Top digital policy developments in 2016:

A year in review

Geneva Internet Platform
DigitalWatch

Overview

The start of 2017 presents an excellent opportunity to look back and reflect on last year. The digital policy year in 2016 was marked by several important developments, including the adoption of the Privacy Shield, the successful IANA stewardship transition process, the US Presidential election, and a handful of new bilateral cybersecurity agreements. The role of the Internet and ICTs in attaining the sustainable development goals (SDGs) was a recurrent theme.

The interplay between security and privacy was in sharp focus during the Apple/FBI case, which unfolded in the first few months of the year. Although the case was settled before the courts had the opportunity to consider and rule on the issue, the main dilemmas remained unresolved and are likely to resurface.

Other updates demonstrated the vulnerabilities of certain systems, and how security needs to be prioritised in the coming months. As new technologies are tried, tested, and developed, cybercriminals continue to take advantage of weaknesses, exploiting them for their own financial gain.

In 2016, courts played a growing role in shaping digital policy globally. A significant number of court judgments left their mark on various issues. Others served to extend the jurisdiction arm to rule over cases with broad cross-border elements.

This document sums up the top 20 digital policy developments for 2016. The overview is based on digital policy developments which expert curators from the Geneva Internet Platform (GIP) followed every month. Throughout the year, the curators looked at hundreds of developments, reporting on them in a neutral way for the *GIP Digital Watch* observatory and monthly newsletters, and analysing them during the GIP's regular Internet governance discussions and other digital policy events.

Our reflections will continue throughout January 2017 with further analysis on our blog roll↗ and observatory,↗ culminating on 31 January with our first GIP briefing of the year.↗ We invite you to join us in the process.

Comments are welcome. Get in touch via gip@diplomacy.edu

Published on 10 January 2017 by the Geneva Internet Platform and DiploFoundation.
Download the digital version from dig.watch/2016
The digital version contains links to additional resources. Click on the resource icon ↗ to access more details.
Click on the observatory icon ● to learn more about each issue.

#1 Cyberpeace: between Cold War and *détente*

The facts

The end of 2016 was marked by cyber tension between the USA and Russia. The US intelligence community accused Russia of using cyber to interfere with the US elections. and on 29 December, the US President ordered a number of actions in response, sanctioning Russian intelligence officials, expelling 35 Russian diplomats, and shutting down 2 Russian facilities in the USA. It remains to be seen if the growing tension will lead towards a cyber-Cold War or a *détente.*

The US-Russian tension is the latest and most visible aspect of the securitisation of cyberspace. More countries are considering cyber as a vital part of national security. Countries are developing their cyber capabilities and strategies. In June, NATO declared cyberspace as an operational domain.

Since most conflicts have a cyber dimension, the decision was aimed at enabling NATO to better coordinate efforts during potential cyberattacks, and to develop capabilities to protect member countries' cyber networks.

The year 2016 also saw many attempts to develop international cooperation in cybersecurity matters. The Organization for Security and Co-operation in Europe (OSCE) adopted the second set of cyber confidence-building measures (CBMs), while countries concluded at least 20 new bilateral agreements on cybersecurity.

The fifth UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) convened with the aim of continuing discussions on enhancing cooperation in the cybersecurity field.

Why is this significant?

Cyber stability affects the critical infrastructure of societies worldwide. Countries have to find ways and means to protect cyberspace. Given their interdependence on cyberspace, the main efforts should be directed at reducing risks from beyond national territory, and developing norms that could regulate a potential cyber conflicts.

The UN GGE reiterated that international law applies to cyberspace. The next main challenge is to address how international law applies to cyberspace, given all its specificities. For example, how can states use the right to self-defence, as prescribed in the UN Chapter, in the case of cyber conflicts? Another main question relates to whether and how can states can be held responsible for cyber attacks originating from computer facilities on their territories.

Insufficient norms and procedures to address conflicts could lead towards instability of cyberspace, which would have a considerable impact on the growth of the Internet and on economic developments.

Which issues are affected?

Cybersecurity | Cybercrime | Critical infrastructure | Cyberconflict

Other cyberspace-related developments

- **10 March.** The OSCE's 57 participating states agree to expand the organisation's list of CBMs. Among other measures, states will 'encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information', on a voluntary basis. The new measures build on the first round of CBMs adopted in 2013.
- **24 June.** Microsoft publishes a white paper on cybersecurity norms for states and the global ICT industry. The paper proposes a set of offensive, defensive, and industry norms for both governments and the industry.
- **8 July.** Through the Cyber Defence Pledge, NATO countries pledge to develop capabilities, allocate adequate resources, and reinforce multistakeholder interaction, as well as improve the understanding of threats, enhance skills and awareness, foster cyber education, and expedite the implementation of cyber defence commitments.
- **29 August.** The fifth UN GGE starts its work. Building on previous work, the group is expected to study existing and potential threats in the sphere of information security and possible cooperative measures to address them; how international law applies to the use of ICTs by states; and norms, rules and principles of responsible behaviour of states, CBMs, and capacity-building.
- **6 September.** G20 leaders stress the role of the digital economy for growth and development and the new industrial revolution.
- **16 October.** Leaders of BRICS countries recognises the 'leading role of states' in ensuring the stability and security in the use of ICTs, and reaffirm that the Internet is a global resource.

Resources
Read more about the work of the UN GGE, its membership, and modus operandi, on our dedicated page on the *GIP Digital Watch* observatory.

#2 Apple/FBI case brings privacy, security, encryption, and surveillance into sharper focus

The facts

On 17 February, a Californian court ordered Apple to assist the FBI with unlocking data from a cell phone belonging to one of the San Bernardino terrorists. Apple was asked to provide software that would 'bypass or disable the auto-erase function', which would allow the agency to try to open the phone by submitting multiple passwords.

Apple objected to the court's request, and received significant support from other tech companies. It argued that in helping the FBI, it would be weakening the phone's security, and endangering the privacy rights of millions of users. A day before the scheduled court hearing, the US government (USG) declared a third party had found a way to unlock the phone. Who the third party was, or how it managed to access the data, was never revealed, yet the case triggered heated debates on many unresolved issues.

Why is this significant?

The case brought the interplay between privacy and security into sharper focus. On the one hand, access to the data would have allowed the FBI to carry on its investigations into a case which took the lives of innocent people. On the other hand, facilitating access would have meant potentially weakening the phone's security and endangering the rights of millions of users – a risk which Apple strongly refused to take.

The main dilemma is whether digital policy can achieve a win-win solution (more security and more privacy), or a win-lose solution (either more security or more privacy).

The case also raised other questions related to the responsibilities of stakeholders. Should the private sector be obliged to weaken the encryption of its products, when governments so request? At which point are authorities considered to have crossed a red line in seeking assistance from the private sector?If users are left to their own devices to ensure their safety, how can less skilful users also be adequately protected?

While the case was resolved outside of the courts, the main issues are still as valid and as unresolved as they were in February 2016. The issues are likely to surface again, whether it is through new court cases which will push judges to rule, or through circumstances which will force governments and the Internet industry to push their cases further.

Which issues are affected?

Privacy and data protection | Cybercrime | Cybersecurity | Encryption | Other economic issues

A timeline of developments

- 17 February. A Californian court orders Apple to assist the FBI in unlocking an iPhone belonging to one of the San Bernardino terrorists.
- 1 March. New York judge: The US Department of Justice (DoJ) cannot force Apple to provide access.
- 1 March. Apple testifies before Congress and argues that a system which can break encryption would weaken the security of every iPhone.
- 4 March. Apple receives significant support from tech companies. UN High Commissioner for Human Rights: Case 'could have extremely damaging implications for the human rights of many millions of people...'
- 8 March. The US DoJ files a request to overturn the New York court ruling.
- 10 March. The US DoJ states that the request is not an 'undue burden', as the order is limited to one specific case.
- 16 March. Apple says the US Constitution forbids it to comply with the court order.
- 22 March. The USG declares it may have found a way to unlock the phone without Apple's help.
- 29 March. The USG drops its case against Apple, after obtaining the 'assistance of a third party'.
- 31 March. The American Civil Liberties Union identifies 63 court orders in which authorities requested companies to help unlock phones.
- 8 April. In a different case, the USG tells a New York Court it still needs Apple's help to access data on an iPhone belonging to a drug dealer.
- 13 April. The FBI is thought to have been aided by professional hackers to unlock the San Bernardino phone.
- 27 April. The FBI declares it cannot reveal how the phone was hacked, as it does not know how the tool works.
- 15 September. A Cambridge University researcher shows how iPhone data could have been accessed.
- 16 September. News organisations file a lawsuit against the FBI to reveal who the 'third party' was.

Resources

Read Diplo's five-part *Socratic Dialogue* on the core concepts and underlying assumptions of the case, played out by three fictitious characters: Privarius, Securium, and Commercias.

#3 Tech companies enhance encryption for users

The facts

In the aftermath of the Apple/FBI controversy, more tech companies began introducing end-to-end encryption for their services. Where services were already encrypted, companies sought to enhance or tighten encryption with the aim of protecting users' communications and their right to privacy.

Apple, Google, Facebook, Snapchat, WhatsApp, and WordPress were among the companies that readily integrated or enhanced encrypted services.

Why is this significant?

The Apple/FBI controversy was triggered by a court ruling which obliged a private company to weaken the security of its product. This was at the request of a government authority. Had the case been allowed to continue, a possible final ruling in the FBI's favour could have set an unparalleled precedent.

