

Geneva Internet Platform


Digital Watch
NEWSLETTER

You receive hundreds of pieces of information on digital policy.
We receive them, too.
We decode, contextualise, and analyse them.
Then we summarise them for you.

DIGITAL POLICY TRENDS IN APRIL

1. RENEWED DISCUSSIONS ON STATE BEHAVIOUR IN CYBERSPACE

This month, Microsoft's Brad Smith announced three new documents that continue to shape the proposal for a Geneva Digital Convention. The first carries key clauses which should form part of the convention; the second outlines a common set of principles and behaviours for the tech sector to help protect civilians in cyberspace; the third proposes the setting up of an independent attribution organisation to identify wrongdoing.

To a limited extent, the key clauses build on the 2015 report of the UN Group of Governmental Experts (GGE); the clauses however go beyond the explicitly mentioned report, to include provisions on backdoors, cyber weapons, and cyber offensive operations. *More on page 6.*

The proposal for an attribution organisation addresses the thorny issue of identifying and proving who is behind an attack, based on sound technical evidence. Accountability must follow attribution, the proposal indicates – assuming that it is indeed possible to attribute attacks even in the case of proxies.

Many open questions remain, such as: How can the convention be implemented? How – and by whom – can the provisions be enforced? Given that the three documents were

published within a short timespan from the first proposal, there is little doubt that Microsoft will continue to add flesh to the proposal in the coming weeks.

Meanwhile, the G7 Foreign Ministers' Communiqué clearly recognises the threat of the use of ICT tools against critical infrastructure and the increased concern over cyber-enabled interference in democratic processes – potentially referring to the alleged Russian interference in the US presidential election last November. It supports the work of the UN GGE, but also specifically invites states 'to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible'.

Their Declaration on Responsible States' Behaviour in Cyberspace notes that when attributing an internationally wrongful act to another state, or when taking action in response, a state 'is free to make its own determination in accordance with international law with respect to attribution of a cyber-act to another State'.

2. NET NEUTRALITY DEBATES CONTINUE

Net neutrality proponents continue to follow the debates in the USA, as the Federal Communications Commission (FCC) chair and Internet companies battle whether to keep or replace the FCC rules in favour of net neutrality.

Continued on page 3

CELEBRATING ISSUE 20

We celebrate the 20th issue of the newsletter this month. In acknowledgement, flip to the end for a special supplement. We have selected two posters related to digital policy, which we invite you to download, print, and use.



IN THIS ISSUE

OBSERVATORY



Key issues such as security, e-commerce, and net neutrality remained prominent this month; others were less so. We round up the main global developments in April.

More on pages 4–5

PRIVACY SHIELD



Several concerns were flagged by the European Parliament (EP) this month. We take a look at the EP's resolution.

More on page 6

E-COMMERCE



UNCTAD's E-commerce Week featured many discussions on e-commerce and trade, digital rights, inclusive development, data flows, and cybercrime and cybersecurity.

More on page 7

NEWSLETTER



To mark the 20th issue, we look at what goes into preparing our monthly newsletter.

More on page 8

Issue no. 20 of the *Geneva Digital Watch* newsletter, published on 30 April 2017, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Stephanie Borg Psaila, Dane Burkholder, Jovan Kurbalija, Marissa Lopresti, Marco Lotti, Marília Maciel, Aida Mahmutović, Roxana Radu, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatović, Diplo's CreativeLab | The Brazilian version in Portuguese is available at <http://dig.watch/newsletter> | In addition to the newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (<http://dig.watch>) and join discussions on the last Tuesday of every month online, at local hubs, or at the GIP (<http://dig.watch/briefings>) | Send your comments to digitalwatch@diplomacy.edu

Knowledge for Development: Global Partnership Conference 2017

The conference, held on 3-4 April, [jointly organised by the Joint Inspection Unit \(JIU\) of the United Nations system and Knowledge Management Austria \(KMA\)](#), reviewed and advanced knowledge management practices in the field of sustainable development. At the conference, the JIU launched its 2016 report *Knowledge Management in the United Nations System*, [which highlighted best practices and recommendations for implementing knowledge management strategies within the UN](#), while the KMA initiated the *Agenda Knowledge for Development* [to provide a platform for stakeholders to share knowledge management experiences](#). The event comprised six panel sessions and two interactive discussions about the benefits and limitations of knowledge management in achieving the UN Sustainable Development Goal 17 (Strengthen the means of implementation and revitalize the global partnership for sustainable development) and Agenda 2030 for Sustainable Development. *Curators of the GIP Digital Watch Observatory reported from the event. [Read the reports.](#)*

UNECE Initiative for Gender-Responsive Standards: First Meeting

The initiative, launched by the UN Economic Commission for Europe (UNECE), dedicated its first meeting [to gaining a better understanding of the need for technical standards, including digital standards, to be looked at from a gender perspective](#). Participants exchanged experiences around standards and gender equality initiatives, focusing on the challenges and opportunities to integrate gender issues into standards work. There were also discussions on how standards could contribute to achieving SDG 5 (Achieve gender equality and empower all women and girls). Moreover, members of the initiative debated the work plan for the group, and discussed possible actions that could be launched in the upcoming period and related deliverables. The Initiative for Gender-Responsive Standards was created by UNECE with the overall goals of challenging the perception that standards and technical regulations are 'gender neutral' and enhancing the contribution of standards in reaching SDG 5.

