Geneva Internet Platform
DigitalWatch
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 JULY & AUGUST

Summer is generally a quiet period for policy-making. This year, however, July and August have been uncharacteristically busy, and have brought significant developments in digital policy.

CYBER AS THE FOURTH MILITARY DOMAIN

In early July, NATO declared cyberspace to be the fourth military operation domain in addition to land, water and air. Nato's decision was triggered by the growing level of cyber conflicts across national borders.

This decision will have numerous impacts not only for NATO but also for global governance. Namely, cybersecurity will gain more prominence on global diplomatic agendas. Stakes in how the Internet is managed will be higher as well.

The question 'what is cyberspace' will keep many policymakers and academics busy in the forthcoming period. On the one hand, cyberspace is anything but new. Hardware and servers are on land; undersea cables carry most of the global Internet traffic; wi-fi connects us to the Internet via 'air'. According to the UNIDIR's recent report, 'cyberspace is being "normalised" and is no longer seen as a unique space where existing rules do not apply.'

On the other hand, the view on the uniqueness of cyberspace is rooted in the profound changes that the Internet brought to social, economic, and security realities of modern societies.

This diplomatic dichotomy between real and cyberspace is very vivid in Pokémon Go. Millions of Pokémon gamers walk in the 'real' world of parks and streets while they search for the virtual creatures. *More on Pokémon Go and the policy research on territorial and virtual on page 8.*

STATE RESPONSIBILITY IN CYBERSPACE

From 28 August to 2 September, some answers to the new challenges in cyberspace will be discussed by the fifth UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which will meet in New York.

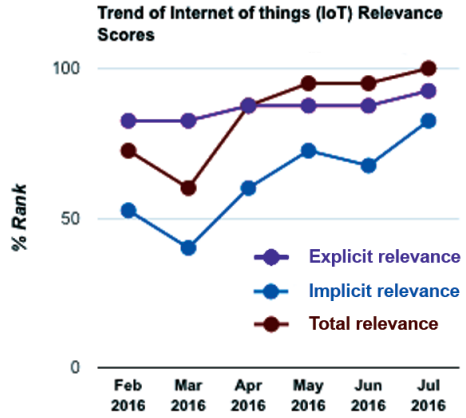
After confirming that international law applies to digital space, the UN GGE's next question will tackle *how* it applies. In particular, the fifth UN GGE will address state responsibility in cyberspace.

Continued on page 3

DIGITAL POLICY IN ONLINE MEDIA

The world of the Internet of Things (IoT) evokes sentiments of optimism and positive anticipation which transpire even in digital policy debates. The IG Barometer of Online Media reveals that together with other issues, IoT is one of the most debated topics this summer.

More on page 6



IN THIS ISSUE

Published on 23 August 2016. In addition to this newsletter, you can find in-depth coverage on the *GIP Digital Watch* observatory (http://digitalwatch.giplatform.org) and join live discussions on the last Tuesday of every month online, at local hubs, or at the Geneva Internet Platform premises | The *Geneva Digital Watch* newsletter is published by the Geneva Internet Platform and DiploFoundation | Design by Viktor Mijatovic, Diplo's CreativeLab | Contributors to this issue: Stephanie Borg Psaila, Marilia Maciel, Aida Mahmutovic, Aye Mya Nyein, Tereza Horejsova, Jovan Kurbalija, Virginia Paque, Roxana Radu, Barbara Rosen Jacobson, Sorina Teleanu | Send your comments to digitalwatch@diplomacy.edu. The Brazilian version in Portuguese is available at http://digitalwatch.giplatform.org

Human Rights Council - 32nd Session

On 1 July, the UN Human Rights Council adopted by consensus the resolution on the promotion, protection and enjoyment of human rights on the Internet during its 32nd session. The resolution builds on a 2012 joint initiative by Brazil, Sweden, Nigeria, Tunisia, Turkey, and the USA, reaffirming that 'the same rights that people have offline must also be protected online', which was further updated in 2014. The 2016 resolution condemns unequivocally 'measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures'. It also calls for a High Commissioner report on ways to bridge the gender digital divide from a human rights perspective.

UNICRI Workshop on Using Big Data Analytics to Reinforce Security

The workshop on Using Big Data Analytics to Reinforce Security, organised by the UN Interregional Crime and Justice Research Institute (UNICRI), on 4-5 July, emphasised how big data analytics can reinforce cybersecurity, biotechnology, trafficking, and supply chains security. The risks of using big data, such as the misuse and leakage of data and legal challenges on protection of data were also highlighted. Recommendations on creating innovative products where security and privacy are designed, and providing training and cooperation in big data analytics to ensure the security of humans, were mentioned during the workshop.

MIKTA Workshop on Electronic Commerce

The full-day workshop organised by Mexico, Indonesia, the Republic of Korea, Turkey, and Australia (MIKTA) on 5 July focused on digital trade and its implications for developed and developing countries. E-commerce was discussed in connection with the World Trade Organization agenda, as well as for essential support services such as transport, logistics, delivery services, and financial services. Discussions also touched on data flows and data localisation, and consumer protection and privacy, and set the stage for further analysis and potential cooperation on these topics.

OPEN CONSULTATIONS, MAG MEETING DISCUSS IGF 2016

The second Open Consultations and Multistakeholder Advisory Group (MAG) meeting, held on 12-14 July in New York, in preparation for the 2016 Internet Governance Forum (IGF), was organised by the IGF Secretariat and the UN Department of Economic and Social Affairs.

Opening the consultations, Under-Secretary General Hongbo Wu stressed that the priority for Internet governance (IG) should be linked to the implementation of the sustainable development goals (SDGs). The UN's commitment to strengthening multistakeholder engagement in IG was reaffirmed, including through remote participation. Wu stressed that as the IGF begins a new cycle of its mandate, it is important to strengthen its outputs and conclusions, and to produce policy recommendations, especially on issues in which there is less divergence among stakeholders.

A considerable part of the consultations was dedicated to discussing the Retreat on Advancing the 10-year mandate of the IGF, which took place on 14-16 July in New York. The retreat was part of a wider ongoing process aimed at improving the IGF.

The participants of the open consultations made additional suggestions to the agenda of the retreat, such as analysing the possibility of creating a mentoring programme, developing a strategy to enhance youth involvement, and improving remote participation. Participants also asked for more clarity on the outputs of the retreat, especially in terms of who will carry the outputs forward, and who will be responsible for their implementation.

Reports from the work being carried out by the five IGF 2016 Best Practice Forums, as well as updates from the second phase of the initiative on Policy Options for connecting and enabling the next billion, were shared during the open consultations. Both processes are part of an effort to extend the IGF's impact and implement the recommendations of the 2012 UN Commission on Science, Technology, and Development Working Group on Improvements to the IGF.

The MAG meeting was dedicated to the preparation of the next IGF, especially the forum's programme. This year, 274 workshop proposals were received, graded, and assessed by MAG members, and approximately 100 will be included on the final agenda.

MAG also discussed the proposed themes for IGF main sessions, which varied across a wide range of issues, such as sustainable development and growth; trade agreements; Internet governance and SDGs; national and regional IGFs; economic, social and cultural rights; and jurisdiction issues.

A third IGF preparatory meeting will likely be held closer to the IGF.

This icon indicates that there is more background material in the digital version. Alternatively, visit http://digitalwatch.giplatform.org for more in depth information.

Continued from page 1

Can and should governments be responsible for cyberattacks triggered by individuals and companies under their jurisdiction? Do they have the means to ensure that 'their' cyberspace is properly used? How would government supervision of cyberspace affect the open and inclusive nature of the Internet?

These and other questions will be addressed by the UN GGE and other policy-making bodies worldwide in the coming period. *Visit the GIP Digital Watch observatory for more information on UN GGE and read Dr Jovan Kurbalija's comprehensive analysis on state responsibility in the digital space.*

PRIVACY SHIELD: THE ATLANTIC DATA HIGHWAY

European and US diplomats have finalised the EU-US Privacy Shield framework that will facilitate the data flow between two different privacy protection regimes. The new Privacy Shield is in response to the Court of Justice of the European Union's invalidation of the Safe Harbour agreement. The court had ruled that Safe Harbour did not adequately protect the privacy of EU citizens whose data was hosted in the USA's more relaxed privacy protection space. *More on page 7.*

Transatlantic data flows and the regulations that surround them will remain high on policy agendas since the flow of data across the Atlantic Ocean is vital for the global Internet industry. As indicated on the map, the Atlantic is the busiest highway in the global digital space.

JURISDICTION AND ACCESS TO DATA

In a landmark judgement, a US appeals court ruled that US authorities cannot use a search warrant to force Microsoft to turn over users' data stored in another jurisdiction. The case concerned the data of a criminal suspect in a drug investigation whose emails were stored on a Microsoft server in Ireland.

The judgement, which overturned a previous ruling, will have far-reaching consequences in the way the USA and other countries can access data of relevance and interest for them which are stored in other jurisdictions.

INTERNET AT THE CENTRE OF TERRORIST AND SECURITY THREATS

The initial investigations following the Nice and Munich attacks pointed towards the different ways in which the Internet was used by terrorists for the organisation of their attacks. The Munich attacker fueled his intentions through the Internet and bought his weapon from the DarkWeb.

In Turkey, at the height of the recent attempted coup d'état, President Erdogan communicated to the outside world through a video message. In the aftermath, Turkish authorities limited access to the Internet and social media, and banned WikiLeaks after it released a series of emails concerning Turkish officials.

DIGITAL POLICY AND THE DEVELOPMENT AGENDA

Earlier this year, the World Bank report indicated that the availability of the Internet per se is not sufficient to reap the dividends, especially in developing countries. Efforts must be supplemented by the so-called analogue complements that include good regulation and skills.

In July, the UN High-Level Forum on Sustainable Development considered the progress one year on, while the United Nations Conference on Trade and Development (UNCTAD) launched the new eTrade for All initiative in Nairobi, aimed at boosting e-commerce in developing countries.

There are many hopes that 'e-' can be an important engine of growth, and this is showcased by good examples from Kenya, Ghana, and Southeast Asia countries, among others.

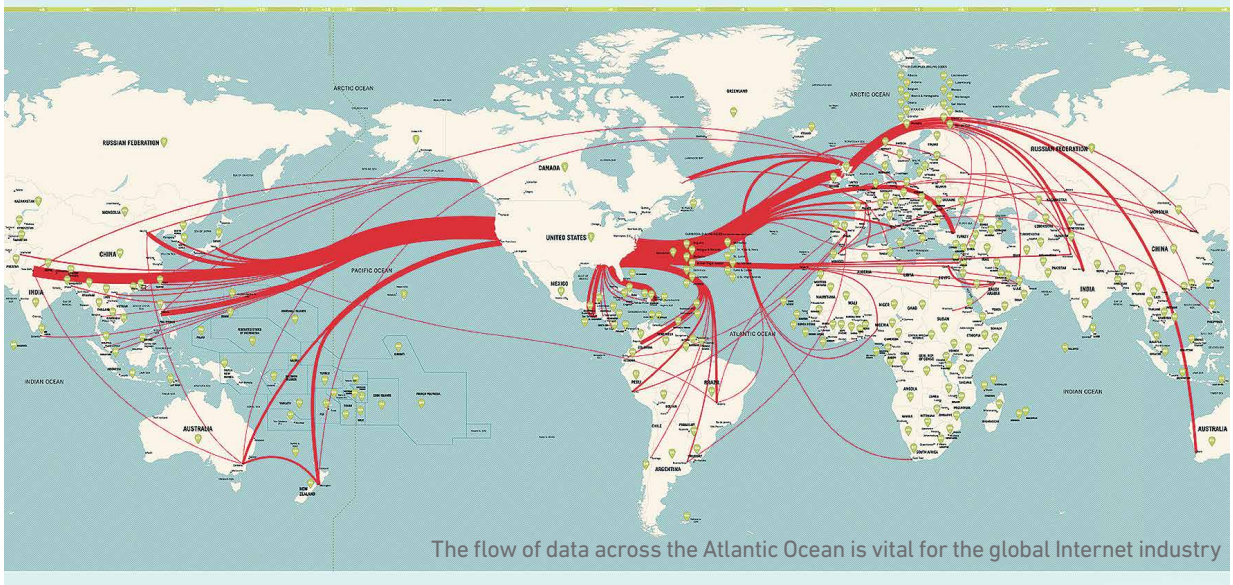
E-COMMERCE GAINING MOMENTUM

The World Bank's report set the stage for numerous activities linking e-commerce, trade, and development. It was followed by other reports - including ITU's report, *ICT Facts & Figures 2016*, and WIPO's *Global Innovation Index* - and a number of events on e-commerce, including those hosted by the World Trade Organization and UNCTAD.

UNCTAD's eTrade for All initiative, the WTO's collaboration with Silicon Valley players on linking e-trade with development, and other trends will set the stage for even more concrete activities. The GIP will host a session on SDGs and e-trade during the upcoming WTO Forum.

Turn to pages 4-5 for more digital policy developments in July and August.

GLOBAL DIGITAL TRAFFIC



The flow of data across the Atlantic Ocean is vital for the global Internet industry

Credit: www.telegeography.com

DEVELOPMENTS JULY & AUGUST

Global IG Architecture

same relevance

The second Open Consultations and MAG meeting discussed preparations for IGF 2016, the work of the five IGF 2016 Best Practice Forums, and updates from the second phase of the initiative on Policy Options for connecting and enabling the next billion. The IGF Retreat, which followed the MAG meeting, looked at ways of improving the overall preparatory process and intersessional activities, and of engaging stakeholders, funding issues, and shaping the output of the IGF.

The EU plans to make broadband Internet access a legal guarantee under proposed changes to universal services rules. The proposal foresees national governments paying for broadband access.

WIPO's *Global Innovation Index* calls for more inclusive governance mechanisms to help improve global innovation. While many frameworks exist within ITU, WIPO, ISO, etc, complementary mechanisms for improving international science and R&D cooperation are needed.

Sustainable development

increasing relevance

The UN High-level Political Forum (HLPF) on Sustainable Development met for the first time since the adoption of the 2030 Agenda in 2015. The UN's *Global Sustainable Development Report* which assessed the progress so far, confirmed that technology is essential for achieving the SDGs and for minimising trade-offs among goals; at the same time, it has also continuously added new challenges.

UNCTAD launched a new initiative, eTrade for All, aimed at boosting e-commerce in developing countries, and facilitating progress towards the SDGs.

The ITU's report, *ICT Facts & Figures 2016*, shows that the digital divide is still very much a reality. An estimated 3.9 billion people, mostly in developing countries, remain cut off from the Internet. GSMA's Mobile Connectivity Index, which measures the performance of 134 countries in enabling mobile Internet adoption, also explores ways in which mobile can help achieve the goals.

Security

increasing relevance

At the Warsaw Summit, NATO recognised cyberspace as its fourth operational domain, in addition to air, land, and sea. Earlier, NATO passed a Cyber Defence Pledge, in which it plans 'to strengthen and enhance cyber defences of national networks and infrastructures, as a matter of priority'.

The European Parliament adopted the Network and Information Security (NIS) Directive, requiring states to establish Computer Security Incident Response Teams (CSIRTs) and to designate competent national authorities for NIS. It also sets up a cross-EU cooperation group for strategic cooperation, and a CSIRT Network for operational cooperation.

Bitfinex, one of the most popular cryptocurrency exchanges, was hacked in one of the largest breaches. Almost 120,000 bitcoin worth around $78 million were stolen. Customers will lose over 36% of assets, but will be compensated for losses.

When it comes to terrorism, one report reveals a wide range of online tools used by terrorists, including VPNs and encrypted messaging services. A US court ruling however, dismissed the claim that Twitter could be held legally responsible for 'material support' to terrorists.

Privacy and human rights

increasing relevance

The European Commission approved the new EU-US Privacy Shield Framework, which will regulate the flow of EU citizens' data to the USA. *More on page 7.*

In the aftermath of the attempted coup in Turkey, citizens continued to face interrupted access to the Internet. In particular, Turkey blocked access to the WikiLeaks website following the leak of thousands of emails from the ruling party.

In Brazil, a court ordered a freeze on Facebook's funds in a dispute on encrypted data forming part of a drug-related investigation. A judge also blocked WhatsApp for several hours until the company revealed encrypted messages pertaining to a criminal investigation.

An Amnesty International report has revealed that Belarusian activists, who are subject to extensive government surveillance, rely on encryption as a 'last line of defence'.

Infrastructure

same relevance

Plans are under way to deploy 5,000 km of fibre-optic cables across five West African countries (Benin, Togo, Niger, Burkina Faso, and Ivory Coast), while a consortium in Qatar has launched the construction of the Asia-Africa-Europe-1 (AAE-1) 25,000 km cable which will connect the three continents. Other cables in the region are also in the works.

In the Netherlands, a nationwide LoRa network has been rolled out for Internet of Things applications. The network went live last year in Rotterdam and The Hague.

Key players in the European telecoms industry have presented a 5G Manifesto to the European Commission. The manifesto pledges to launch fast 5G mobile network in all EU member states by 2020, and will be used by the Commission in its development of the 5G Action Plan.

Net neutrality

decreasing relevance

The 5G Manifesto presented by the Body of European Regulators for Electronic Communications, as criticises the draft EU net neutrality rules presented by the EU body for regulators of electronic communications, as the guidelines could obstruct innovation and lead to significant uncertainties.

E-commerce and Internet economy

increasing relevance

EU rules on electronic signatures, seals, timestamps, electronic delivery service, and website authentications, as well as electronic documents have started to apply in all EU countries.

UNCTAD's eTrade for All initiative aimed at boosting e-commerce in developing countries, will assist developing countries in several areas, including e-commerce assessments, ICT infrastructure, legal and regulatory frameworks, and skills development.

EU regulators have accused Google of blocking its competitors in online advertising. The European Commission has previously charged Google with two other cases in which it would hinder competition.

Ride-hailing service Uber has abandoned its China strategy, selling out to local competing app Didi, in return for a stake in the company.

Jurisdiction

increasing relevance

A US appeals court ruled that the government cannot use a search warrant to force Microsoft to turn over the email communications of a criminal suspect in a drug case, which were stored at Microsoft's data centre in Dublin. A search warrant, therefore, cannot be applied internationally.

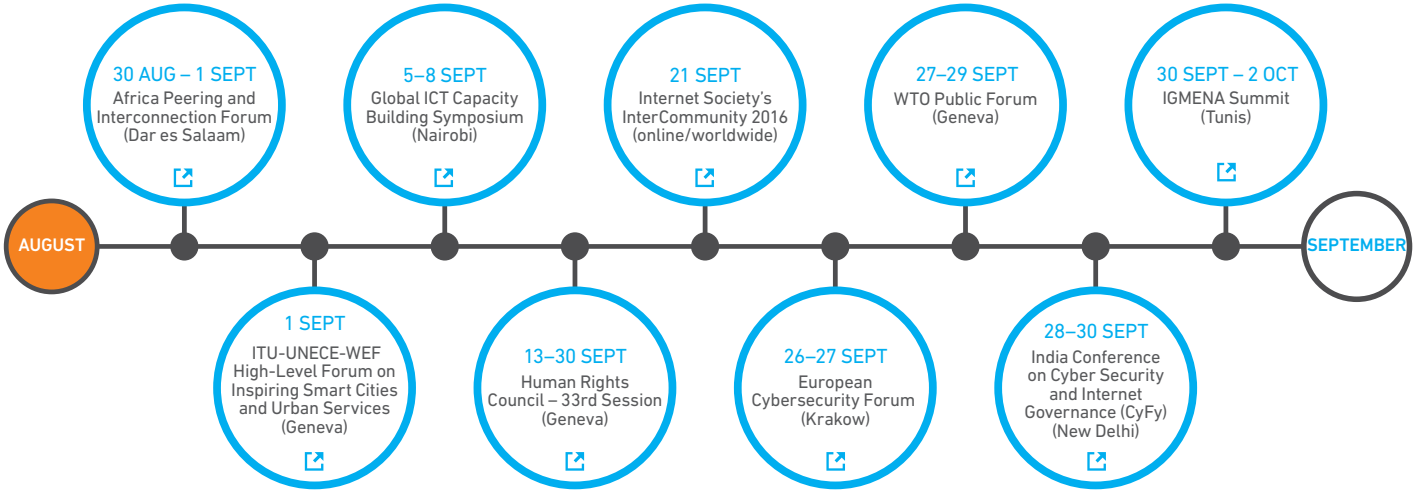
IANA Transition

same relevance

ICANN has submitted the IANA stewardship transition implementation plan to the US government, confirming that remaining tasks in support of the transition will be completed before 30 September. The existing contract will be allowed to expire, NTIA has confirmed.

The Post Transition IANA entity that will start performing the IANA functions has been legally incorporated under the name Public Technical Identifiers (PTI). Meanwhile, two new committees – the Customer Standing Committee and the Root Zone Evolution Review Committee – required for the completion of the transition, were formed.

AHEAD IN SEPTEMBER



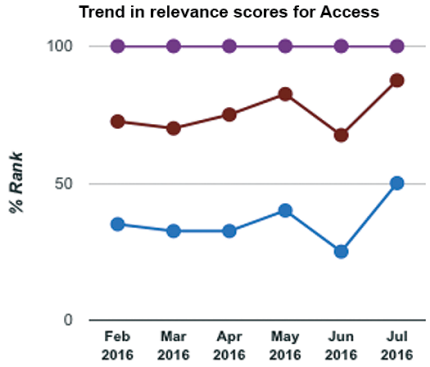
For more information on upcoming events, visit http://dw.giplatform.org/events

DIGITAL POLICY IN THE MEDIA

In digital policy discussions, some issues are more often debated than others. Issues related to privacy and other human rights, cybersecurity, net neutrality, and e-commerce – to take a few examples – are regularly in focus. At the same time, debates not only take place within IG communities, but also play out in the media. Ranging from mainstream journals to specialised portals, the media is often a good indicator of the status of a debate.

Our IG Barometer of Online Media analyses thousands of media sources every month to compute the relevance of issues, the type of language used, the positive or negative sentiment expressed, and which countries the issues mostly relate to – among many other computations.

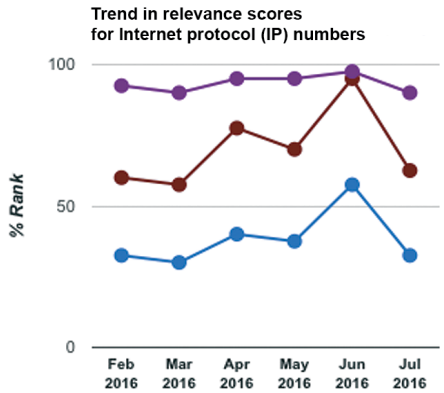
The barometer's scores for July and six-month trends reveal a few fluctuations. While the results provide input for our researchers to assess whether the fluctuations hint at deeper policy shifts, we can determine which are the top three debated topics so far this summer.



Access and **digital divide** (the latter to a lower but significant extent) saw an upward spike in July, after a relatively quiet June. *What happened in July?*

The UN Human Rights Council passed a resolution condemning the intentional disruption of citizens' Internet access. In New York, the UN High-level Political Forum (HLPF) on Sustainable Development met for the first time since the adoption of the 2030 Agenda in 2015.

In addition, several reports were published in July: the UN's *Global Sustainable Development Report*, which provided an overview of the progress made, and which informed the HLPF; the International Telecommunication Union (ITU) released its *ICT Facts and Figures 2016*, containing end-2016 estimates for key indicators in the ICT/telecommunication field; the World Economic Forum published the *2016 Global Information Technology Report*, examining countries' capacity to use ICTs for 'increased competitiveness and well-being' and summarising the Networked Readiness Index; the GSMA published the *Mobile Connectivity Index*, measuring the performance of 134 countries in enabling mobile Internet adoption.



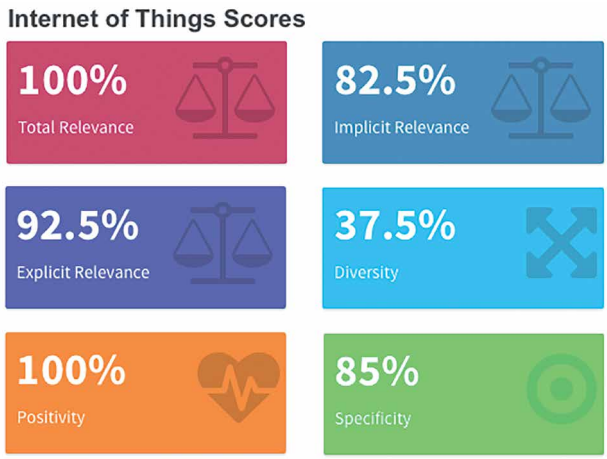
IP numbers and root zone were also increasingly debated in June, compared to other months. *What happened in June?* The US government announced it had reviewed the IANA stewardship transition proposal and gave it the green light. The so-called Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability) began its work on nine additional areas where ICANN community, staff, and Board accountability could be improved (known as Work Stream 2).

ICANN, the Internet Engineering Task Force (IETF), and regional Internet registries – the organisations that manage the allocation of IP resources across various regions – concluded agreements for post-transition provision of IANA services. This came on top of a draft bill, circulated by US Senator Ted Cruz, requiring Congress to approve the transition.

The world of the **Internet of Things** – which generally evokes sentiments of optimism and positive anticipation, even in digital policy – is growing at a fast rate, and so is the rate of innovation. The worldwide IoT market is expected to grow to $1.3 trillion in 2019, reaching an estimated 27 billion devices in 2025, and an estimated worldwide spending on IoT security of $547 million in 2018.

Researchers continue to spur innovation, from the use of LED bulbs for connecting devices, to the use of such technologies to build smart cities, while countries such as Korea and the Netherlands expand the dedicated infrastructure. It therefore comes as no surprise that the IoT has been increasing in relevance over the past few months, reaching a peak in July, and making it one of the most visible IG issues in online media. The trend in high positivity scores – the level of emotionally charged words used in the debate – is also visible for telecommunications infrastructure and convergence.

View the results of the IG Barometer of Online Media every month on the GIP Digital Watch observatory and learn more about the barometer.



- Explicit relevance looks at the number keywords and phrases in the same sources which are specific to each issue
- Implicit relevance looks at the presence of similar jargon for each issue in the analysed sources of online media
- Total relevance is computed from the implicit and explicit relevance scores

The scores are expressed as percentile ranks.

EUROPEAN COMMISSION ADOPTS NEW PRIVACY SHIELD

Nine months after the invalidation of the Safe Harbour Agreement, the European Commission (EC) confirmed that the new EU-US Privacy Shield affords adequate protection to the privacy of EU citizens. The framework imposes stronger obligations on US companies and requires the US government to more robustly enforce the new provisions and monitor their implementation.

The different privacy and data protection regimes in the EU and the USA have for long been a matter of concern for the EU, which has been intent on ensuring that the personal data of its citizens are adequately protected when transferred to and processed in the USA.

Up until October 2015, this issue was tackled within the context of the Safe Harbour Agreement, through which US companies committed to handle personal data in accordance with EU rules. In October, the Court of Justice of the European Union declared the framework invalid, sparking a wave of negotiations between European and US diplomats in search for a new mechanism. These negotiations resulted in the Privacy Shield, approved by EU member states in July, with four countries abstaining – Austria, Bulgaria, Croatia, and Slovenia.

The Privacy Shield aims to ensure a stronger protection for the personal data of EU citizens, when transferred to the USA. In practice, US companies will self-certify annually to meet the Privacy Shield requirements, while individuals will be able to make use of new complaint and redress mechanisms if their data is not adequately processed.

There are seven major privacy principles that companies self-certified under the Privacy Shield must adhere to:

Notice: Users must be provided with information on several aspects relating to the processing of their personal data (type of data collected, purpose of data collection and use, third parties to which data is disclosed, etc).

Choice: Users must be able to object to the processing of their personal data when this is done with a new purpose, different from the one for which the data was initially collected.

Accountability for onward transfer: Any transfer of personal data to a third party can only take place for limited and specified purposes, and on the basis of a contract which provides the same level of protection.

Security: Companies must take reasonable and appropriate security measures to ensure the protection of personal data.

Data integrity and purpose limitation: Personal data must be limited to what is reliable, accurate, complete, current, and relevant for the purpose of the processing. Moreover, personal data can only be retained for as long as it serves the purpose for which it was initially collected, or subsequently authorised.

Access: Users have the right to obtain information as to whether companies are processing their personal data; they must also be able to request that the data is corrected, amended, or deleted where it is inaccurate or has not been processed in line with the principles.

Resource enforcement and liability: Companies must provide robust mechanisms to ensure compliance with the principles, as well as recourse for users whose personal data have been processed in a non-compliant manner.

Under the Privacy Shield, individuals will be able to raise complaints directly with the company (which must reply within 45 days), to make use of Alternative Dispute Resolution solutions (to be provided free of charge), or to submit their complaints to data protection authorities (which will work with US authorities to ensure that such complaints are investigated and swiftly resolved). As a last resort, an arbitration mechanism will ensure an enforceable decision.

In addition, the Privacy Shield also addresses one issue that has presented a major area of concern: the US government's access to personal data of EU citizens. The Shield brought in written assurances from the USA that any such access will be subject to appropriate limitations, safeguards, and oversight mechanisms.

Moreover, the US government has brought clarifications related to the fact that bulk collection of data by intelligence agencies does not equate to mass surveillance; it explained that any bulk data collection involves the application of methods and tools to filter collection in order to focus it on needed material, while minimising the collection of non-pertinent information.

In addition, the US government has committed to creating an Ombudsperson mechanism for receiving and responding to complaints from individuals regarding US government access to their personal data. The Ombudsperson will oversee operation of the Privacy Shield, independent of US intelligence services, and will report directly to the Secretary of State.

The US government further commits to cooperate with data protection authorities in EU member states, and conduct annual joint reviews to monitor the functioning of the Privacy Shield. In addition, the USA will inform the EC of material developments in US law relevant to the Privacy Shield.

The Commission is to assess the level of protection provided by the Privacy Shield following the entry into force of the General Data Protection Regulation, in May 2018.

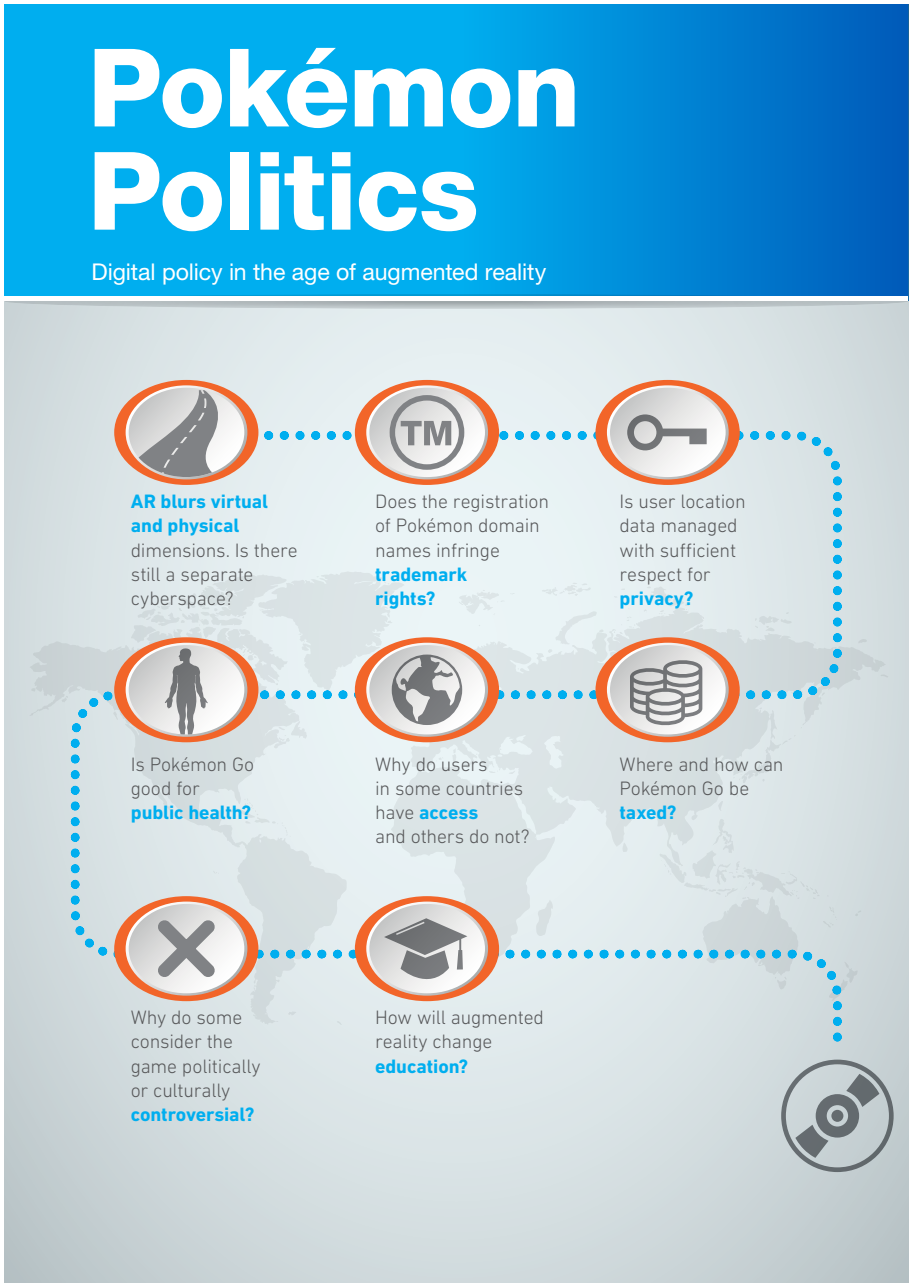
The US Department of Commerce began accepting Privacy Shield self-certification applications from US companies as of 1 August. On the other side of the Atlantic, the Commission has issued a guide for EU citizens on how to file complaints against US companies which self-certify under the Privacy Shield, but fail to handle personal data in line with its principles.

POKÉMON POLITICS: DIGITAL POLICY IN THE AGE OF AUGMENTED REALITY

Millions of people are searching for Pokémon worldwide. While Pokémon Go is a fun activity for many people, there are important social, economic, and political dynamics to discover that go beyond the actual game.

Pokémon Go brings into sharper focus many issues related to how we use the Internet and how the Internet affects our society. Conceptually speaking, Pokémon Go is an in vivo experiment of an interplay between the virtual and physical experiences of our reality. On a more practical level, this game moves people from houses into the open space, potentially leading to healthier lifestyles, but also to increased accident levels and urban planning challenges. Pokémon Go creates new possibilities for education as well. Learning can become more experimental and fun.

But, as it always goes with technology, Pokémon Go creates security risks. Deeply immersed in search for Pokémon, gamers can endanger themselves and others. Traffic incidents are increasingly reported worldwide. The security of users and their environment has even triggered the first bans on Pokémon Go, such as in the small French city of Bressolles. Wider concerns have also arisen, mostly related to the impact of the game on national security and religious values, leading to country-wide bans in Iran and Saudi Arabia.



Lastly, Pokémon Go is about business. It represents a new way of making money, primarily through its 'freemium' business model and the potential of the geospatial data generated by the game's players. Wherever there is a money flow, there are questions of taxation and customer protection – to name a few.

Read the full text on the *GIP Digital Watch* observatory, which analyses the impact of the game on each of the digital policy issues. The analysis includes a map showing the countries which have adopted or banned the game, and the countries in which the game is controversial. The discussions will continue during a webinar on Thursday, 15th September, dedicated to Digital Policy in the Age of Augmented Reality.