Tech companies responded to the controversy in a number of ways. Major companies showed their strong support for Apple throughout the proceedings.

They also sought to introduce or tighten the security of their services to ensure that private communications remained between the sender and the recipient only.

In doing so, the private sector showed it had an important stake in the protection of users' rights. Although this was to the users' benefits, important considerations nonetheless emerged.

To what extent can the private sector be expected to protect users' rights, when the sector is justifiably driven by commercial interests? Should devices be impermeable or undecryptable, or should weaker encryption be allowed in the interests of security, public safety, and justice?

Stakeholders are likely to have to face these open issues again.

Which issues are affected?

Privacy and data protection | Cybersecurity | Encryption | Telecommunications infrastructure

The main updates

- **15 March.** Several Internet companies including Facebook, Google, and Snapchat, announce their plans to enhance encryption for their services, in the context of the clash over encryption between Apple and the FBI.
- **16 March.** Google announces that over 75% of requests to its servers are using encrypted channels. The company introduces a new section in its Transparency Report dedicated to reporting on the use of encryption on its own websites and across the web.
- **5 April.** WhatsApp introduces full end-to-end encryption for its service. Photos, videos, files, voice messages, and group text messages are now also encrypted.
- **8 April.** WordPress introduces encryption for all custom domains hosted on WordPress.com.
- **3 May.** Google enables HTTPS for all blogs on blogspot.com. An HTTPS Redirect setting is also introduced; with this option enabled, visitors going to the HTTP version of a blog will be automatically redirected to its HTTPS version.
- **18 May.** Google's new applications Allo and Duo to have end-to-end encryption.
- **15 June.** Apple announces that as of 1 January 2017, all applications in its App Store will need to have the App Transport Security (ATS) feature enabled. ATS forces an application to connect to web services over an HTTPS connection, thus encrypting user data while in transit.
- **2 August.** Google states that 97% of connections to YouTube and 93% of connections to Google Calendar, are encrypted. The company intends to gradually phase out insecure connections.
- **10 August.** Netflix explains its move towards encrypting video streams; the majority of streaming sessions are expected to be using Transport Layer Security (TLS) encryption by the end of 2016.
- **9 September.** From January 2017, the Chrome browser will start flagging non-HTTPS websites as 'not secure'. The gradual introduction of the label is aimed at educating users about the risks of unencrypted websites, while avoiding 'warning fatigue' which can occur when a user gets used to warnings and overlooks them.
- **1 October.** VeriSign announces that it has doubled the size of the cryptographic key that generates the Domain Name System Security Extensions. The transition, conducted by VeriSign in cooperation with ICANN, IANA, and the US National Telecommunications and Information Administration (NTIA), aims to strengthen the zone signing key for the DNS root zone.
- **5 October.** Facebook introduces 'secret conversations for Messenger chats, allowing users to opt in for encrypted end-to-end conversations.'

#4 Initiatives and measures are introduced to combat violent extremism online

The facts

In 2016, terrorists made increasing use of the Internet for spread of terrorist propaganda and violent extremism. Terrorists have been using encryption and the dark web, as well as virtual private networks (VPNs) and a wide range of online tools.

The private sector took the initiative of introducing measures, such as deleting social media accounts, filtering content, establishing policies for the removal of content, and directing searches for extremist content to anti-terrorist content. However, intermediaries also faced several court cases over their alleged failure to act or their provision of material support to terrorists.

The authorities undertook new initiatives, from collaborating with the industry and setting up dedicated task forces, to cooperating with civil society to engage critically on online forums with the aim of challenging online content. The United Nations Security Council tasked the Counter-Terrorism Committee (CTC) to present a proposal for a comprehensive international framework by 30 April 2017.

An initial report on the findings of a joint project on *Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes,* referred to an emerging policy framework that is shaping private and public action. The report was presented by ICT4Peace and the UN Counter Terrorism Executive Directorate (UNCTED) during a Special Meeting of the CTC in December. Leaders of the G7 referred to the need for cooperation with the private sector, civil society, and communities in putting a stop to terrorists' illegal activities online; leaders of BRICS countries – Brazil, Russia, India, China, and South Africa – also emphasised the need to enhance international cooperation against terrorist and criminal misuse of ICTs.

Why is this significant?

The need to tackle extremist content has become a recurrent theme in international politics. Since most extremist and terrorist content is distributed online, this is also a cause for concern for Internet companies.

A main development is characterised by Silicon Valley companies increasingly cooperating with governments in the fight against online terrorism and extremist content. In 2016, efforts were kick-started by a 'technological brainstorming meeting', held between the USG and tech companies to discuss cooperation. Industry players also collaborated on automatic take-down of content, reportedly based on 'hashing' technology – the same tools used in combatting child sexual abuse material.

At the same time, the private sector was under significant pressure, both from authorities, and from the families of victims who instituted court action over the intermediaries' failure to act. On the one hand, families of victims and security proponents claim that intermediaries are not doing enough; on the other, human rights activists claim that certain measures may stifle freedom of expression. Given that the spread of online radicalisation is taking place at a very fast rate, the question of whether intermediaries are doing enough to counter such content is likely to persist.

Which issues are affected?

Content policy | Cybercrime | Freedom of expression | Intermediaries | Jurisdiction

The main cases

Intermediaries were faced with various court cases over their alleged failure to act:

- **17 June.** The father of a victim of the November 2015 Paris attackas accuses Google, Facebook, and Twitter of offering 'material support' to terrorists. Tech companies respond by citing their policies against extremist materials and the US law stipulating that Internet companies 'are generally exempt from liability for the materials users post on their networks'.
- **12 July.** The families of US victims in a Palestinian attack sue Facebook for 'knowingly provid[ing] material support and resources to Hamas' and 'facilitat[ing] this terrorist group's ability to communicate, recruit members, plan and carry out attacks, and strike fear in its enemies.'
- **10 August.** A California court dismisses claims that Twitter provided 'material support' to terrorists. The two widows of government contractors killed in Jordan, in November 2015, allege that the social network 'knowingly permitted... ISIS to use its social network as a tool for spreading extremist propaganda, raising funds, and attracting new recruits.' However, they fail to explain how Twitter's provision of accounts to ISIS led to the shooting.
- **21 December.** The families of some of the victims of the Orlando Pulse nightclub shooting, in June 2016, sue Google, Twitter, and Facebook, over their alleged role in the radicalisation of the shooter. According to the lawsuit, 'without... Twitter, Facebook, and Google (YouTube), the explosive growth of ISIS over the last few years into the most feared terrorist group in the world would not have been possible.' The lawsuit also claims that the tech companies 'profit from ISIS postings through advertising revenue'.

#5 Cybercrime increasingly exploits vulnerabilities

The facts

Cybercrime featured often in news headlines throughout the year, underlining the vulnerabilities of cyberspace. Targets ranged from individuals, Internet companies, and universities to public institutions and political organisations.

Yahoo! acknowledged that two cyber-attacks in 2013 and 2014 resulted in the theft of massive amounts of user account information. Over 1 billion accounts were affected in 2013, and around 500 million in 2014. A database of almost 33 million Twitter accounts was offered for sale through Dark web cybercrime markets, although the company argued that the credentials were not obtained through a hack of its servers. The banking and financial sectors were also on high alert after the secure SWIFT system was compromised due to a sophisticated malware that penetrated the Bangladesh central bank, resulting in a loss of over $80 million.

Zero-day flaws targeting operating systems such as Windows continued to be popular on cybercrime markets, causing concerns among experts. In August, a group of hackers revealed the software code of highly sophisticated cyberattack tools belonging to another hacking group believed to be associated with the US National Security Agency (NSA). A hack into the systems of a large crowdfunded investment fund based on blockchain technology led to a loss of an estimated $60 million.

A 2015 cyber-espionage attack against a Japanese nuclear research lab was disclosed in October 2016; it was revealed that the research information and personal data of about 1500 researchers were stolen. The hack into an e-mail server belonging to Mossack Fonseca, a Panamanian law firm and corporate service provider, led to the leak of the so-called Panama Papers, which revealed tax avoidance efforts by public officials and wealthy individuals.

In the USA, e-mails of individuals and institutions were affected by massive hacks, and the US intelligence community officially blamed the Russian government for involvement in the attacks. This was followed by sanctions towards the end of the year.

Why is this relevant?

While being only the tip of the iceberg, these examples show how the vulnerabilities of cyberspace are exploited by a wide variety of actors. While the risks of and losses from cybercrime are growing, the misuse of the Internet by politically motivated actors (states and their proxies) is increasingly dominant.

Moreover, cyber-attacks continue to increase and move from mass frauds to sophisticated attacks targeting individuals, as well as hacking particular companies or institutions. Lead technology, financial, and government institutions have also become targets of cybercrime, which shows that no one is immune. The consequences of the attacks are increasingly geo-political rather than localised.

This trend calls for increased efforts from governments, intergovernmental organisations, and private companies to work towards identifying and implementing more adequate responses. But the perspectives do not look very encouraging. While more countries are strengthening their law enforcement agencies, the general level of resources available to these agencies in developing countries remains small, mainly due to a limited political understanding of cybersecurity challenges.

With 50 parties to the treaty, the Council of Europe's Convention on Cybercrime, which celebrated its 15th anniversary (on 19 November), remains the most relevant international agreement for combating cybercrime, both in terms of guidelines for national legislation, and as a framework for capacity building and cooperation across stakeholders.

Which issues are affected?

Cybercrime | Cybersecurity | Cyberconflict | Privacy and data protection | Other economic issues

Authorities and companies' main response to threats

- **6 July.** The European Parliament adopts the Network and Information Security (NIS) directive, requiring member states to establish a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority, and to set up a cross-EU cooperation group for strategic cooperation and a CSIRT Network for operational cooperation.
- **2 November.** The UK approves its new National Cyber Security Strategy 2016 to 2021, which is built around three main pillars: to defend its infrastructure, deter criminals, and develop cyber-capabilities.
- **7 November.** China adopts a new cybersecurity law to counter cyberthreats, such as hacking and terrorism. The law enters into force on 1 June 2017. A National Cybersecurity Strategy is announced on 27 December.
- **16 November.** The US administration activates a secure voice communication line connecting the Kremlin and the White House, to prevent cyber-incidents around the US elections.
- **1 December.** The US Commission on Enhancing National Cybersecurity presents 16 recommendations in its *Report of Security and Growing Digital Economy.*

#6 DDoS attacks bring IoT security into focus

The facts

Two large attacks utilising smart devices were carried out in October. Over a million security cameras, video recorders and other IoT devices were used in distributed denial of service (DDoS) attacks on a US security researcher and a French network security provider in a first attack. In a second attack, another series of DDoS attacks against Dyn Inc., a large DNS hosting and DDoS-response provider serving top online service providers, rendered many services – including Twitter, PayPal, Reddit, and Spotify – temporarily unavailable, and slowed down Internet traffic across the globe. Nearly one million routers accessing Germany's largest telecom operator's Internet services were targeted through a third cyber-attack in late November, which was described as being part of a larger campaign targeting web-connected devices around the globe. The attack could have spread to other countries such as Brazil, the UK, and Ireland.

Why is this significant?

The attacks brought the issue of IoT security into sharper focus, as only a few manufacturers had taken active steps to ensure the safety of devices connected to the Internet.

While DDoS is not a new type of attack, the magnitude of an attack that can be achieved from millions of insecure connected devices is unprecedented.

It will be ever harder to mitigate DDoS attacks even for institutions and companies that have the required skills and capacity.

As powerful botnet tools like Mirai become publicly available, it could even be possible for a motivated group with basic skills to launch a devastating attack against any institution.

Alerts about IoT vulnerabilities had been given months before the attacks: for instance, an AT&T report emphasised that organisations adopting IoT technologies needed to pay more attention to the related security implications, while research carried out by Symantec (published in September) showed that IoT devices were increasingly being used to carry out DDoS attacks.

In response to the attacks, discussions on the responsibility of vendors for the security of their products heightened, while standard-setting organisations placed IoT security standards more into focus.

Which issues are affected?

Cybercrime | Cybersecurity | Internet of Things | Cyberconflict | Consumer protection

How are authorities reacting to the threats?

- **25 August.** The US National Institute of Standards and Technology (NIST) explores lightweight encryption for IoT devices. According to NIST, the shift from desktop computers to smaller devices 'brings a wide range of new security and privacy concerns'. As conventional cryptographic algorithms do not perform well on small devices, given their limited resources, more suitable solutions need to be used.
- **14 September.** The US DoJ convenes a threat analysis team to study national security challenges posed by IoT devices. The aim of the group is to secure the IoT from exploitation by terrorist threats and by others who might try to hack devices to cause loss of life or achieve political or economic gain. The group aims to identify and address security challenges presented by the IoT before they are exploited.
- **5 October.** The EU plans to propose legislation on security for IoT devices. Such rules would would require tech companies to meet drastic security standards and go through certification processes to guarantee privacy. Moreover, companies would be encouraged to develop a labelling system for IoT devices that are approved and secure.
- **19 October.** The US NTIA launches a multistakeholder process on IoT security upgradability and patching. The aim is to develop a broad, shared definition or set of definitions around security upgradability for consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers. The ultimate objective is to foster a market that offers more devices and systems that support security upgrades through increased consumer awareness and understanding.
- **10 November.** US experts ask for government intervention, in the form of regulations and public policy, to improve IoT security. Such regulations would cover issues related to security standards, interoperability, and software update requirements, among others. Supporters of governmental regulations argue that the tech companies are mostly concerned about commercial interests, and are not sufficiently motivated to appropriately address the problem. Others, however, draw attention to the fact that the IoT is a broad concept, and any regulation in this area would have to be extensive enough to cover the various sectors and products.
- **16 November.** US Congress holds subcommittee hearings on IoT security. Experts highlight the increasing risks posed by the inadequate security of Internet-connected devices, and call for governmental intervention.

#7 Artificial intelligence brings new applications and growing concerns

The facts

Artificial intelligence (AI) attracted increased attention over the past year, as new applications continued being developed in multiple areas, ranging from communications and intelligent education systems, to robotics and smart vehicles.

Several companies have been working towards enabling self-driving cars, new automatic translation tools have been developed, and researchers have proposed AI-based techniques for various purposes such as detection of abusive domain names at the time of registration and identifying gang members based on their Twitter posts.

Google's DeepMind made the headlines for its partnership with the UK's National Health Service to use machine learning to analyse the records of more than 1.6 million patients annually. Facebook built an AI program, called DeepText, that could help catch spam and other unwanted messages. Jigsaw, a Google initiated start up, has been working on Conversation AI, a tool aimed to automatically detect hate speech and other forms of verbal abuse and harassment online. Japan launched a project aimed at creating an Artificial Intelligence Bridging Cloud (AIBC), a supercomputer which could have initial applications in medical research or in software for controlling AI systems such as driverless cars and robots.

These ongoing developments have encouraged policymakers to more carefully explore the policy implications of AI. The US National Science and Technology Council outlined its strategy for promoting AI research and development, while the White House made recommendations on how to prepare the workforce for an AI-driven economy. The UK Parliamentary Committee on Science and Technology asked the UK government to take proactive measures. Earlier in the year, the Committee on Legal Affairs in the European Parliament published a draft report on Recommendations to the Commission on Civil Law Rules on Robotics.

Why is this significant?

The policy implications of AI are far-reaching. While AI can potentially lead to economic growth, there are growing concerns over the significant disruptions it could bring to the labour market. Issues related to privacy, safety, and security have also been brought into focus, with calls being made for the development of standards that can help ensure that AI applications have minimum unintended consequences.

As AI systems involve judgements and decision-making – replacing similar human processes – concerns have also been raised regarding ethics, fairness, justice, transparency, and accountability. The risk of discrimination and bias in decisions made by autonomous technologies is one such concern, very well illustrated in the debate that has surrounded Jigsaw's Conversation AI tool. While potentially addressing problems related to misuse of the Internet public space, the software also raises a major ethical issue: How can machines determine what is and what is not appropriate language?

These and other social, economic, and ethical challenges for AI call for a broader societal dialogue, with governments, the private sector, academia, and civil society contributing to identifying the most appropriate policy answers. Such dialogue will also help governments determine whether new legislation and regulations are needed to address AI-related challenges, or whether existing frameworks can effectively and efficiently be applied (with eventual necessary adjustments).

Which issues are affected?

Infrastructure | Web standards | Tech standards | Internet of Things | Convergence | Other economic issues

Timeline of developments

- **28 September.** Amazon, DeepMind/Google, Facebook, IBM, and Microsoft launch a Partnership on Artificial Intelligence, aimed at addressing AI opportunities and challenges in areas such as ethics, fairness, reliability, and privacy.
- **2 November.** Carnegie Melon University announces the creation of a research centre that will study ethical challenges posed by AI and other computational technologies.
- **13 December.** The Institute of Electrical and Electronics Engineers (IEEE) publishes a draft guide on ethics and AI, aimed at encouraging technologists to prioritise ethical considerations in the creation of autonomous and intelligent technologies.
- **20 December.** New research brings AI algorithms closer to being able to explain themselves, as researchers at the University of California, Berkeley, and the Max Planck Institute for Informatics design a 'pointing and justification' system that enables algorithms to point to the data used to make a decision and justify why they were used that way.

Resources

Read more about the policy implications of AI, including economic and social, safety and security, privacy, and intellectual property rights (IPR).

#8 SDGs and Internet access permeate digital policy discussions

The facts

Community networks as a bottom-up solution for sustainable access was widely discussed at this year's Internet Governance Forum (IGF). Although they face many challenges, these networks empower communities to find solutions for Internet access without waiting for connectivity to become available. Could community networks become a key approach in connecting the next billion users?

Other projects, such as Google's Project Loon for balloon-powered connectivity and its Project Skybender for solar-powered drones for 5G connectivity, also aim to bring access to remote and rural areas.

Efforts to connect the unconnected contribute to attaining the SDGs, and specifically, Goal 9 which seeks to significantly increase and provide universal and affordable Internet access. Yet, the Internet is also essential for attaining other goals, and for implementing and monitoring them. This interplay was widely reflected in SDG-related discussions during the year, from events on sustainable development, to meetings on other digital policy areas.

Why is this significant?

The discussions in 2016 solidified the view that the Internet is essential in the attainment of the SDGs. The key issue, as the 15-year milestone of the 2030 Development Agenda slowly approaches, is to see how the goals can become a reality.

The development aspect was tackled not only in discussions on sustainable development, but also during many sector-specific discussions. Whether the debate was on e-trade, human rights, or new technologies, the community made a conscious effort to consider the development aspect, and what progress could be made towards attaining the goals.

The emphasis on access, narrowing the digital divide, capacity development, and other development aspects, is likely to be stronger in the coming years.

Given the role of the Internet, connecting the unconnected is seen as crucial to reaching the SDGs. Community initiatives and projects by the private sector can contribute widely.

Which issues are affected?

Access | Digital divide | Development - other | Capacity development | Telecommunications infrastructure

SDG developments in 2016

- **29 January.** The UN Secretary-General announces the appointment of a group of 10 experts to support the Technology Facilitation Mechanism (TFM). Announced during the UN SDGs Summit in September 2015, the TFM supports the implementation of the SDGs with a task team on science, technology, and innovation (STI), an annual STI multistakeholder forum, and an online platform that functions as a gateway for information on initiatives, mechanisms, and programmes.
- **3 March.** The first of several meetings between the Inter-agency Task Team on STI and the 10-member Expert Group discusses the organisation of the STI multistakeholder forum.
- **8–11 March.** The UN Statistical Commission agrees on the Global Indicator Framework, which denotes the indicators used to measure progress made in achieving the goals and targets of the 2030 Agenda.
- **1 April.** Inter-agency and Expert Group on SDGs agree on a tier system for indicators, procedures for the methodological review of indicators, and global reporting mechanisms.
- **2–6 May.** The WSIS Forum gathers the ICT for Development and Internet governance communities. The forum is strongly linked to sustainable development, as it has explicitly linked the WSIS Action Lines to the SDGs.
- **6–7 June.** The STI Forum takes place in New York and addresses the contributions on STIs towards achieving the SDGs.
- **11–20 July.** The High-Level Political Forum on Sustainable Development meets for the first time in New York since the adoption of the 2030 Agenda for Sustainable Development. The forum discusses the utility of ICT tools, forums, and platforms. The UN's Global Sustainable Development Report assesses the progress made so far in achieving the SDGs, and confirms that technology is essential for achieving the SDGs and minimising trade-offs among goals.
- **19 September.** The Broadband Commission states that the SDGs cannot be achieved without affordable and universal access to ICTs and broadband connectivity.
- **6–9 December.** The 11th IGF, with the theme of 'Inclusive and Sustainable Growth', is anchored in the framework of the SDGs. Although the most focused-on SDG is Goal 9 on access to ICTs, many discussions deal with the link between Internet governance and the SDGs.

Resources

Read the GIP's final reports of the WSIS Forum and the 11th IGF, which form part of the GIP's just-in-time reporting initiatives from each event. Read more about the SDGs and the Internet, on our dedicated page on the *GIP Digital Watch* observatory.

#9 Debates on data governance increase after a series of data breaches

The facts

The year 2016 counted numerous data breaches. The biggest breach was targeted at Yahoo!, which confirmed in September that half a billion users may have had their data stolen, and in December that up to one billion user accounts were thought to have been affected.

In November 2016, user records were leaked from Friend Finder Networks, a network comprised of adult-content websites. In total, more than 412 million user records were published online. In China, Taobao (a Chinese online shopping website similar to eBay, Amazon, and Rakuten) was targeted, and 20 million records were released. In the Philippines, a breach of the election database resulted in the loss of personal information on every voter in the country: approximately 55 million people. A detailed account of the trend of data breaches can be read in the Internet Society's *Global Internet Report 2016*.

The leaked Panama Papers – the result of a hacked e-mail server – wreaked havoc for public officials embroiled in the offshore scandal. The leak led to public outcry in many countries, resignations of politicians, and reputational damage for parties involved in the scandals and countries where politicians held office.

Why is this significant?

Data is increasingly stored and processed online, whether it concerns health records, personal information, economic transactions, or company records. The consequences of data breaches can have significant financial and non-financial costs for consumers and organisations. Data breaches feed into a larger discussion on data governance.

As data flows across borders, it becomes increasingly complex to manage and protect. Issues of data privacy, security, sharing, and storage have risen on the political agenda. The intensity of debates surrounding these issues has intensified with the advent of Big Data and the IoT, and were discussed, among other places, in China during the Big Data World Forum and in the Netherlands during the European Data Forum 2016.

Faced with the global movement of data, governments have started to adopt data localisation rules, which require data to be stored on national servers, for reasons ranging from economic protectionism, to security, privacy, and political considerations. Yet data localisation practices have been opposed by the G7 *Principles* and *Actions on Cyber*.

Which issues are affected?

Privacy and data protection | Cloud computing | Cybersecurity | Critical infrastructure | Jurisdiction | Intermediaries

Data governance developments in 2016

- **27 February.** The *2016 Data Threat Report* shows that the majority of companies are concerned about the security of data stored in the cloud.
- **12 April.** A few days after hackers publish a massive database containing the personal information of approximately 50 million Turkish citizens, a new data protection law comes into force in Turkey.
- **19 April.** The United Nations Conference on Trade and Development (UNCTAD) report on *Data Protection Regulations and International Data Flows* suggests that a 'core set' of data protection principles can serve as a useful starting point for more compatibility and harmonisation.
- **5 August.** Among the principles for cloud adoption within governmental agencies, the Canadian government's draft Cloud Adoption Strategy states that 'all sensitive or protected data under government control will be stored on servers that reside in Canada', in order to 'ensure Canada's sovereign control over its data'.
- **3 October.** Responding to European businesses' need to comply with data sovereignty and security regulations, Microsoft announces plans to open data centres in France.
- **27 October.** The US Federal Communications Commission (FCC) approves new privacy rules requiring Internet providers to obtain their customers' explicit consent before using or sharing behavioural data with third parties. The data includes application usage, browsing history, mobile location, health data, financial information, content of e-mails, and other sensitive personal information being gathered while using the Internet.
- **7 November.** China adopts a cybersecurity law that requires 'personal information and important business data' to be stored on Chinese servers.
- **17 November.** Russia blocks LinkedIn after the social network fails to transfer Russian users' data to servers located within the country's territory, in violation of Information Law No. 242-FZ which requires data to be stored on local servers as of September 2015.
- **22 December.** The CJEU states that 'general and indiscriminate retention' of data is prohibited for EU member states, questioning the legality of the UK's Investigatory Powers Act.

#10 Privacy Shield framework replaces Safe Harbour agreement

The facts

Five months after an agreement on a new framework for transatlantic exchanges of personal data for commercial purposes was reached between European Commission and the USG, the Commission approved the new Privacy Shield framework. The new framework provides a mechanism which should protect the fundamental rights of European users whose personal data is transferred beyond EU shores.

The new Privacy Shield is in response to the Court of Justice of the European Union's (CJEU) 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. Towards the end of the year, the framework faced its first two legal challenges when privacy advocacy groups requested the annulment of the new framework.

Why is this significant?

The Privacy Shield is a high-stakes issue. The lack of a policy solution on privacy could block data transfers on the main data highway across the Atlantic Ocean. It could create major consequences, from affecting businesses in Europe and the USA to millions of users of Facebook, Google, and other Internet platforms.

It was the backdrop for finding the Privacy Shield solution in such a short time-frame. Both the relevance and the fragility of this arrangement will put additional pressure on all main actors to ensure that it works in reality.

Substantively different privacy regulations between the EU and the USA will create permanent jurisdiction tension in the way data is managed.

In addition, the implementation of the Privacy Shield will be carefully monitored by other countries which tend to follow how the EU deals with the Internet industry, as was the case with countries worldwide adopting regulations on the right to be forgotten.

Transatlantic data flows and the regulations is expected to remain high on policy agendas since the flow of data across the Atlantic Ocean is vital for the global Internet industry.

Which issues are affected?

Privacy and data protection | Intermediaries | Consumer protection | Other human rights

Timeline of developments

- **2 February.** The EU Justice Commissioner announces a new deal, after a cabinet meeting of the EU Executive in Strasbourg. For the Commission, the key aims are 'to ensure that citizens fundamental right to protection of personal data is guaranteed when their data is transferred abroad'; and 'to allow transatlantic data flows – which are important to the economy – to continue, with the necessary safeguards'.
- **29 February.** The European Commission publishes the legal texts, including principles which companies would need to abide by.
- **13 April.** The Article 29 Working Party (WP29; composed of representatives of national Data Protection Supervisory Authorities, the European Data Protection Supervisor, and the European Commission) issues its opinion, expressing concerns over commercial aspects and public authorities' access to the data. It is also concerned about the lack of clarity of the framework, the fact that key principles under EU law are not reflected therein, and the lack of sufficient independence of the Ombudsman – a new redress mechanism in the framework.
- **30 May.** The European Data Protection Supervisor publishes his opinion: a more robust and sustainable solution needed.
- **8 July.** EU member states approve the Privacy Shield agreement.
- **12 July.** The Privacy Shield is formally adopted by the European Commission.
- **1 August.** US companies can sign up for the framework. The US DoJ will evaluate applications and monitor companies for compliance.
- **16 September.** The Privacy Shield is challenged, as Digital Rights Ireland, an Irish privacy advocacy group, files for the annulment of the Commission's Adequacy Decision in front of the Luxembourg-based General Court.
- **20 November.** The Privacy Shield faces a second legal challenge. French privacy advocacy group La Quadrature du Net, non-profit Internet service provider French Data Network, and its Federation FDN industry association, are objecting to the restrictions on US surveillance activities, in particular the bulk collection of data, and the purposes for which the data can be used.

Resources

Read more about the Privacy Shield's seven principles, and the legal challenges the framework is facing.

#11 Courts rule on privacy, data protection, and data retention

The facts

The Apple/FBI case brought the interplay between privacy and security into sharper focus, as facilitating access to the phone would have had endangered the rights of users worldwide. While the case was resolved before the courts could rule on it, other judgments throughout the year further shaped the application of the right to privacy for users in different countries.

One of the main judgments was a CJEU ruling which prohibited general and indiscriminate retention of data by providers of electronic communications services. The court ruled that access to the retained data by the government should be restricted for the purpose of preventing and detecting serious crime, and must be subject to prior review by a court or an independent authority.

The ruling also stated that notice must be given to the individuals affected by the retention, as soon as such notice no longer jeopardises any investigation, to enable them to exercise their legal rights, if necessary.

A new UN resolution on the right to privacy called on states to refrain from requiring companies to take steps that interfere with the right to privacy in an arbitrary and unlawful way, and to inform users about company policies that may impact their right to privacy. The first report of the Special Rapporteur on the Right to Privacy identified seven areas for in-depth thematic studies, and proposed a ten-point action plan.

The protection of children's rights in the digital environment, including the protection of children's privacy, is one of the priorities of the Council of Europe's Strategy for the Rights of the Child (2016–2021). UNCTAD's report on *Data Protection Regulations and International Data Flows* suggests that a 'core set' of data protection principles can serve as a useful starting point for more compatibility and harmonisation of rules.

The EU's tough stance on privacy landed Facebook in hot water after the company was accused of providing misleading information on its takeover of WhatsApp. Although Facebook had informed regulators that it would not be able to match Facebook accounts with WhatsApp accounts, a privacy policy change in August meant that matching data and sharing user accounts could be done automatically.

Why is this significant?

The landmark judgment on data retention called into question the UK's newly enacted Investigatory Powers Act, also referred to as the Snoopers' Charter, and legislation in other EU countries that allow for indiscriminate retention of data. The Investigatory Powers Act, enacted in November, was one of the most vividly debated bills in 2016, mostly due to the controversial sections on mass surveillance.

The court's ruling set a new precedent for the EU member states' data retention regimes, with particular implications for the UK Act. Although it is unclear how the government will respond, activists have already called on the government to make changes to the Act to comply with the ruling. The fact that the UK is expected to leave the European Union in the near future adds to the uncertainty.

The other developments are a strong reminder of the interplay between privacy, consumer protection, surveillance, and cybersecurity. Stakeholders need to balance various interplays, such as that between the government's need to protect its citizens and the user's right to privacy, and that between surveillance and data protection.

Which issues are affected?

Cybercrime | Privacy and data protection | Intermediaries | Other human rights

Main privacy-related judgments

- 12 January. In another ECHR judgment, the court rules that Hungary's surveillance of private individuals on anti-terror grounds is illegal.
- 12 January. The European Court of Human Rights (ECHR) rules that private communications made during office hours may be read by employers. With six votes to one, the Court ruled that it is not unreasonable for an employer to want to verify that employees are completing their professional tasks during working hours.
- 19 October. The CJEU rules that the dynamic IP address of a website visitor constitutes personal data, in specific circumstances. The operator of a website may have a legitimate interest in storing certain personal data relating to visitors to that website in order to protect itself against cyber-attacks.

#12 Fragmentation and restrictions to Internet services continue

The facts

In the past year, several restrictions to Internet services were reported worldwide. Political turmoil, content control, refusal to hand over users' data, and breach of localisation laws were among the reasons for disruptions in the services, amid concerns over freedom of expression.

The 2016 *Freedom of the Net* report confirmed that Internet freedom continued to declined for the sixth consecutive year, with communication apps being particularly targeted. The report assesses government involvement in targeting social media and communication apps, and looks into the unprecedented penalties that social media users face, the more diverse content which governments are censoring, security measures that threaten free speech and privacy, and online activism in general.

In July, the UN Human Rights Council (UNHCR) passed a significant resolution condemning unequivocally 'measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law', and called on countries to refrain from and cease such measures. The resolution reaffirmed that human rights must also be protected online.

Why is this significant?

Internet freedom has been increasingly under threat for many years. With the emergence of mobile apps, and their popularity as a communication tool, authorities turned to restrict access not only to websites or services, but to apps such as WhatsApp.

In other cases, Russia's suspension of LinkedIn sent clear signals that non-compliance with localisation laws would not be ignored. Brazil's requests for user data from WhatsApp reminded the global community of the Apple/FBI controversy. The suspension of service and the detaining of a Facebook employee, however, was viewed as disproportionate.

Which issues are affected?

Content policy | Access | Freedom of expression | Intermediaries

Restrictions to Internet services

- **17 February.** Indonesia's Information Ministry blocks Tumblr due to concerns over pornographic content. Access to 477 websites are blocked due to adult material. The country also blocks Netflix and urges social media sites to remove gay emojis (small digital images or icons used in electronic communication) as it considers the issue to be 'a matter of political stability'.
- **1 March.** In Brazil, Facebook's Latin America Vice-President is detained after WhatsApp's (a Facebook subsidiary) refusal to hand over data to the authorities in relation to a drug trafficking case. The Vice-President is accused of 'repeated non-compliance'; Facebook calls the police actions 'extreme and disproportionate'. The case continues in May when a Brazilian judge orders a country-wide shutdown of WhatsApp for 72 hours, which is repeated a few months later; in July, a Brazilian court orders that Facebook's funds be frozen.
- **2 March.** Morocco's National Telecommunications Regulatory Agency imposes a ban on VoIP services, over the lack of necessary licences by the providers to operate in the country. The authority lifts the ban in November, basing its decision on an evaluation of the telecom national and international market, the legal context, and the overall implications for consumers.
- **14 March.** A Turkish court bans access to Facebook and Twitter after the car bombing in Ankara, in an effort to prevent users from sharing images of the attack. Broadcast media is also banned from covering aspects of the attack.
- **1 April.** The North Korean government announces that it is blocking Facebook, YouTube, Twitter, and South Korean websites. Although few North Koreans have access to the Internet and can usually only see a 'sealed-off, government-sanctioned intranet', foreigners in North Korea have had almost unrestricted access to the Internet.
- **21 July.** Internet traffic in Turkey is significantly slowed down in the aftermath of an attempted coup. Following social unrest in November, access to social media networks is blocked 'for security reasons'. The blocking came after representatives of the pro-Kurdish Peoples' Democratic Party were detained. Shortly after the arrests, social unrest hit Diyarbakir, the largest city in Turkey's mainly pro-Kurdish south-east region.
- **16 October.** In Montenegro, the regulator orders telecom operators to prevent access to WhatsApp and Viber on election day, allegedly because of users' complaints over 'unwanted communication'.
- **7 November.** Russia blocks LinkedIn after the network fails to transfer Russian users' data to servers located in national territory, in violation of the law. The decision is issued by Russia's communications regulator, Roskomnadzor, following a decision from the Moscow city court. Russia has described its rule on localised servers as a way of protecting users' personal data.

#13 New guidelines on net neutrality emerge alongside fresh debates on zero-rating

The facts

In comparison with previous years, debates on net neutrality and zero-rating were not as prominent. Nonetheless, significant developments took place around the world and are expected to continue in the coming months, as more companies seek zero-rating practices to attract customers.

In Europe, the EU's net neutrality rules came into effect in April, following the adoption of Regulation (EU) 2015/2120 in November 2015. Under these rules, all traffic must be treated equally. Blocking, throttling, and discriminating against Internet traffic by Internet service providers (ISPs) is not allowed. In August, after a period of vibrant public discussion, the Body of European Regulators for Electronic Communications (BEREC) published its guidelines on the implementation of the rules by national regulatory authorities (NRAs).

In the USA, Facebook initiated talks with government officials over plans to launch Free Basics in the country, reigniting the debate on zero-rating practices. Internet companies called on the FCC to publish its evaluation of zero-rating practices, which the FCC determines on a case-by-case basis. FCC chairman Tom Wheeler, a strong supporter of net neutrality, announced his resignation, due to take effect on 20 January; members of the Commission disclosed their plans to work on revising the net neutrality rules adopted by the FCC in 2015.

In India, the regulator banned Free Basics after months of discussions. Fresh debates were sparked in other countries.

Why is this significant?

In the EU, BEREC's guidelines were highly anticipated, especially since the 2015 regulation remained silent over zero-rating practices. While not expressly forbidden, the guidelines shed a clearer light on which practices would be in breach of the regulations. As expected, the guidelines were received with enthusiasm by Internet activists, but with a degree of reticence by telecom operators, who argued that many of their concerns had not been taken into account.

The assessment of such practices will now be carried out by NRAs, which places EU countries in a similar position to the USA. The positions taken by each will most likely be monitored closely as the rules are put into practice. It also remains to be seen whether Facebook's Free Basics will be introduced in the USA, despite being strongly opposed in India and Egypt.

In the USA, the FCC chairman's departure may be a blow for net neutrality. His resignation could pave the way for a new battle over net neutrality, especially considering that members of the Commission have already disclosed their plans to revise the FCC's 2015 rules.

Which issues are affected?

Net neutrality | Intermediaries | Consumer protection | Other economic issues

Other developments

- **13 January.** The Council of Europe's net neutrality recommendation underlines that 'Internet users' right to receive and impart information should not be restricted by means of blocking, slowing down, degrading or discriminating Internet traffic.'
- **8 February.** After months of intense debate, India's Telecom Regulatory Authority opposes Facebook's Free Basics: 'No service provider shall offer or charge discriminatory tariffs for data services on the basis of content', declared the institution.
- **14 October.** The Dutch Parliament's revised net neutrality law is seen as too severe; the GSMA, a trade body that represents the interests of mobile operators worldwide, believes it will stifle innovation;
- **17 October.** In a letter sent to the FCC, 76 public interest and civil rights groups ask the agency to protect the open Internet and the rights of consumers in the digital age. They ask the FCC to adopt privacy rules that would request broadband providers to protect the privacy of their customers (which the FCC does), and to prohibit commercial practices that involve abusive data caps and zero-rating plans that breach the net neutrality principles.
- **1 November.** The Canadian telecom regulator holds a public consultation on 'differential' Internet pricing, following complaints over zero-rating practices.
- **7 November.** Debate is likely to resurface also in the UK after a major telecom operator introduces a zero-rating data plan.
- **15 December.** The FCC's chairman announces his resignation. The net neutrality debate is likely to resurface as two Republican members of the FCC disclose their plans to work on revising FCC rules.
- **23 December.** The Dutch Consumer and Markets regulator bans T-Mobile Netherlands' zero-rating practices, introduced by the company in October.

#14 Digital revolution fosters economic growth

The facts

'Globalization is good... when trade stops, war comes', said Jack Ma, chairman of Alibaba, on the margins of the G20 Hangzhou Summit in September. Alibaba is the biggest e-commerce company in China, which saw a boom in the retail market over the last 12 months. Leveraging the emerging market position, China together with Pakistan introduced a potential solution for a stalemate in e-commerce negotiations, during the World Trade Organization (WTO) Council for Trade in Goods meeting, by proposing to work on the promotion and facilitation of cross-border trade in goods enabled by the Internet.

2016 was also notable for intense negotiations around trade-related plurilateral agreements, such as the Trans-Pacific Partnership (TPP) or Trade in Services Agreement (TISA), in parallel with strong opposition from civil society activists. Among the controversial provisions of such treaties are those related to digital policy: cybersecurity, net neutrality, data localisation, and cryptography.

Why is this significant?

The digital revolution is expected to play a key role in fostering economic growth in the coming years. This has been recognised, for example, by the G20 Communiqué from the 2016 Hangzhou Summit. Among the new business models enabled by ICTs, e-commerce has been considered key to fostering development and achieving the SDGs. Business-to-business e-commerce is valued over US$19 trillion and business-to-consumer already accounts for over US$2 trillion. If small companies in developing regions are connected to the Internet, they can enjoy access to the global market, fostering inclusion and development. For the potential of e-commerce to be fully realised, however, proper regulatory frameworks need to be in place. Given the cross-border nature of e-commerce, these enabling conditions should also be discussed and harmonised on a global level, through the work of the many international organisations that play a role in the development of aspects related to digital trade.

Issues related to e-commerce fall into two policy circles. In the first, there are organisations that directly deal with e-commerce, such as UNCTAD, which focuses on trade and development, and the OECD, which is responsible for carrying out a wide range of e-commerce activities.

In the second circle, there are organisations dedicated to other policy issues that affect e-commerce, including the World Intellectual Property Organization (WIPO), the ITU, and the International Organization for Standardization (ISO). The UNHCR focuses on privacy, which is relevant for the movement of data, an important aspect of e-commerce. There is a growing understanding that the WTO could play an important role in e-commerce.

WTO member states seem to be divided between those that express a readiness to start delineating outcomes from the discussions on e-commerce and those that believe it is too early to draw any conclusions. Among the latter are many developing countries who see e-commerce as a new issue, not included in the priorities set by Doha. According to them, access to infrastructure and e-literacy skills – which would allow developing countries to make e-commerce flourish – need to be discussed before the development of multilateral rules for e-commerce.

In addition, traditional digital policy issues are being included in the multilateral trade agenda. An exchange of views among WTO member countries mapped the trade-related aspects of e-commerce that would fall under the remit of the WTO, including issues such as network neutrality, data localisation, interoperability, and encryption.

Which issues are affected?

Consumer protection | Net neutrality | Cybersecurity | Taxation | E-commerce

Relevant developments

- **27 July.** UNCTAD launches the eTrade for All initiative, aimed at boosting the progression of e-commerce in developing countries.
- **6 September.** G20 leaders stress the role of the digital economy for growth and development and the new industrial revolution.
- **7 November.** China's new cybersecurity law receives criticism as it would exclude foreign companies from China, due to requirements such as security reviews and data storage on Chinese servers. According to Human Rights Watch, the law would further restrict online freedom. Zhao Zeliang, Director of China's Cyberspace Administration, claims the law is in accordance with international trade rules.
- **17 November.** China and Pakistan's 'pragmatic solution' for e-commerce proposes to work on the promotion and facilitation of cross-border trade in goods enabled by the Internet.

#15 Guidelines and rulings further shape the sharing economy

The facts

In recent years, the latest model in the Internet economy, the so called sharing economy, catapulted new players – such as Uber and Airbnb – into the global market.

Such businesses have taken full advantage of the opportunities offered by the Internet economy. At the same time, such models have found opposition from traditional businesses, such as taxi and hotel services. Court cases and regulation continued in an effort to determine the status of the market players.

In June, the European Commission issued new guidelines on the sharing economy, aimed at reaping the benefits of new business models, and addressing concerns over the uncertainty of rights and obligations arising from the sector. The non-binding guidelines, published as a *Communication on a European Agenda for the Collaborative Economy* covered ways in which existing EU law should be applied to the collaborative economy.

In particular, restrictions to services such as Uber and Airbnb should be justified and proportionate. Total bans should be used as a measure of last resort to be applied only 'if and where no less restrictive requirements to attain a legitimate public interest objective can be used', the guidelines state.

Courts were faced with new issues, mostly related to Uber. In an ongoing case, a Spanish judge asked the CJEU to confirm whether Uber could be considered a transport service provider or a digital platform. Courts were also asked to confirm whether Uber drivers were employees or independent contractors.

Why is this significant?

In 2015, companies such as Uber were hit by a large number of court cases and fierce opposition by taxi drivers over licensing, labour law, and the 'disruptive' economic model.

The European Commission's guidelines are a departure from the 'wait-and-see' approach adopted in recent years. They also promote a less restrictive approach than that adopted by several European countries in the past few years.

Whereas some countries initially banned Uber, for example, the Commission is recommending that bans are only adopted as a last resort.

The new business model has significant implications for labour law. Uber may be obliged to follow employment rules – including minimum wage and leave entitlement – in cases where the courts confirm that drivers are employees. The CJEU's Uber ruling in the Spanish case is expected to be delivered in 2017.

Which issues are affected?

Labour law | Intermediaries | E-commerce | Convergence | Other economic issues

Notable cases

- **27 June.** Airbnb sues the city of San Francisco over a new regulation which requires companies to crack down on illegal renting. The company is claiming that this kind of regulation would violate the Communications Decency Act, which gives intermediaries immunity.
- **28 July.** In China, a new regulation – effective from November – allows the use of private cars for taxi rides, under certain conditions. These require drivers to have at least three years' driving experience; vehicles to be equipped with safety features, including alarms and GPS; and vehicles to have no more than seven seats.
- **28 October.** In a landmark ruling, a UK employment tribunal rules that Uber drivers are employees and should enjoy workers' rights. This means that drivers are entitled to a national minimum wage, to leave and sick benefits, and to other statutory benefits. Uber argued that it considered itself to be a tech company rather than a transport one, and that its drivers were self-employed contractors. 'Any driver who has the app switched on' and is in the area they are allowed to work and is able to 'accept assignments' is 'working for Uber under a "worker" contract.'
- **19 December.** Uber and Express Group, Indonesia's second largest taxi company, partner up for a three-month trial. The partnership will allow Uber to increase its pool of cars in the Indonesian capital, Jakarta, while the taxi drivers will enjoy more business. The partnership comes after thousands of Express Group drivers staged a protest, earlier in 2016, to demand a ban on Uber.

#16 Companies hit by tax bills and investigations

The facts

On 31 August, the European Commission ordered Apple to pay the Irish state up to €13 billion in taxes, after an investigation into Apple's 'sweetheart tax' granted by Ireland. According to EU competition officials, the Apple-Ireland agreement resulted in unlawful state aid. Throughout the year, a number of countries sought to investigate Internet companies for potentially unpaid tax bills related to revenues generated within the country.

Why is it significant?

In this era of austerity, governments under fiscal pressure have been looking to the fast-growing Internet economy as a way to boost state coffers. Governments are likely to pursue taxation of the Internet economy in two directions. First, they will put additional pressure on the Internet industry to pay taxes as other industries do. The EU tax-fine of Apple is one example. Secondly, governments will look for ways and means to tax new types of Internet industries, such as Uber and Airbnb.

There will be increasing pressure, especially in the EU, on countries that try to strike tax deals with the Internet industry. National governments will try to 'normalise' taxation of the Internet industry by ensuring that taxes are paid in jurisdictions with the most relevant element of Internet transactions (such as the country where the Uber drive was performed).

Such an approach would be in accordance with the OECD Ottawa principles for e-commerce taxation that specify the 'destination' principle for taxation, focusing on consumer of e-commerce services.

As with any taxation, the impact can be complex, affecting economic dynamics and job creation.

Which issues are affected?

Taxation | Intermediaries | E-commerce | Labour law | Other economic issues

Other tax investigations

- **7 April.** According to Reuters, Indonesia's tax office will examine the tax reports of Yahoo!, Twitter, Google, and Facebook. Finance Minister: 'Revenue from ads should be part of those taxable by us... we will be serious in straightening up taxes on digital economy.'
- **1 August.** An investigation by the US Internal Revenue Service concludes that Facebook faces a $3–5 billion tax bill related to the transfer of assets to Ireland. Facebook responds that it 'complies with all applicable rules and regulations in the countries where [it] operate[s]'.
- **19 August.** Taiwan requests Uber Technologies to pay a sales tax bill of around $6.4 million, partly due to the government's new tax regime on global online service providers. Uber rejects the allegation that it owes taxes to the government of Taiwan, and argues that it 'is meeting all of its tax obligations under relevant local laws'.
- **16 September.** The Indonesian government is to launch an investigation into Google over alleged unpaid taxes from its advertising revenue. It is also reported that the authorities may issue Google a tax bill of more than $400 million in unpaid taxes for 2015.
- **10 October.** Facebook pays £4.2 million to the UK tax authorities. In April, the company ceased routing advertising sales through Ireland, which could lead to a large increase in tax paid to UK authorities for 2016. Skepticism arises following a decision by the tax authorities to award the company a tax credit of £11.3 million, 'which it can use to cut its future bills from HM Revenue and Customs'.
- **23 November.** Google is expected to reach a tax settlement with the Indonesian government, paying back taxes and fines. A month later, reports announce that Google's settlement offer was deemed too small by the Indonesian government, and a deal will not be reached in 2016. 'Because we couldn't reach a settlement, the investigation continues. Now we want Google to open its books and the tax office will calculate the tax owed,' the main investigator explains.
- **21 December.** Sellers on Amazon and eBay reportedly evade millions of pounds in value added tax (VAT) in the run-up to Christmas, leading British Members of Parliament to launch an investigation. According to the UK government, VAT evasion in online shopping is a 'very big issue', costing about £1.5 billion a year in lost tax.

#17 Court cases tackle intellectual property rights

The facts

IPR and the role of intermediaries in copyright infringement were the subject of several court cases and other developments.

Google's Java case was a major win for proponents of the fair use principle. The notion of fair use allows individuals to copy content, under certain terms, without the need to request permission from the author. Several other judgments, such as the Vimeo judgment, were significant for IPR.

In the EU, new copyright proposals by the European Commission, however, were met with mixed reactions. The proposals are aimed at modernising copyright rules, setting out clearer rules for all stakeholders. Among the priorities are to offer better access to content online and across borders, and to create a fairer and more sustainable marketplace for creators and press.

While the Commission's President believes that the aim is for authors to be paid fairly for their work, Google believes there are worrying elements. 'Today's proposal suggests that works including text, video, images and more must be filtered by online services. This would effectively turn the Internet into a place where everything uploaded to the web must be cleared by lawyers before it can find an audience.'

Mozilla shared a similar concern, explaining that the proposals do not effectively address exceptions to copyright law, such as panorama, parody, remixing, user-generated content, and fair use. Several groups of authors and artists have also expressed concern.

Why is this significant?

The judgments confirm the general notion that an Internet intermediary cannot be held responsible for hosting materials that breach copyright if the intermediary is not aware of the violation.

Google's Java case also confirmed the fair use principle, in the public's interest, especially in an important area such as technical development.

The EU's copyright proposals can be seen as a stricter approach to protect the rights of authors.

The proposals indicate that such rights are protected through a filtering system, which can affect the balance between IPR and public interest. Implementing such a system may require further shaping of intermediary responsibility in the field of copyright infringements; at the same time, it may also risk creating a complex system of content control.

Which issues are affected?

Copyright | Trademarks | E-commerce | Content policy | Intermediaries

Main IPR rulings

- 26 May. Google wins a major US court battle brought by software firm Oracle over Google's use of Java in its Android smartphone operating system. The San Francisco jury rules that Google's use of the software amounted to 'fair use' as it was part of a larger system which the tech giant created for a new purpose. The news was welcomed by developers who generally rely on free access to application programming interfaces (APIs) to develop third-party services.
- 17 June. A US appeals court decides not to prosecute video-sharing website Vimeo for copyright infringements for 'unknowingly hosting older music uploaded by its users'. The case is a positive development for online platforms, but a blow for record labels looking for broader protection.
- 9 September. Following the earlier advice of the Advocate General, the CJEU rules that operators of websites linking to materials that infringe copyright can be found guilty of copyright infringement if the operators knew or could reasonably have known that the material constituted an infringement. Operators would be presumed to know about the infringements if the links were provided for 'the pursuit of financial gain'. Activists argue that the ruling infringes on Internet freedoms, and that sites should not be responsible for the content of the links they refer to.
- 15 September. In another judgment, the CJEU rules that a business offering free Wi-Fi to customers cannot be held liable for copyright infringements by users. Following the Advocate General's advice, the court rules that the service provider cannot be held liable as long as it did not initiate the offending data transmission, select its recipient, or select or modify the information in that transmission.

#18 Fake news and filter bubbles make the headlines

The facts

In the lead-up to and aftermath of the US Presidential election, the role of intermediaries in the spread of fake news attracted attention. Internet companies faced a backlash over the spread of false information on their platforms, prompting them to introduce changes to their policies.

The German chancellor Angela Merkel's comments on filter bubbles also focused on the role of intermediaries in the dissemination of information. Without entering into the merits of responsibility, she urged platforms to reveal their search engine algorithms, as their lack of transparency might 'lead to a distortion of our perception' and 'shrink our expanse of information'.

Why is this significant?

The backlash which Internet companies faced prompted a discussion on the extent of responsibility of intermediaries. To what extent are they de facto regulators of content? Should intermediaries be expected to take a more proactive role in eliminating fake news? And to what extent would this infringe on freedom of expression?

Search engine algorithms have long been a strongly guarded commercial secret for Internet platforms.

One justification is that by revealing how algorithms work, this would actually lead to more distorted search results due to stronger efforts to manipulate results and ranking.

Merkel's argument, on the other hand, is that Internet users have a right to know on what basis they receive information through search engines.

Algorithms operated by search engines could lead to a lack of confrontation with opposing ideas – leading to so-called filter bubbles and echo chambers – which can harm a healthy democracy.

Which issues are affected?

Content policy | Intermediaries | Other economic issues

Tackling fake news

- **4 July.** The Cyberspace Administration of China announces the media would no longer be able to rely on news obtained from social media. 'It is forbidden to use hearsay to create news or use conjecture and imagination to distort the facts'.
- **14 October.** Google announces plans to introduce a 'fact check label', tagging news from 'nonpartisan' websites in sensitive areas, such as urban legends, the media, politics, and health. The label aims to 'shine a light on [the Fact Check community's] efforts to divine fact from fiction, wisdom from spin'.
- **28 October.** German chancellor Angela Merkel urges Internet platforms to reveal their search engine algorithms, arguing that Internet users have a right to know on what basis they receive information through search engines. She explains that the algorithms operated by search engines could lead to a lack of confrontation with opposing ideas – leading to so-called filter bubbles and echo chambers – which can harm a healthy democracy.
- **9 November.** In the aftermath of the US elections, a fierce debate arose regarding the role of fake news and filter bubbles in the election results.
- **16 November.** Google and Facebook announce changes to their policies to prevent fake news websites from using their respective advertising networks.
- **19 November.** The spread of fake news on social networks leads Chinese officials to address it during the third World Internet Conference in Wuzhen in November. Fake news is a sign that 'cyberspace has become dangerous and unwieldy', the Cyberspace Administration of China said, recommending that those who post fake news are punished.
- **6–9 December.** The 11th IGF 2016 brings a slight shift in focus on the issue of fake news. It is discussed more in connection with how to validate information (role of users), than how platforms should tackle the issue (role of intermediaries), as has been the case in public debate. Speakers argue that there needs to be greater social media literacy 'to understand that what we're reading is not the whole picture', while others discuss the distinction between reputable and non-reputable news outlets, acknowledging that even the most established outlets can get it wrong.

Resources

Read our article on Post-election concerns over fake news and filter bubbles, in Issue 16 of the *Geneva Digital Watch* newsletter.

#19 Microsoft case delineates extent of jurisdiction

The facts

On 15 July, a US Appellate Court ruled that the USG could not use a search warrant to force Microsoft to turn over the e-mail communications of a criminal suspect in a drug case, as the communications were stored at Microsoft's data centre in Dublin, Ireland. The ruling, which overturned a previous order granted in 2014, said that a search warrant granted under the Stored Communications Act cannot be applied internationally. On 21 October, the US DoJ petitioned the Court of Appeals for the case to be reheard.