The Future of Work we want: A Global Dialogue

The dialogue, organised on 6-7 April, [under the framework of the International Labour Organization \(ILO\) Future of Work Centenary Initiative](#), provided a space for discussions on the developments and changes in the nature of work (as triggered by ongoing technological advancements), as well as possible approaches for effective policies to shape the future of work. The conference offered participants the opportunity to debate and provide perspectives on the drivers of change in the work environment, as well as on the need for innovation in the governance of work. Some of the specific topics tackled were the impact that the transformations in the world of work have on how individuals interact; the interplay of technological innovations, structural transformation, economic development, and social challenges and its impact on the future of work; challenges and opportunities faced by young people in the new world of work; and the organisation of work and production in the context of the fourth Industrial Revolution. *Curators of the GIP Digital Watch Observatory reported from the event. [Read the reports.](#)*

UNCTAD E-Commerce Week 2017

E-Commerce Week, 24-28 April, [was organised by the UN Conference on Trade and Development \(UNCTAD\) under the overarching theme 'Towards inclusive e-commerce'](#). The event featured sessions dealing with issues such as e-commerce and trade, cybersecurity and cybercrime, digital rights, consumer protection, inclusive development, and data flows. Entities involved in the organisation of these sessions included the Ali Research Institute, the International Telecommunication Union (ITU), the International Trade Centre (ITC), the Internet Society, the World Trade Organization (WTO), the Organisation for Economic Co-operation and Development (OECD), and the World Bank Group. The inter-linkages between e-commerce, digital trade, and other digital policy issues were explored in the multistakeholder discussions, while a High-level Event on Digital Transformation for all: Empowering Entrepreneurs and Small Businesses focused on how innovative digital technologies and e-commerce solutions could contribute to sustainable development. *More on page 7.*

Briefing for Heads of Mission: Digital Policy in Latin America and the Caribbean

The briefing [was held on 25 April at the Geneva Internet Platform, and was organised in partnership with the Permanent Mission of Paraguay to the United Nations in Geneva](#). The aim of the briefing was to assist Heads of Permanent Missions of GRULAC (Latin American and Caribbean Group) countries to navigate the digitalisation of agendas of the main international organisations and events hosted in Geneva. Discussions were held on how many of the traditional policy issues – such as trade, health, human rights, and labour – are influenced by digital developments, as well as on the inter-linkages among various digital issues addressed in International Geneva. An overview was also given of the ongoing policy processes, in the framework of the WTO, the ITU, and the Internet Governance Forum (IGF), among others, with particular attention paid to the links between digital policy in Geneva and regional/national developments in the GRULAC region.

DIGITAL POLICY TRENDS IN APRIL

Continued from page 1

At least two meetings were held with the new FCC chair. During the first meeting, the Internet Association – representing companies such as Facebook, Google, Twitter, and Microsoft – strongly defended the current rules. In the second meeting, media reports stated that Internet companies were in favour of finding common ground.

What could this indicate about future directions? There are several possibilities. If a recent proposal¹ from Chairman Ajit Pai is approved, the FCC will overturn the declaration of broadband as a utility-like service, which it established in 2015. As an information service, companies would have more freedom to establish tiered services, as the FCC would have limited ability to regulate Internet services in the case of another U-turn.

Changes in the FCC rules could also have a broader impact on zero-rating services. So far, the FCC has been tackling zero-rating services on a case-by-case basis. However, another U-turn would also mean that companies could have more freedom in offering zero-rating services to customers.

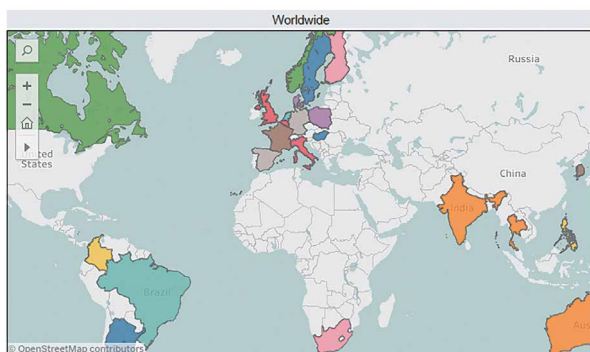
3. UBER FACES MORE LEGAL WOES

Ride-sharing applications such as Uber continue to pose legal and economic-related challenges due to their disruptive model. Uber has already faced numerous challenges in many jurisdictions:² this month, its legal woes continued.

