns were raised about the scope, human rights safeguards, undefined cybercrime definitions,

and the role of the private sector in the UN treaty on cybercrime negotiations. Clarity, separation of cyber-dependent and cyber-enabled crimes, and international cooperation were emphasised.

**6. Will the new global tax rules be as effective as everyone hopes for?** The IGF discussed the potential effectiveness of the OECD/G20's two-pillar solution for global tax rules. Concerns lingered about profit-shifting, tax havens, and power imbalances between Global North and South nations.

**7. How can misinformation and protection of digital communication be addressed during times of war?** Collaborative efforts between humanitarian organisations, tech companies, and international bodies were deemed essential.

**8. How can data governance be strengthened?** The discussion emphasised the importance of organised and transparent data governance, including clear standards, an enabling environment, and public-private partnerships. The Data Free Flow with Trust (DFFT) concept, introduced by Japan, was discussed as a framework to facilitate global data flows while ensuring security and privacy.

**9. How can the digital divide be bridged?** The digital divide requires comprehensive strategies beyond connectivity involving regional initiatives, deploying LEO satellites, and digital literacy efforts. Public-private partnerships, especially with RIRs, were highlighted as crucial for fostering trust and collaboration.

**10. How do digital technologies impact the environment?** The IGF explored the environmental impact of digital technologies, highlighting the potential to cut emissions by 20% by 2050. Immediate actions, collaborative efforts, awareness campaigns, and sustainable policies were advocated to minimise the environmental footprint of digitalisation.

Read more in our [IGF 2023 Final report](#).

## Upcoming: UNCTAD eWeek 2023

Organised by the UN Conference on Trade and Development (UNCTAD) in collaboration with [eTrade for all](#) partners, the [UNCTAD eWeek 2023](#) is scheduled from 4 to 8 December at the prestigious International Conference Center Geneva (CICG). The central theme of this transformative event is 'Shaping the future of the digital economy'.

Ministers, senior government officials, CEOs, international organisations, academia, and civil society will convene to address pivotal questions about the future of the digital economy: What does the future we want for the digital economy look like? What is required to make that future come true? How can digital partnerships and enhanced cooperation contribute to more inclusive and sustainable outcomes?

Over the week, participants will join more than 150 sessions addressing themes including platform governance, the impact of AI on the digital economy, eco-friendly digital practices, the empowerment of women through digital entrepreneurship, and the acceleration of digital readiness in developing countries.

The event will explore key policy areas for building inclusive and sustainable digitalisation at various levels, focusing on innovation, scalable good practices, concrete actions and actionable steps.

For youth aged 15–24, there's a dedicated online consultation to ensure their voices are heard in shaping the digital future for all.

### GIP just-in-time reporting and Diplo's sessions at UNCTAD



The GIP will be actively involved in eWeek 2023 by providing reports from the event. Our human experts will be joined by DiploAI, which will generate reports from all eWeek sessions. Bookmark our [dedicated eWeek 2023 page on the Digital Watch Observatory](#) or download the app to follow the reports.

Diplo, the organisation behind the GIP, will also co-organise a session entitled 'Scenario of the Future with the Youth' with UNCTAD and Friedrich-Ebert-Stiftung (FES), and a

session entitled 'Digital Economy Agreements and the Future of Digital Trade Rulemaking' with CUTS International. Diplo's session will be titled 'Bottom-up AI and the Right to be Humanly Imperfect.' For more details, visit our [Diplo @ UNCTAD eWeek page](#).

**About this issue:** Issue 84 of the Digital Watch monthly newsletter, published on 11 November 2023 by the Geneva Internet Platform and DiploFoundation. For more coverage and analysis, visit the [Digital Watch observatory](#)

**Team:** Andrijana Gavrilović (author), Boris Begović (contributor), Yung-Hsuan Wu (contributor), Ginger Paque (editor), Diplo's CreativeLab (design) | Get in touch: [digitalwatch@diplomacy.edu](mailto:digitalwatch@diplomacy.edu)

**On the cover:** *Shaping the global AI landscape*. Credit: Vladimir Veljasević DiploFoundation (2023) <https://creativecommons.org/licenses/by-nc-nd/4.0/>

The Geneva Internet Platform is an initiative of:

