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 NOVEMBER

The digital policy community followed the US Presidential campaign with interest in November, due to the potential implications of US digital policy for global developments. At the same time, as policy shifts started taking place in the USA, other developments gave rise to recurrent and new trends.

1. US ELECTION AND THE ROLE OF INTERNET INTERMEDIARIES

The US Presidential election attracted more than its fair share of attention. In the aftermath, Internet giants faced a backlash over the spread of 'false news' on their platforms, prompting them to introduce changes to their policies.

Google will change its policy to prevent websites that misrepresent content from using its AdSense advertising network. Facebook updated its advertising policies to spell out that its ban on deceptive and misleading content applies to fake news. In the process, this can be seen as strengthening the role of intermediaries as *de facto* content regulators. *The issue of fake news and filter bubbles is explored in more detail on page 6.*

On a separate note, 40 US Internet companies, including Amazon, Facebook, Google, and Twitter, have sent the President-elect, Donald Trump, a list of policy priorities, from promoting strong encryption, to maintaining liability protection from content that users share on their platforms. While some of the priorities are aligned to Trump's position, others differ substantively, as our analysis of Trump's position on key issues shows.

This also marks the first contact between the US President-elect and Silicon Valley. All eyes will be on relations between the two, and on US digital policy developments as they unfold.

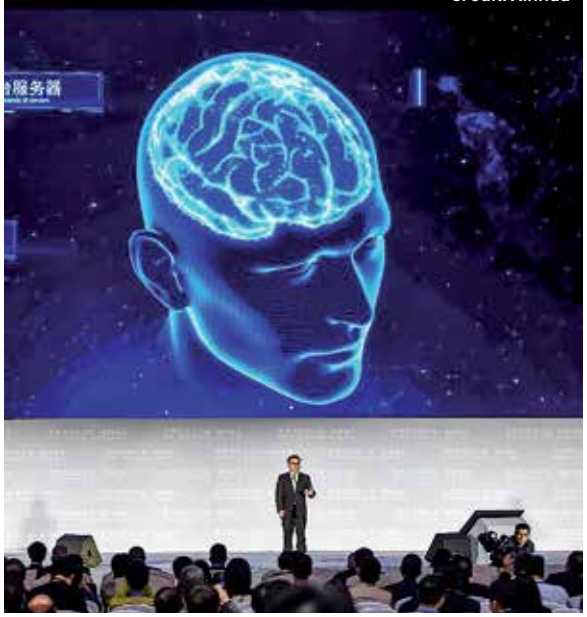
2. LOCALISATION OF DATA UNDER FOCUS

The storage of users' data within national borders - often referred to as data localisation - is not a new phenomenon. In the past few years, stricter privacy rules and taxation concerns have driven an increasing number of Silicon Valley companies to look across the pond for the storage of European users' data.

Other reasons, most notably to have direct access to users' data for the purposes of implementing content regulation, have driven a few other countries, including Russia and China, to change their laws in this direction.

Continued on page 3

A Baidu representative introduces artificial intelligence (AI) technology at the 3rd World Internet Conference (WIC) in Wuzhen, China, on 16 November. Other updates from the WIC are on page 6.
Credit: Xinhua



IN THIS ISSUE

Published on 29 November 2016, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Stephanie Borg Psaila, Jovan Kurbalija, Marilia Maciel, Aye Mya Nyein, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatovic, Diplo's CreativeLab | The Brazilian version in Portuguese is available at dw.giplatform.org/newsletter | In addition to the *Geneva Digital Watch* newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (dw.giplatform.org) and join discussions on the last Tuesday of every month online, at local hubs, or at the Geneva Internet Platform (dw.giplatform.org/briefings) | Send your comments to digitalwatch@diplomacy.edu

GENEVA DIGITAL DEVELOPMENTS

Geneva Peace Week

During Geneva Peace Week (7-11 November), non-governmental and international organisations in Geneva organised a total of 52 events with 'peace' as the overarching theme. Two events focused on digital technologies. The session by the Geneva International Centre for Humanitarian Demining, GIS for Peace, on 7 November, brought together international experts working in the field of geographic information systems to discuss how such systems can be used to promote peace and security through peace-building maps and satellite imagery. The GIP's session Competence Building for Cyberpeace, on 9 November, addressed the competences that are needed among individuals, international organisations, governments, and the private sector to build and maintain peace in cyberspace. The session also discussed the results of DiploFoundation's 2016 study on *Cybersecurity Competence Building* Trends.

Geneva Trialogue on Knowledge and the SDGs

The Geneva Trialogue on Knowledge and the SDGs, organised by the University of Geneva on 15 November, brought together international organisations, private sector representatives, and academics to discuss how to collaborate in the progress towards the sustainable development goals (SDGs) in the digital era. There was a focus on online education, e-learning, and massive open online courses (MOOCs), as well as the use of digital technologies in humanitarian situations. Furthermore, the event extensively discussed (big) data, and launched the GVA DATA initiative, a one-stop portal containing the largest collection of published data and information from UN agencies, international organisations, and NGOs based in Geneva.

WTO Council for Trade in Goods meeting

During the World Trade Organization (WTO) Council for Trade in Goods meeting, on 17 November, China and Pakistan proposed working on promoting and facilitating cross-border trade in goods enabled by the Internet. More than 20 countries participated in the debate, bringing in a wider range of e-commerce-related issues: consumer protection, data privacy, and intellectual property rights. *More on page 5.*

Our Internet: Can the Internet remain open, secure, trustworthy, and inclusive?

A panel discussion entitled Our Internet: Can the Internet remain open, secure, trustworthy, and inclusive? on 22 November, organised by the Permanent Mission of Canada and the Centre for International Governance Innovation (CIGI), addressed the outcomes and recommendations of *One Internet*, a report by the Global Commission on Internet Governance. The report was presented by Carl Bildt, Chair of the Commission and former Swedish Prime Minister, and Commission members Latha Reddy and Eileen Donahoe. The presentation was followed by a discussion, which addressed a wide range of Internet governance (IG) issues and concerns. Recurring topics were the threat of Internet fragmentation, the opportunities and challenges of the multistakeholder governance model, and the need to bridge gaps between sectors.

Towards a Secure Cyberspace via Regional Cooperation

Towards a Secure Cyberspace via Regional Cooperation is the theme of a luncheon event on 30 November, organised by the GIP and the Federal Department of Foreign Affairs of Switzerland, on the occasion of the second meeting of the 2016-2017 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). A full report will be available on the event webpage.

DIGITAL POLICY PRACTITIONERS JOIN THE GIP AS SENIOR FELLOWS

Markus Kummer

Mr Markus Kummer and Prof. Rolf H. Weber joined the GIP as Senior Digital Policy Fellows as of 1 November.

More than 50% of global digital policy is addressed in Geneva, which hosts 35 international organisations, hundreds of NGOs, and more than 200 diplomatic missions and representation offices. The senior fellows will further the work of the GIP by engaging these digital actors in Geneva.

Mr Kummer, ICANN Board Member, was the Internet Society's Senior Vice President until 2014. Prior to that, he worked for the United Nations, first as Executive Coordinator of the Working Group on Internet Governance (WGIG) and subsequently of the Secretariat of the Internet Governance Forum (IGF).

Prof. Weber was ordinary Professor for Civil, Commercial and European Law at the University of Zurich, Switzerland from 1995 to 2016, and permanent Visiting Professor at the Law Faculty of Hong Kong University, Hong Kong from 2000 to 2015. He was a founding member of the Global Internet Governance Academic Network (GigaNet) and of the European Dialogue on Internet Governance (EuroDIG).

Rolf H. Weber

The fellows will be involved in GIP programmes and related research, participate in the delivery of courses and training programmes, and interact with a wide variety of stakeholders.

Learn more about the appointments and the Geneva Digital Fellowship.

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

DIGITAL POLICY TRENDS IN NOVEMBER

Continued from page 1

Earlier this month, Russia blocked professional networking site LinkedIn from operating in the country, after breaching Information Law No. 242-FZ which requires data to be stored on local servers as of September 2015. The fact that the site was blocked sent clear messages from authorities that non-compliance will lead to suspension of service in the country.

The implications of data localisation are varied. The practice places data within physical reach of authorities. It facilitates the implementation of content regulation, investigations, and protectionist economic policies - despite being often controversial - as authorities have local control over data servers.

Legally, however, it is perhaps one less headache, as companies would then have to deal directly with one local law. Migration of data is more challenging, and so is the legal certainty surrounding new rules, especially when authorities start enforcing them. At the same time, this spells more business for content delivery and data storage providers.

3. MAKING THE IOT MORE SECURE

Last month's cyber-attacks showed that smart devices, such as cameras, camcorders, watches, and other 'connected' devices, can be used to launch a wide-scale attack. Following the attacks, companies are looking at ways to make devices more secure. Cisco, for example, launched a device-certification program allowing only devices that are deemed secure to access its networks.

The emerging question will be how to ensure that devices are secure and that vulnerabilities are patched. Following last month's initiative launched by the US National Telecommunications and Information Administration (NTIA), experts have asked for regulations to impose minimum security standards on manufacturers. US Congressional members, however, are calling for self-regulation, arguing that IoT security is a global problem and not solely a national one.

Other sectors have shown us that self- and co-regulation can be an effective solution. In the light of the faced-paced nature of cybercrime, however, timely developments will be crucial.

4. ZERO-RATING: TO CHARGE OR NOT TO CHARGE?

The debate over zero-rating practices, which was recently under focus after Facebook revealed its intention of launching Free Basics in the USA, was reignited again in other parts of the world.

In Canada, zero-rating plans came under scrutiny during a public consultation set up to discuss differential pricing practices. The aim was not only to discuss specific cases of zero-rating practices - which enables customers to access a number of services without counting towards their monthly data caps - but to look at wider policy implications. Similarly, in the UK, the debate was stirred up again after a mobile telecom operator introduced a zero-rating data plan.

Zero-rated practices have been debated in many countries, both developing and developed. The arguments often depend on the country's economy, the Internet usage rates, and the users' ability to afford an Internet connection.

In developing countries, one of the main arguments comes from an Internet rights perspective: it is to a user's advantage to have limited access to some Internet services, rather than no access at all. The counter-argument is that in undeveloped markets, the user is disempowered and disillusioned through partial access.

In developed countries, as we have seen in the USA, zero-rating services present stronger arguments for consumer choice and undue competition. Canada's public consultations, in fact, have sought the public's views on whether the preferential treatment arising from zero-rating practices is undue or unreasonable.

Despite these distinct arguments, the regulatory effects will yield the same options: allowing such practices, perhaps on a case-by-case basis, or prohibiting the practice in favour of stronger net neutrality principles.

The debate is expected to continue during the upcoming IGF. *Turn to page 7 to learn about our activities at the IGF.*

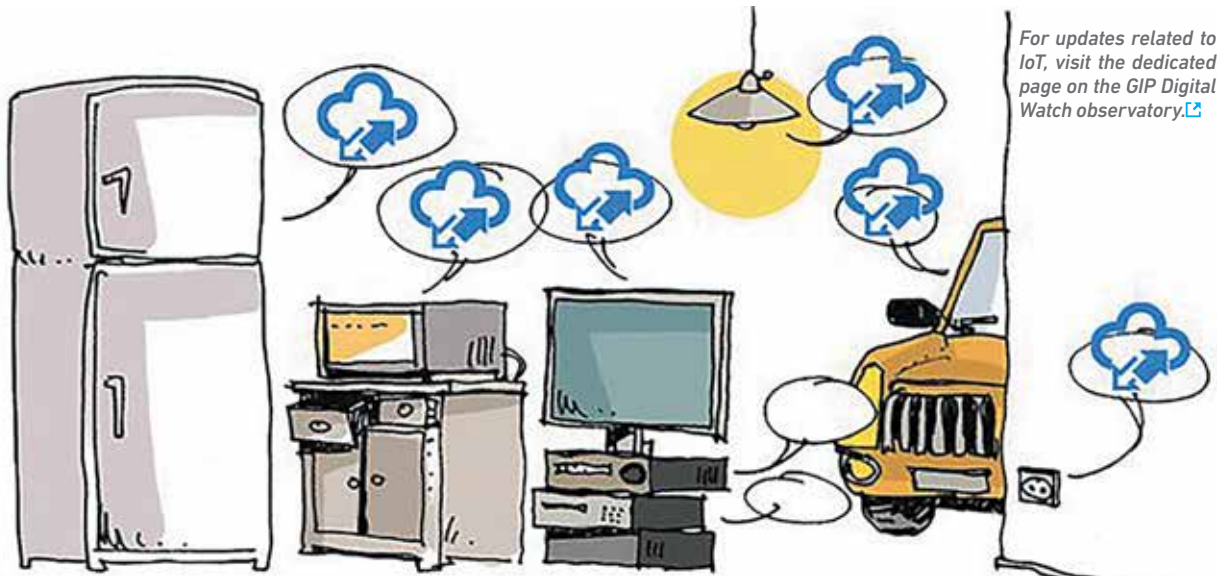
5. UN GGE MEETS AGAIN

The second session of the UN GGE takes place from 28 November to 2 December. The group has been tasked with studying existing and potential cyberthreats, and possible cooperative measures to address them.

Former working groups can be credited with two main achievements: outlining the global cybersecurity agenda, and introducing the principle that international law applies to the digital space.

The GIP's discussion on 30 November, on the work of regional organisations in cybersecurity, the interplay with the GGE, and the organisations' role in the universalisation and operationalisation of the group's work, will be timely.

Turn to pages 4–5 for more digital policy developments in November.



For updates related to IoT, visit the dedicated page on the GIP Digital Watch observatory.

DIGITAL POLICY: DEVELOPMENTS IN NOVEMBER

Global IG Architecture

same relevance

The *Wuzhen Report*, adopted after the 3rd WIC this month (16-18 November, Wuzhen), referred to five future trends in IG: developing countries will maintain momentum while digital dividends will continue to increasingly become available to everyone; cultural diversity will become more important; countries will agree on more international rules that respect sovereignty; multilateral and 'multi-party' participation will become the norm; international cooperation on cyberspace and Internet governance will be among the 'most popular' topics. *More on page 6.*

Preparations for this year's IGF are well under way, as stakeholders prepare to meet in Guadalajara on 6–9 December. The call for nominations for members of the 2017 Multistakeholder Advisory Group (MAG) has been launched; names of nominees are to be submitted by 16 December.

Sustainable development

same relevance

The ITU's *Measuring the Information Society Report 2016* refers to the role of ICTs in monitoring the SDGs, and looks at the 6 of 230 indicators that are explicitly related to ICTs. While there is substantive data available to measure ICT infrastructure and adoption, data on other topics, such as ICTs in education, skills, and gender equality, are often less substantial.

The Republic of Korea tops the global ICT Development Index (IDI) for a second straight year.

Security

increasing relevance

The Council of Europe marked the 15th anniversary of the Convention on Cybercrime during the Octopus Conference (16-18 November, Strasbourg). The conference recognised that while cybercrime is increasing, attacks against critical infrastructure, fraud, hate speech, and terrorist activities were regarded as major threats. *Turn to page 8 to test your knowledge of cybersecurity.*

China has adopted a cybersecurity law to counter cyberthreats, such as hacking and terrorism. The main criticism of the law is that it could shut foreign companies out of various sectors in China, due to requirements such as security reviews and data storage on Chinese servers, and would affect online freedom.

A direct secure voice communication line connecting the Kremlin and the White House, established as part of the 2013 cyber-agreement between Russia and the USA, was activated by the US government on 31 October, *The Washington Post* reported. According to its source, the Russian party was asked to stop its cyber-activities related to undermining US elections.

The UK has approved its new National Cyber Security Strategy 2016 to 2021 built around three main pillars: to defend its infrastructure, deter criminals, and develop cyber-capabilities.

In the light of recent cyber-attacks involving IoT devices, experts in the USA asked for governmental intervention through regulations and public policy; Members of Congress noted that that it might be more appropriate for the industry to develop best practices, as IoT security is a global issue.

Privacy & other human rights

same relevance

The UK Parliament has adopted the controversial Investigatory Powers Bill, also known as the Snoopers' Charter. Internet service providers (ISPs) will be obliged to retain browser history and make it available to the courts on request; companies providing online services will be required to decrypt user data on demand. The draft law has been criticised as intrusive to privacy and described as disproportionate by the UN Special Rapporteur on Privacy.

Turkey blocked access to social media websites due to civil unrest. The country's Prime Minister acknowledged that 'from time to time for security reasons they can use such measures.'

The EU-US Privacy Shield was challenged a second time by a French privacy advocacy group over the alleged inadequacy of the framework. This is the second legal challenge for the new framework.

Internet freedom declined for a sixth consecutive year, the *Freedom of the Net* report concluded, while new statistics revealed that almost half of US Internet users have experienced online harassment, abuse, or invasion of privacy.

Infrastructure

increasing relevance

China has built a 712-km quantum communication line between Shanghai and Hefei, making it the longest quantum network in use. It is believed that the highly secure communication line makes it impossible to wiretap, intercept, or crack the information transmitted by it.

Among the outcomes of the World Telecommunication Standardization Assembly 2016 (WTSA-16) is a call for ITU's standardisation arm to expand its study related to smart 5G systems. Meanwhile, the Groupe Speciale Mobile Association (GSMA) has called on governments and regulators around the world to commit to supporting the needs of 5G spectrum allocation. The association believes that a global agreement on spectrum allocation is a precondition to successful 5G uptake.

The global cloud computing market is predicted to reach $146 billion in 2017; however, businesses are still reluctant to adopt cloud computing due to security concerns.

The Internet Architecture Board (IAB) is encouraging standards-developing organisations to ensure that networking standards support IPv6. Meanwhile, a survey showed differences in how various ISPs deploy IPv6.

Net neutrality

same relevance

The Canadian Radio-television and Telecommunications Commission (CRTC) launched a hearing on differential pricing practices related to Internet data plans. This came after complaints over zero-rating practices introduced by an ISP. In the UK, a similar debate is likely to resurface after a major telecom operator introduced a zero-rating data plan. In Morocco, the Telecommunications Regulatory National Agency (ANRT) has lifted the ban it had previously imposed on voice over Internet protocol (VoIP) services.

E-commerce & Internet economy

increasing relevance

China and Pakistan have introduced a potential 'pragmatic solution' for e-commerce, during the WTO Goods Council meeting, by proposing to work on the promotion and facilitation of cross-border trade in goods enabled by the Internet. This would enable e-commerce to be addressed within the existing mandate, leading to a successful 2017 Ministerial Meeting. China also proposed a seminar on e-commerce and trade in goods. Pakistan said it was ready to engage with other WTO members to continue work on e-commerce.

Starting 1 December, India will impose a 15% service tax on content from overseas service providers. Google is expected to reach a tax settlement with the Indonesian government to pay back-taxes and fines.

The Swiss Federal Department of Finance (FDF) outlined its plans for innovative financial technologies. The Federal Council called for an easing of the regulatory framework for fintech providers.

Senegal has announced the introduction of a virtual currency into the mainstream monetary system. After Tunisia adopted the virtual currency eDinar early last year, the Banque Régionale de Marchés (BRM) partnered with blockchain startup eCurrency Mint to provide a virtual currency in the West African Economic and Monetary Union (WAEMU). Meanwhile, Sweden's Riksbank, the oldest central bank in the world, is studying the possibility of issuing e-krona. The digital currency is not intended to replace cash but to complement it.

Jurisdiction & legal issues

same relevance

Russia has blocked LinkedIn over the social network's failure to move Russian users' data to servers located in Russia, which amounts to a violation of a Russian law requiring all online sites to store personal data on national servers. The decision was issued by Russia's communications regulator, Roskomnadzor, following a decision from the Moscow city court. *More on page 1.*

Following the US Presidential election, Internet companies Google, Facebook, and Twitter faced criticism regarding the spread of 'false information' on their platforms, which may have convinced voters to vote for the Republican candidate. The topic was also addressed during the 3rd World Internet Conference. The Cyberspace Administration of China said that false news is a sign that 'cyberspace has become dangerous and unwieldy'. *More on page 7.*

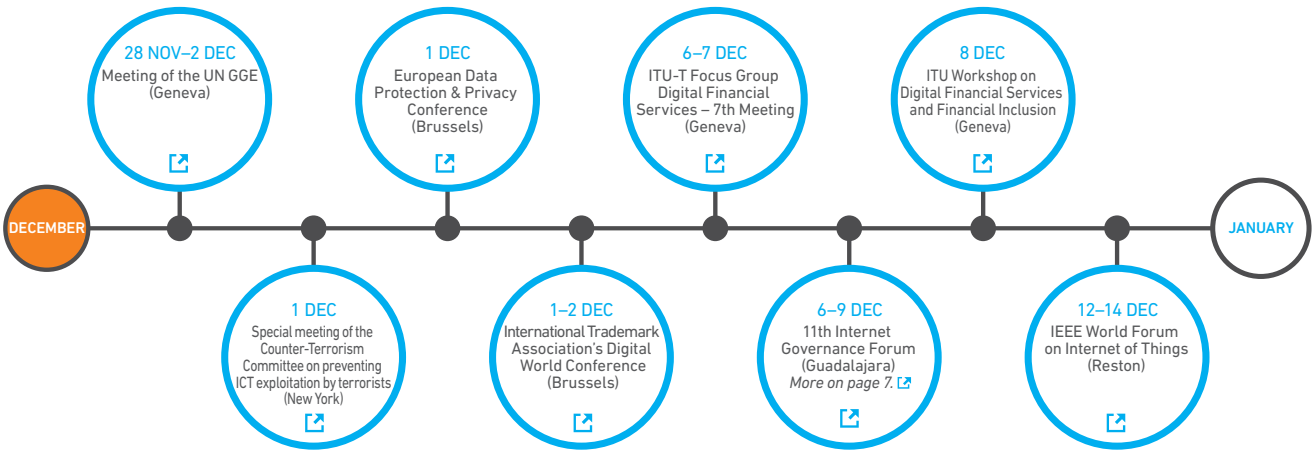
Indonesia has passed new legislation allowing people who are acquitted in court cases to apply for the 'right to be forgotten'. Indonesia's version of this right is said to 'go beyond European-style rules covering search results', as it requires web administrators to remove the actual content.

IANA Transition

same relevance

The Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability), which met during the Internet Corporation for Assigned Names and Numbers (ICANN's) 57th public meeting, made progress on several areas related to ICANN accountability. It agreed on a set of Draft Supplementary Rules for the Independent Review Process; it developed a set of questions to identify existing accountability mechanisms within ICANN's supporting organisations and advisory committees; it developed an initial set of guidelines for bringing forward any proposed Board removal actions; and it discussed a comprehensive set of recommendations to enhance ICANN's transparency policies.

AHEAD IN DECEMBER



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

JURISDICTION AND THE CHALLENGES OF A BORDERLESS DIGITAL WORLD

In search for justice on the Internet, people worldwide are bringing their cases to court. Courts judge and increasingly shape the rules for online spaces. The court judgments often have a regional and even global impact.

The judgments on the right to be forgotten, the invalidation of the Safe Harbour Framework, and rulings involving the sharing economy (Uber, Airbnb) are notable examples of how policy is being shaped by the courts.

What is striking in these cases is that while traditional jurisdiction remains territorially based, the outcomes of these decisions cut across national borders when it comes to applying them to the online environment. An example of these extraterritorial consequences can be found in the context of WhatsApp being blocked in Brazil, in December 2015, following a court order. This decision was quickly reverted by the appeals court; the consequences, however, were significant. Since infrastructure does not necessarily conform to state borders, WhatsApp users in neighbouring countries, such as Argentina and Chile, faced difficulties in accessing the platform.

In this complex and challenging context, initiatives such as the Geneva Internet Dispute Resolution Policies 1.0 (GIDRP 1.0) project, developed by the University of Geneva, could make many contributions to debates on jurisdiction.

The project's recently launched website includes the work of a team of investigators dedicated to advancing policy proposals on pressing issues that can arise in the course of legal disputes relating to the Internet, such as the criteria to fix jurisdiction of a national court, the possibility to structure an alternative dispute resolution system for Internet-related disputes, and ways in which immunities should apply in the online environment.

The WIC in Wuzhen, China (18-21 November 2016) hosted a Smart Court Forum on the rule of law in cyberspace. The forum addressed many issues related to the digitalisation of the Chinese legal system. Beijing-based itslaw.com presented the first Chinese intellegent legal robot, which uses AI to serve as counsel to companies. The question of jurisdiction was raised in the context of developing a stable international legal framework for the growth of e-commerce.

The tension between the cross-border Internet and national jurisdictions was also tackled recently during the Internet and Jurisdiction Conference (I&J) in Paris, France (14-16 November 2016). Discussions clustered around three parallel workstreams: data, content, and domain names.

The first examined cross-border requests for access to personal data. How to harmonise them with data protection was discussed, as well as the criteria that could possibly be used to fix jurisdiction, such as nationality or residency of the user, for example. The second workstream discussed procedures to enable authorised public authorities to request the removal of illegal content hosted in foreign countries. The third focused on cross-border requests for domain name suspension, which usually aim to make a website unavailable, based on the alleged illegality of its content or activities. A background paper produced by the I&J as an input to the conference proposed questions to be discussed in each of the workstreams.

A view that emerged from the workstreams was that a common lexicon that facilitates dialogue among stakeholders is necessary, and that dialogue on jurisdiction needs to include all interested actors. In addition, further dialogue, research, and financial and human resources need to be dedicated to finding solutions that could reconcile jurisdiction and the Internet.

Looking back at the World Internet Conference

'China needs to increase its voice in cyberspace' was the underlying message from the WIC. Now in its third year, the WIC is becoming one of the main Internet gatherings bringing together thousands of Chinese and foreign experts in the digital field. In conference discussions, two pillars of Chinese digital foreign policy emerged.

First, China is basing its policy on the concept of cybersovereignty. It prefers the multilateral approach to the multistakeholder approach to international digital policy. A possible third approach, hinted at in Wuzhen by the adoption of a new term – 'multi-party' – will be discussed more in the forthcoming period.

Secondly, China's main focus is on economic digital diplomacy. China needs a stable and predictable digital economic space for its export-oriented industry. At the G20 Summit (4–5 September), China positioned e-commerce prominently. In fact, both the communique released at the end of the summit, and the adopted Blueprint on Innovative Growth, emphasise the role of the digital economy and the new industrial revolution. Alibaba's Jack Ma's proposal for an Electronic World Trade Platform, welcomed by G20 leaders, is another example.

世界互联网大会
World Internet Conference
乌镇峰会 · Wuzhen Summit

IN FOCUS

POST-ELECTION CONCERNS OVER FAKE NEWS AND FILTER BUBBLES

In its aftermath of the US election, concern was raised over the spread of 'fake news', placing Internet intermediaries in the spotlight. Is fake the new real on social media?

Immediately after the US election, observers began analysing the election result, raising concerns over the role of Internet companies. The companies were criticised over the dissemination of 'fake news' through their platforms and the creation of 'filter bubbles' that may have led to the polarisation of the political debate.

The Guardian called it 'Facebook's failure', and *The Washington Post* referred to it as 'Trump's fake-news presidency'. Before election day, the question was whether Trump would win *despite* Silicon Valley - which overtly promoted Democratic candidate Hillary Clinton - and now the question has arisen whether he has won *because of* it.

Fake news can be described as deliberately created, factually incorrect stories, which are spread by outlets to promote their own interests. With the growth of social media, fake news has proliferated; it has found a platform to disseminate these stories to a massive audience. According to a recent analysis, fake news stories created more Facebook engagement than the top election stories from 19 of the main news outlets combined. On top of that, a Stanford study recently found that more than 80% of students cannot identify sponsored content from 'real' news stories.

The 'filter bubble' is another post-election buzzword, although concerns had already surfaced in recent years. Filter bubbles relate to the personalisation of online content, for example on Facebook and Google, which leads users to content that almost always reinforces their pre-existing views. The filter bubble was criticised in relation to the Brexit vote, leading German Chancellor Angela Merkel to warn against its chilling effects on 'a healthy democracy'.

According to Pew Research Center, 20% of social media users say they have changed their position on a social or political issue, and 17% say social media has helped to modify their view about a political candidate.

However, Facebook CEO Mark Zuckerberg said, 'I think the idea that fake news on Facebook, which is a very small amount of the content, influenced the election in any way - I think is a pretty crazy idea', as 'voters make decisions based on their lived experience'.

Nevertheless, both Facebook and Google have taken measures to restrict advertisements linking to fake news, although Zuckerberg insisted that 'we do not want to be arbiters of truth ourselves'.

It might indeed be likely that social media might not have been the all-explanatory theory why Donald Trump was elected, although it could be safe to assume that social media platforms did play a role among a multitude of factors.

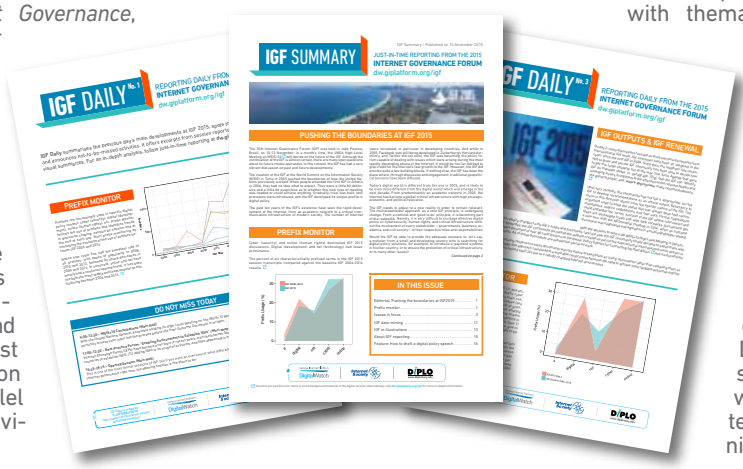
Furthermore, with so much of our 'lived experience' taking place online, especially with regard to accessing and assessing information, platforms may have the inevitable responsibility of ensuring that they are not used to disseminate false news. As Angela Merkel remarked earlier this month: 'We should not underestimate what is happening in the context of the Internet and with digitalization; this is part of our reality.' Democracy can only live up to its promise with a well-informed citizenry; informed decision-making will inevitably be affected when being exposed to false or one-sided information.

UPCOMING

WHAT TO EXPECT DURING IGF 2016

The GIP is gearing up for another packed annual IGF meeting. Close to 200 workshops on a wide range of issues - from cybersecurity to privacy, from net neutrality to e-commerce - are scheduled to take place from 6 to 9 December in Guadalajara, Mexico. The GIP is planning several workshops, the launch of the 7th edition of *An Introduction to Internet Governance*, and a get-together for alumni.

An important initiative will be to provide just-in-time reports from the IGF. With so many parallel sessions, the initiative will address the challenge faced by participants and the wider community, both at the IGF and online, to absorb the vast amount of information emanating from parallel sessions and other activities.



Workshop reports will be uploaded within a few hours on the *GIP Digital Watch* observatory, at dw.giplatform.org/igf2016, to enable readers to catch up with sessions that they missed, either due to timezones, or other parallel sessions.

The GIP will also publish a daily newsletter with thematic summaries of the previous day's discussions, and a final report rounding up the main issues. Illustrations, data analysis, and other updates will be included in the *IGF Dailies*, and on the observatory.

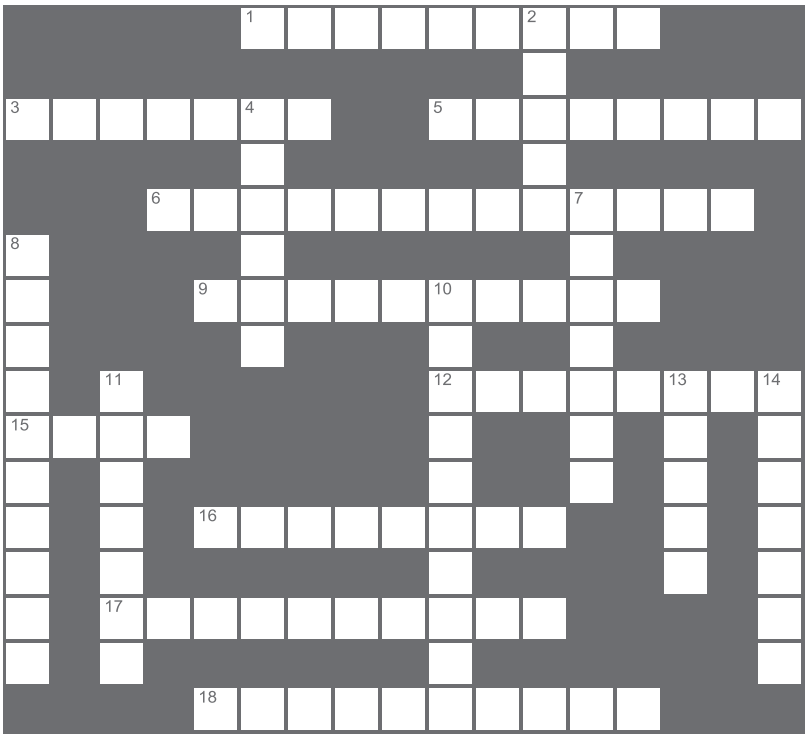
The GIP team behind this initiative consists of rapporteurs, editors, Diplo's CreativeLab, and social media experts working to bring the content closer to the community.

CROSSWORD

TEST YOUR KNOWLEDGE ON CYBERSECURITY

This month marks the 15th anniversary of the Council of Europe's Convention on Cybercrime. To date, 67 countries have signed, ratified, or been invited to accede to the convention.

Test your knowledge of the Convention on Cybercrime, of some of the most common criminal acts, and of processes related to securing the cyberspace.



Across

1 Computer _____ is the practice of collecting and analysing data contained on computer systems and computing devices during an investigation (9)

3 The name of the most popular crypto-currency (7)

5 City where the Council of Europe Convention on Cybercrime was adopted in 2001 (8)

6 A process of adjusting legal frameworks across countries to meet common standards and requirements (13)

9 The Additional Protocol of the Cybercrime Convention, which came into force in 2006, criminalises racist and _____ acts (10)

12 _____ infrastructures are vital systems on which a country's society and economy rely extensively (8)

15 Unsolicited e-mail messages used mainly for commercial promotion, and increasingly, to distribute malicious content (4)

16 The process through which the perpetrator of child sexual abuse first tries to build a relationship with the young victim (8)

17 The scrambling of electronic documents and communication into an unreadable format which can be accessed after decoding (10)

18 A type of malicious software deployed to obtain a ransom from victims (10)

Down

2 A country that has bilateral cybersecurity agreements with both the USA and Russia? (5)

4 The non-European country which has most recently ratified the Cybercrime Convention (6)

7 Name of the social media network which suspended over 200,000 accounts in the first half of 2016, for threatening or promoting terrorist acts (7)

8 A mutual legal _____ treaty (MLAT) is a bilateral agreement that facilitates the gathering and exchange of information across borders (10)

10 Politically motivated computer crime; may consist of distributed denial of service attacks, web defacement, or penetration of networks for acquiring documents or data (10)

11 Part of the web that search engines cannot access, and that is often used for black market activities (4, 3)

13 The storage of data in the _____ makes criminal investigation increasingly complex (5)

14 Country that suffered an Internet blackout due to cyberattacks in early November (7)

Across: **1** Forensics, **3** BitCoin, **5** Budapest, **6** Harmonisation, **9** Xenophobic, **12** Critical, **15** Spam, **16** Grooming, **17** Encryption, **18** Ransomware.
Down: **2** India, **4** Israel, **7** Twitter, **8** Assistance, **10** Hacktivism, **11** Dark Web, **13** Cloud, **14** Liberia.