Italian and UK authorities have criticised Uber's contracts with its drivers. A court in Rome ruled that drivers are employees, while the chair of the UK Work and Pensions parliamentary committee has called the contracts as 'gibberish'.

Of all the court cases involving Uber, two main issues are at stake. The first is related to classification: Is Uber a traditional taxi service, or a technology company? The answer to this question – currently tackled also by the Court of Justice of the European Union (CJEU) – may help resolve issues related to licensing and regulations.

The second is related to whether drivers are employees or independent contractors. If they are considered employees, the company would be obliged to abide by the employment rules of each jurisdiction. If they are considered independent contractors, serious concerns arise over the lack of protection of the labour force, including social security benefits which a normal employee would be entitled to. Uber is expected to appeal both the Rome ruling this month, and the UK ruling a few months ago, in which both authorities ruled that drivers are employees.



Uber has been involved in legal action over several issues, and in more than 25 countries. The interactive database – at [dig.watch/uber](#) – describes the relevant court cases and other rulings, and includes details such as the court or authority passing the ruling, dates, and status of the case.

4. THE WORK OF INTERMEDIARIES ON CONTENT POLICY INTENSIFIES

This month saw intermediaries intensify their work on content issues, including the development of new tools.

Microsoft's role as an important stakeholder in developing cyber-norms continued to take shape. After proposing a Digital Geneva Convention to tackle cyber-risks emanating from state actors, it launched three additional documents this month to further shape its proposed convention. It is currently in discussions with government officials, industry peers, and end-users over the proposal. We can expect the company to take even more proactive steps in the shaping of a potential convention soon.

Facebook announced³ the launch of new tools designed to combat the sharing of intimate images without permission, usually reported as 'revenge porn'. It is also reviewing its reporting flows as a reaction to a violent video posted by one of its users. This will add more pressure on Facebook to respond to user reports in a more expeditious way to determine whether content meets the grounds for removal.

Google has started to expand its fact-checking tools for Google Search and Google News to a global level.⁴ This is in response to mounting pressure on online platforms to curb the proliferation of violent extremism, hate speech, and fake news. Although the new feature will not directly address the use of Google's platforms to disseminate fake news, it will provide links to fact-checking organisations and information about their ranking of information as true, false, partly true, or partly false.

The pressure faced by intermediaries is leading companies to take on a stronger approach as de facto content arbiters.

5. ALARMING NEW TRENDS RELATED TO CHILD SEXUAL ABUSE MATERIAL (CSAM)

The Internet Watch Foundation (IWF) 2016 report⁵ has revealed new trends that show the perpetrators' increasing proficiency in masking online CSAM:

- Criminals are increasingly using masking techniques to hide child sexual abuse images and videos on the Internet and leaving clues to paedophiles so they can find it. The IWF saw an increase of 112% in this technique.
- Another growing trend is the use of new gTLDs to share CSAM. Many of these new gTLDs are dedicated to illegal imagery.
- While the majority of CSAM was hosted in North America in the past, now it is hosted in Europe (specifically, the Netherlands).

Despite the alarming trends, there are tools which help law enforcement authorities (LEAs) combat CSAM. Apart from active searching, the IWF and local authorities rely heavily on user reports, which are generally anonymous. In 2016 alone, the IWF processed over 100 000 reports.

Image hash lists, i.e., digital fingerprints of known imagery, are another effective tool, as these can help to quickly match and remove CSAM before it spreads online. Beyond CSAM, image hash lists represent an important achievement resulting from collaboration between the technical community, the industry, and LEAs. It will be interesting to see whether the model can be successfully replicated to combat other types of unwanted content.

DIGITAL POLICY: DEVELOPMENTS IN APRIL

Global IG architecture



increasing relevance

Microsoft has published three additional papers in support of a Digital Geneva Convention. *More on pages 1 and 6.*

The G7 Foreign Ministers' Joint Communiqué expressed support for the work of the UN GGE, but invited states 'to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible.' The Foreign Ministers' Declaration on Responsible States Behaviour in Cyberspace underlines that 'customary international law of state responsibility supplies the standards for attributing acts to States, which can also be applicable to activities in cyberspace'.

The G20 ministers responsible for the digital economy reiterated concerns brought about by digitalisation, and reaffirmed a commitment to the multistakeholder approach to Internet governance.

Sustainable development



same relevance

The World Bank has published an Atlas of Sustainable Development Goals (SDGs), containing maps and visualisations which show progress made by countries towards achieving the 17 SDGs. Included is statistical data covering issues such as the expansion of Internet access, and Internet use by men and women.

The President of the UN General Assembly convened a high-level event on financing for the SDGs, which looked at how countries can approach the financing of different SDGs. A call was made for stronger multistakeholder partnerships to ensure that financial resources are available for achieving the SDGs.

Security



increasing relevance

Cybersecurity and cyber issues were among the issues which China's and the US President discussed in April. A report released by China said that both sides should make use of high-level dialogue mechanisms - diplomacy and security; economy, law enforcement, and cybersecurity; and social and people-to-people exchanges.

Cybercrime syndicate Lazarus Group, thought to have been behind major incidents including the 2014 Sony hack and last year's \$81 million Bangladesh Central Bank heist, is described as 'one of the most successful in large scale operations against the financial industry' in Kaspersky Lab's new report.

There were at least two major cyber-attacks this month. Executives of some of the largest US companies were possible victims of cyber-espionage, after the US National Foreign Trade Council's website was hacked to include a malicious link, inviting board members to accept an infected calendar invite for a meeting. Hackers hit Amazon.com's third-party sellers, after bank-deposit information for sellers was maliciously changed.

E-commerce & Internet economy



increasing relevance

Uber continues to face legal woes. An Italian court has banned Uber over unfair competition. The chair of a UK parliamentary committee has criticised Uber, Deliveroo, Amazon, and Hermes over the 'unintelligible' self-employment contracts these companies are offering their contractors. Lawmakers in Brazil's lower house of Congress have approved a bill that would require local authorities to regulate ride-hailing services like Uber. In the USA, a federal judge in Seattle has temporarily blocked the application of a law allowing drivers of companies like Uber to unionise over pay and working conditions. Meanwhile, a Brazil court has ruled that Uber drivers are employees.

As of 1 April, Japan recognises Bitcoin as a legal method of payment, although not a currency.

Digital rights



increasing relevance

A 93-day shutdown of the Internet in Cameroon's English-speaking regions has ended, returning Internet access to some 20% of the country. The government statement announcing the restoration of Internet services notes that the government reserves the right to cut services again if misuse occurs.

The European Parliament has identified several privacy-related concerns regarding the Privacy Shield, in a resolution adopted in early April. The Article 29 Working Party (WP29) also outlined points of concern related to the proposed ePrivacy Regulation, as did the European Data Protection Supervisor over the proposed directive related to contracts for the supply of digital content.

US President Donald Trump signed a bill repealing the FCC Internet privacy rules. In accordance with the FCC regulations, broadband companies were required to get permission from their Internet users to use their data - including browsing history, geolocation, financial and medical information - for targeted advertisements. The bill had just been passed by the US Senate.

Germany has drafted a new Network Enforcement Law to tackle hate speech and fake news, raising concerns over the scope of application for social networks and the lack of clarity about the obligations imposed on platform operators.

Facebook announced the launch of new tools to combat the sharing of intimate images without permission, usually reported as 'revenge porn'. Reports will be reviewed and resolved according to the company's Community Standards.

Jurisdiction & legal issues



decreasing relevance

Twitter has filed a complaint against the US Custom and Border Protection (CBP)'s attempt to force Twitter to release user information related to an account tweeting against the Trump administration. [The American Civil Liberties Union \(ACLU\) announced its intention to file papers on behalf of the user.](#) [The CBP later withdrew its demand, and the US Department of Homeland Security announced an investigation to determine whether the demand was improper.](#)

Facebook faced criticism over a violent video posted by one of its users, [especially for the long delay in removing the video.](#) Although Facebook is generally reluctant to overly arbitrate what is posted on its site, the company wrote in a statement that it is exploring new ways to ensure a safe environment on Facebook.

Infrastructure



same relevance

gTLDs .com and .net are among those with the most webpages hosting child sexual abuse material, according to the latest Internet Watch Foundation report. [More on page 3.](#)

Research by the NATO Cooperative Cyber Defence Centre of Excellence and the Tallinn University of Technology shows that the IPv6 transition opens a wide scope for potential cyber-attacks.

AFRINIC, the regional Internet numbers registry for Africa, will discuss a proposal to stop allocating IP addresses to governmental entities in countries that shut down Internet access.

Net neutrality



increasing relevance

In the USA, FCC Chairman Ajit Pai issued a proposal to limit the Commission's oversight of Internet service providers, by overturning the classification of broadband providers as utility carriers. [Although Pai mentioned that his intention is to still keep in place the net neutrality principles, commentators argue that, without this classification, the Commission's ability to enforce net neutrality rules would be weakened.](#)

In a new framework for assessing the differential pricing practices of Internet service providers, [the Canadian Radio-television and Telecommunications Commission reinforced its commitment to net neutrality.](#) It stated that differential pricing generally gives an unfair advantage or disadvantage to certain content providers and consumers.

New technologies (IoT, AI, etc.)

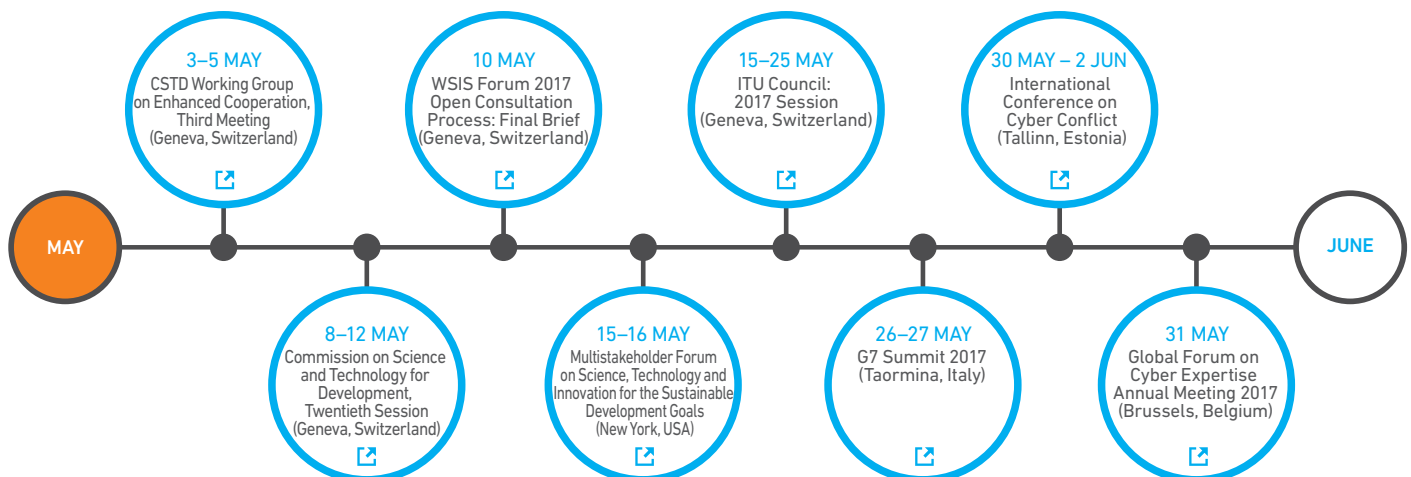


same relevance

Google has proposed 'federated learning' to address privacy concerns in artificial intelligence (AI) solutions. Although AI algorithms involve the centralisation of users' data in a data centre for machine-learning, federated learning would only require encrypted updates to be sent to Google, rather than raw data.

Facebook is developing helicopter drones to provide Internet access to disaster areas. The Tether-tenna drone could be used in natural disasters where infrastructure is damaged but fibre lines still work.

AHEAD IN MAY



For more information on upcoming events, visit <http://dig.watch/events>

ADDING SUBSTANCE TO THE GENEVA INTERNET CONVENTION

In February 2017, Microsoft proposed a Digital Geneva Convention that would commit governments to protecting civilians from nation-state cyberattacks in times of peace. This month, the company published three additional policy papers, further shaping its vision on the role of states and the private sector in ensuring cybersecurity.

In *Advancing a Digital Geneva Convention to protect cyberspace in times of peace*, Microsoft outlines 10 'key clauses' for such a convention. A few clauses relate to critical infrastructures and the need for states to refrain from attacking systems that are important for the safety and security of citizens, or for the global economy, as well as to limit engagement in cyber offensive operations that could damage such infrastructures.

Other clauses touch on the issue of privacy: states should refrain from hacking personal accounts or private data, as well as from inserting or requiring a backdoor into technology products. In one clause tackling intellectual property, states are asked to refrain from using ICTs to steal the intellectual property of private companies.

Governments are also expected to support the private sector's cybersecurity-related efforts, by agreeing to a policy for acquiring and reporting vulnerabilities in technology products and services, and by assisting companies in their efforts to prevent and address cyber-attacks. Lastly, states should commit to exercise restraint in developing cyber weapons, as well as agree to limit their proliferation.

Microsoft also proposes the creation of an *International Cyberattack Attribution Organization*, lead by the private sector, to identify and attribute state or state-sponsored cyberattacks, and present technical evidence to governments, enterprises, and the public. Such an organisation should only focus on the most significant attacks, such as those targeting critical infrastructures, elements of the global economy, or critical Internet resources. While the organisation would



identify the attackers, it would be up to states to determine the appropriate political and economic responses.

Microsoft also turns its attention to the private sector's role in keeping the Internet secure for end-users. In its vision, a *Tech Accord* should be created to demonstrate the technology industry's commitment to cybersecurity. The Accord should be based on six objectives: no assistance for offensive cyber operations, assistance to protect customers everywhere, collaboration to bolster first-response efforts, support for government response efforts, coordination to address vulnerabilities, and fight against the proliferation of vulnerabilities.

PRIVACY SHIELD: EUROPEAN PARLIAMENT FINDS WEAKNESSES IN THE AGREEMENT

The Privacy Shield, created to allow US companies to transfer and process personal data of EU citizens without breaching EU rules, continues to attract concerns over the adequacy of the protection it offers. Such concerns have recently been raised by the EP and the European Data Protection Supervisor (EDPS).

In its 6 April resolution, the EP outlines several shortcomings and weaknesses of the Privacy Shield, and asks the European Commission (EC) to properly address them.

In the EP's view, neither the Shield nor the US administration's letters of assurance demonstrate the existence of effective judicial redress rights for EU citizens whose personal data is processed by US LEAs. The EP also notes that 'bulk surveillance' remains possible under the agreement, and points out that US rules on the bulk collection of personal data of non-US citizens do not meet the EU criteria of necessity and proportionality. Concerns have also been raised concerning the fact that the Privacy Shield is based on the Presidential Policy Directive (PPD-28) which can be repealed by the US President without consent of the US Congress.

As the date of the Shield's first annual review approaches (September 2017), the EC is called to monitor whether EU citizens' personal data is deleted when no longer necessary for the purpose for which it was originally collected, including by LEAs; ensure that the Shield will fully comply

with the EU General Data Protection Regulation (applicable from May 2018); and evaluate whether the mechanisms and safeguards indicated by the US administration are effective and feasible.

The EP is not the only one concerned about the adequacy of the Privacy Shield. In March, Věra Jourová, EU Commissioner for Justice, Consumers and Gender Equality, visited Washington to discuss the Shield, after the American Civil Liberties Union and Human Rights Watch sent a joint letter to the EC calling for a re-examination of the agreement. In a speech made during her visit, Jourová underlined the importance of placing limitations on government access to personal data for national security. Giovanni Buttarelli, EDPS, expressed his scepticism with regard to the US administration's commitment to the data transfer agreement, especially in the light of the US Congress's vote to roll back the privacy rules for Internet service providers.

Keep track of privacy-related developments on the GIP Digital Watch observatory at dig.watch/privacy.

UNCTAD E-COMMERCE WEEK: AN OVERVIEW

UNCTAD's annual E-commerce Week ran from 24 to 28 April 2017, at the Palais des Nations, in Geneva. The overarching theme of the event was 'Towards Inclusive E-Commerce' and a key goal was to promote multi-stakeholder discussions that would lead to concrete actions towards more inclusive digital trade, global benefits, and sustainable development, in line with the SDGs.

The various sessions planned by UNCTAD and several other organisations covered a wide range of issues under the topics of regulatory frameworks, facilitation of digital commerce, and transparency. Development and inclusion were transversal topics that guided the reflections presented in all sessions. The Geneva Internet Platform provided just-in-time reporting from most of the sessions, summarising the key issues raised by the speakers.

The development dimension of E-commerce Week was made even more prominent with the launch of the eTrade for All online platform, which serves as an information hub for developing countries to navigate the technical and financial services available to drive development through e-commerce, and which is a central component of UNCTAD's eTrade for All initiative. The platform will allow donors to easily view projects and programmes waiting to be funded, and will enable organisations to communicate about obstacles and solutions regarding e-commerce. A special session was held on how to help least developed countries to achieve e-trade readiness. Enabling aspects that support the involvement of SMEs and promote investment, internationalisation, and export were also tackled during the event.

Under the topic of regulatory frameworks, consumer protection, privacy, and cybersecurity were emphasised. The event kickstarted with a session that presented the results of a global survey on Internet Security & Trust conducted by Ipsos and the Centre for International Governance Innovation (CIGI), in collaboration with UNCTAD and the Internet Society, revealing that nearly 50% of Internet users surveyed do not trust the Internet. It confirmed the importance of having adequate consumer protection and data protection in place for promoting e-commerce. Among those worried about their privacy, the top sources of concern were cybercriminals (82%), Internet companies (74%), and governments (65%).

With regard to privacy, speakers made some recommendations on the way forward, such as engaging in Conven-

tion 108, from the Council of Europe, which is open for signature of non-European countries. Points were raised on the need for developing the necessary regulatory frameworks at national level, while avoiding regulation that is too prohibitive and hinders the flow of data, such as provisions on data localisation. The role of data flows in achieving the SDGs, as well as potential policies enacted by international organisations and governments, were also topics of discussion.

In the field of cybersecurity, the need for co-operation between states and other stakeholders, the importance of building consensus around agreed international protocols and for implementing capacity building for countries that lack expertise, were some of the points mentioned. The World Bank introduced a portal, comprising a toolkit, an assessment tool, and a virtual library with the aim of building capacity among policymakers, legislators, public prosecutors, and civil society in developing countries.

The highlight of the week was the High-level Event on Digital Transformation for All: Empowering Entrepreneurs and Small Business, which brought together ministers, the secretary-generals of UNCTAD, the WTO and the ITU, Jack Ma, Chairman of Alibaba Group, and Amanda Long, Director General of Consumers International. The event also gave the opportunity to discuss the priorities for the different stakeholders. The G20 presented its agenda in the field of digital trade and the private sector shared its views and priorities for the future.

E-commerce Week was the kickstart of the the Just-In-Time Course on Digital Commerce delivered by the GIP, in partnership with the ITC, the Consumer Unity & Trust Society (CUTS International), UNCTAD, and DiploFoundation. The course will run in May and aims, among other things, to shed light on the interplay between trade and digital policies, in preparation for the WTO Ministerial Conference at the end of the year.



Credit: UNCTAD

Jack Ma, Chairman of Alibaba Group, and UNCTAD Special Advisor for Youth Entrepreneurship and Small Business, speaking at the High-level Event on Digital Transformation for All: Empowering Entrepreneurs and Small Business, on 25 April.

THE DIGITAL WATCH NEWSLETTERS: FROM CONCEPT TO PRINT

Digital policy is a complex field, involving daily developments on a global level. The *Geneva Digital Watch* newsletter was born out of the need to distil valuable information from the noise, analysing it, and sharing bite-size content.

Readers of this newsletter may be very familiar with the regular briefings, held on the last Tuesday of every month (in Geneva, at one of our hubs, or online), where monthly developments are summarised and presented. The briefing is supported by the 8-page newsletter which describes the developments in more detail, and includes an analysis of the main trends and other topical updates.

The cycle is therefore quite simple. The preparations, however, are a bit more complex.

A 40-strong team of curators – including computer scientists, lawyers, academics, and other experts – monitor, discuss, analyse, and report on the main global and regional developments. Underlying the cycle is the *GIP Digital Watch* observatory (<http://dig.watch>), which is continuously updated with the latest content and data on each of the 40+ issues it covers.

Over time, the team started following important processes, such as the work of the UN GGE, and those related to the SDGs. Many developments warrant further research. For example, what are the implications of the sharing economy for employment? How are financial institutions worldwide responding to new technological advancements such as cryptocurrency? How is net neutrality regulated around the world?



The team is now growing; more curators will join the *Digital Watch* team at the end of May, to undertake more research, go deeper into the issues, and strengthen our reporting initiatives.

FROM FACTS TO... FACTS

One of the most important elements in the work of *Digital Watch* is objectivity in reporting and analysing developments. Editorial policies are quite strict, ensuring high standards and meticulousness.

Concerns over the spread of fake news and false information brought more attention to the quality of sources and the reliability of content. In a bid to deal with fake news quickly and efficiently, artificial intelligence filters have been suggested, and counter-campaigns proposed. Yet, the best immunisation against fake news is a stronger public space.

A formula for ensuring a solid information space is a credible and current approach, adopted by the team.

Basing analysis on reliable and original sources is crucial, and contributes to the *Digital Watch's* credibility. The ubiquitous blue link icon in the newsletters – often as many as 100 links in any one issue – represents the efforts of backing content with links to sources, and providing additional information or resources for more in-depth reading.

In such a fast-changing environment, timeliness in delivering the analysis is crucial. The *Digital Watch* newsletter is consistent with its monthly appointment, and it is put to the test time and again during reporting initiatives from major digital policy events, where session reports go online and daily newsletters are published and distributed within hours.

Factual, though, does not mean boring. Interactive visualisations, intuitive infographics and illustrations, and contemporary designs, contribute to a better understanding of complex issues.

This approach requires time, resources, and gradual development. While it might not offer a quick-fix to the problem of fake news, *Digital Watch* contributes to an inclusive, responsible, and robust public policy space.

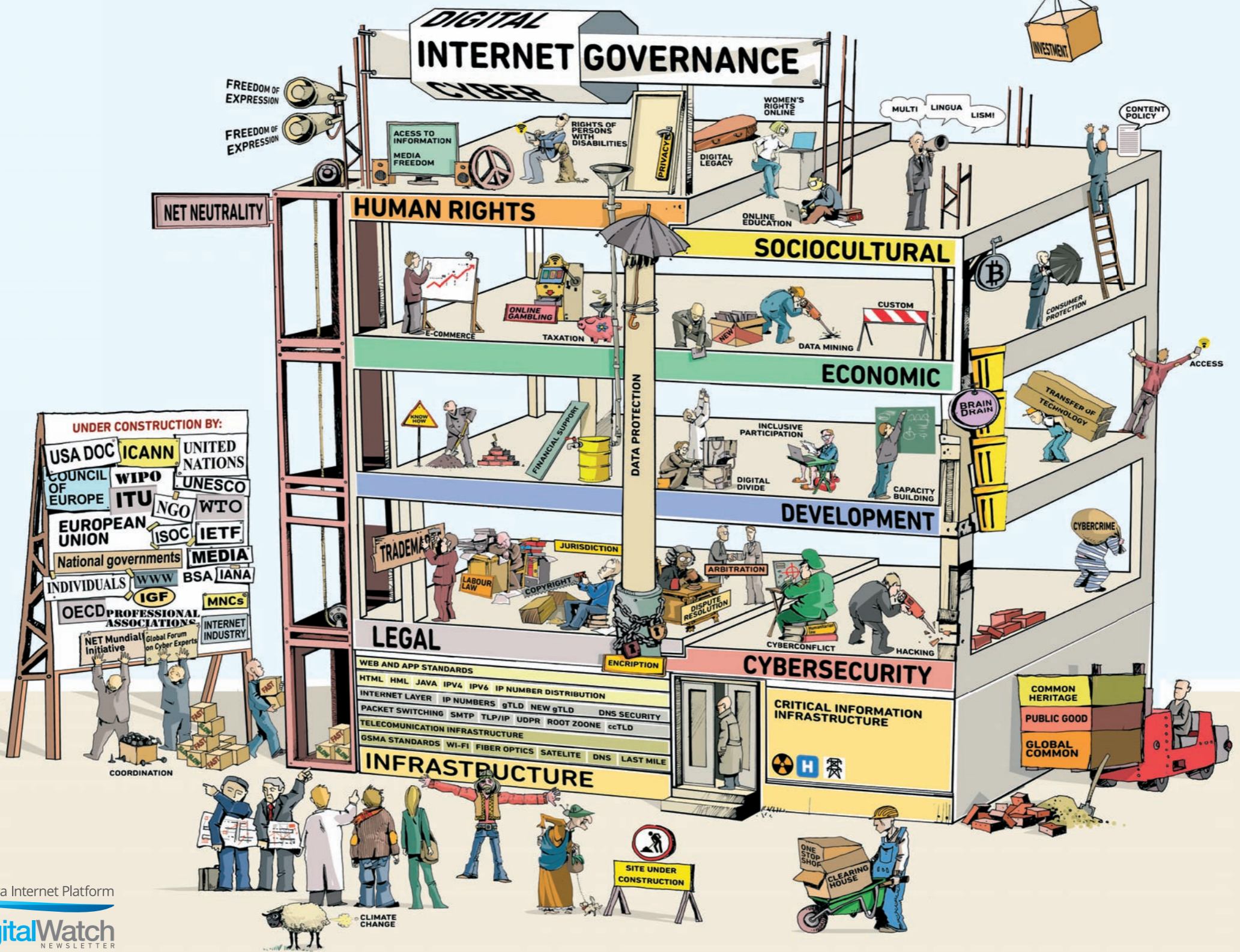
In the next phase, the Digital Watch will focus on publications in other languages. If your institution is interested in partnering and/or supporting new versions of the Digital Watch newsletter, get in touch at digitalwatch@diplomacy.edu



Subscribe to *GIP Digital Watch* updates at <http://dig.watch>

INTERNET GOVERNANCE BUILDING UNDER CONSTRUCTION

v. 2016



2017

June: WSIS Forum
December: Internet Governance Forum

Follow also:
UN CSTD,
WTO Forum

Standardisation

ISO, ITU, IEC, UNÉCE

Digital Trade

WTO UNCTAD ITC

Infrastructure

ITU ISOC

Development

SDG Lab ITU UniGeneva

UN GGE DCAF

UNIDIR GCSP

SECURITY

EMERGENCY

Geneva Internet Platform
DigitalWatch



CYBERSECURITY
ENCRYPTION MULTILINGUALISM
PRIVACY JURISDICTION
INTERNET OF THINGS
COPYRIGHT
DIGITAL DIVIDE

ICANN

POLICY RADAR

Data CERN WMO WHO

Copyright WIPO

Digital and future of work ILO

HUMAN RIGHTS ONLINE

PRIVACY Freedom of information

UN Human Rights Council

CHECK ALSO

- Cloud computing
- Net neutrality
- Artificial intelligence
- Big data
- Content policy
- Cyber currency

NAVIGATING THE DIGITAL POLICY LANDSCAPE IN GENEVA



Geneva Internet Platform
DigitalWatch
NEWSLETTER

DIPLO
www.diplomacy.edu

Geneva Internet Platform