In 2016, other notable cases delineated the extent or limits of jurisdiction. These included court judgments involving Facebook's activities, and an ongoing battle between the French data protection regulator (Commission Nationale de l'Informatique et des Libertés, CNIL) and Google over the right to be forgotten, or more appropriately, the right to be delisted. In the latest development, CNIL requested Google to apply its delisting not only for non-European sites accessed by European users, but across search results globally – a request which Google is objecting to.

Other jurisdictions introduced – and in one case turned down – the right to be delisted.

Why is this significant?

The Microsoft judgment was seen in particular by human rights advocates as a positive precedent that limits the USG's ability to demand access to data stored in data centres located outside US borders, even when the companies storing the data have their headquarters in the USA. Although the case may be reheard, it has important ramifications for jurisdiction and the legal tools used for mutual assistance. This development also opened the door for enhancing data protection by opening data centres in different countries.

In judgments concerning Internet companies, the courts set aside the argument that jurisdiction is established in the country where the company is headquartered, even if this is also stated in the terms of service. The judgments therefore continued to expose Internet companies to other jurisdictions.

The right to be forgotten rulings also continued to delineate the extent of jurisdiction. CNIL's request, if upheld, could impose its interpretation of French law on searches conducted in other jurisdictions. Will this mean that countries could effectively request their laws to be applied globally? Google says this is not a far-fetched scenario: 'We have received demands from governments to remove content globally on various grounds – and we have resisted, even if that has sometimes led to the blocking of our services.'

A related consequence is the impact on freedom of expression. The CJEU's landmark case in 2014 divided public opinion: while some viewed the case as a positive development to users' right to privacy, others were concerned about the implications for freedom of expression. The developments in Google's case before the French court, and specifically CNIL's latest request – especially if it is upheld – represent an additional concern. The case could create another precedent due to the extent of its application, and could upset the delicate balance between both rights.

Which issues are affected?

Jurisdiction | Intermediaries | Content policy | Privacy and data protection | Freedom of expression | Consumer protection

Other notable jurisdiction cases

- 9 February. CNIL gives Facebook three months' notice to comply with a formal notice to stop tracking the browsing activity of Internet users who do not have a Facebook account.
- 12 February. A Court of Appeals in Paris confirms that Facebook could be sued in France. The case involves a French teacher whose account was suspended after they shared a photo of a nude painting which hangs in the Musee d'Orsay in Paris.
- 2 May. South Korea's Communications Commission announces that users could request that their own postings be restricted from being publicly accessible.
- 4 May. A Beijing court in China rules that citizens do not have a right to be forgotten under Chinese law.
- 19 May. Google appeals a decision by the French data protection authority to apply a search-results ruling to all its domains in requests under the right to be forgotten.
- 17 June. An Israeli court approves a $400 million class action case against Facebook. Filed in the Central District Court, the case argues that Facebook violates users' privacy by using their private posts to determine which advertisements they should see, without obtaining their knowing consent to this policy.
- 1 November. Indonesia enacts new legislation allowing individuals to seek a court order to clear their names following acquittal in a court case. Web administrators will be required to remove the content.

#20 IANA stewardship transition is completed; accountability reform continues

The facts

The IANA functions contract between ICANN and the USG expired on 1 October, bringing to an end a large part of the transition process initiated in March 2014.

Despite last-minute developments that threatened to stall the process indefinitely, the stewardship of the IANA functions was successfully transitioned to the global Internet community. As the transition process triggered a review into ICANN's accountability, work on this stream continued throughout the year.

In practice, the work carried by the ICANN community in the framework of the IANA transition and ICANN accountability processes led to several changes within ICANN. A new legal entity – the Public Technical Identifiers (PTI) – was created as an affiliate of ICANN entrusted with the performance of the IANA functions (under the oversight of a multistakeholder Customer Standing Committee, which replaced the role of the USG).

To increase the accountability of ICANN, the organisation's bylaws were amended with provisions on an 'empowered community' (a non-profit association consisting of most of ICANN's supporting organisations and advisory committees) which will be able to enforce a set of community powers such as rejecting ICANN budgets and operation plans, rejecting or approving changes to ICANN bylaws, and removing ICANN Board Directors.

Why is this significant?

The transition process had been in the works since 2014, when the US Department of Commerce announced its intent to cede its oversight role of the IANA functions. The transition marked the start of a new epoch for the IANA functions, and signalled a win for the multistakeholder model which was seen as central to the 2.5-year process. This has led to several debates, including at the 11th IGF, on whether and how the multistakeholder work behind the IANA transition could be replicated in other Internet governance processes.

While the USG's role as steward of the IANA functions came to an end, ICANN became an entity solely accountable to the global multistakeholder community. The processes put in place for the community to be able to hold ICANN accountable for its work and decisions are rather sui generis in the Internet governance environment, and it remains to be seen if they will function as planned.

The community will continue to work on additional elements aimed at strengthening ICANN's overall accountability. The new area of work, called Work Stream 2, will focus, among others, on additional transparency considerations, diversity across ICANN, accountability of ICANN staff, accountability of supporting organisations and advisory committees, a Framework of Interpretation on respecting human rights within ICANN's mission and scope, and expanding the list of jurisdictions in ICANN's contracts.

Which issues are affected?

Root zone | Domain Name System | IP numbers

Timeline of main developments

- **10 March.** ICANN's Board submits to the USG the plan to transition the stewardship of key Internet functions.
- **27 May.** New ICANN bylaws are adopted. These reflect the changes necessary as a result of the recommendations contained in the transition and accountability proposals.
- **9 June.** The USG gives the green light for the IANA stewardship transition to move forward.
- **11 August.** ICANN announces the creation of the Public Technical Identifiers.
- **16 August.** The USG tells ICANN it intends to allow the IANA contract to expire as of 1 October.
- **14 September.** A hearing is held in the US Congress, at the initiative of Sen. Ted Cruz, with the aim of investigating the possible dangers of the transition.
- **28 September.** Attorneys general of four US states – Arizona, Oklahoma, Texas, and Nevada – file a lawsuit asking for a freeze on the IANA transition process. They argue the USG needs Congressional authorisation to 'abandon this government property right', and that the transition could lead to a violation of the First Amendment in the absence of a firm guarantee that ICANN will protect free speech.
- **1 October.** The IANA functions contract between ICANN and the USG expires. This marks the successful transition of the IANA functions from the USG to the global Internet community.
- **17 October.** The attorneys general lawsuit is dropped.
- **2 November.** The community working group on ICANN accountability (CCWG-Accountability) meets in the context of the ICANN57 meeting and continues discussions on Work Stream 2.

Resources

Read more about the IANA transition process and access additional resources from our dedicated page on the GIP Digital Watch observatory.

The IG Barometer of Trends

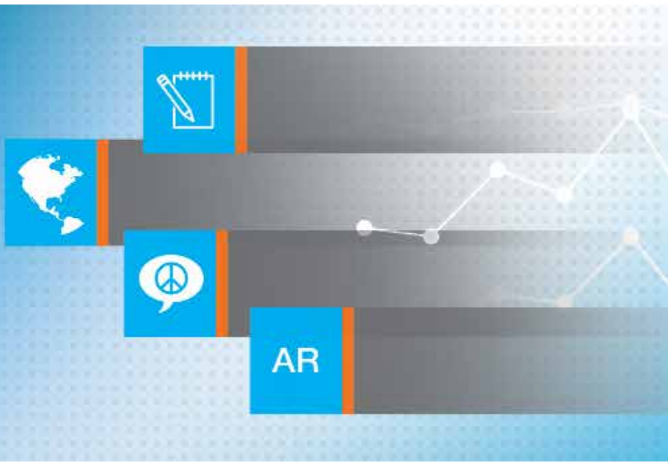
The IG Barometer of Trends tracks specific Internet governance issues in the public policy debate and reveals focal trends by comparing the issues every month. The barometer determines the presence of specific Internet governance issues in comparison to the previous month.

In 2016, the barometer tracked the trends for the following issues: global IG architecture, sustainable development, security, privacy and human rights, infrastructure, net neutrality, e-commerce and the Internet economy, jurisdiction and legal issues, and the IANA transition. The following diagram illustrates the trends throughout the year.

Month Issue	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
Global IG architecture	↗	=	↙	=	=	=	=	=	=	=	=	=
Sustainable development	↗	↙	=	=	↗	=	↗	↗	=	=	=	↙
Security	=	↗	↗	↗	↗	↗	↗	↗	=	↗	↗	=
Privacy and other human rights	↗	↗	↗	↗	=	↗	↗	↗	=	↗	=	↗
Infrastructure	=	=	=	=	↗	↙	=	=	↗	↗	↗	↗
Net neutrality	↗	↗	=	=	=	↗	↙	↙	↗	↗	=	↗
E-commerce and Internet economy	↗	=	=	=	↗	↗	↗	↗	↗	=	↗	↙
Jurisdiction and legal issues	=	↗	=	=	↗	=	↗	↗	=	=	=	↗
IANA transition	=	=	↗	=	=	↗	=	=	↗	=	=	↗

The barometer is published at the end of each month and forms the basis of discussions during the monthly briefings on Internet governance. Held on the last Tuesday of every month, the GIP briefings provide a zoomed-out update of the major global digital policies and Internet governance developments. Learn more about the briefings, and join us online or from Geneva, or via one of the GIP hubs worldwide. We also invite you to read our monthly *Geneva Digital Watch* newsletters, usually published on the last day of each month, for discussions, analyses, updates, and other content.

The *GIP Digital Watch* observatory is a comprehensive platform dedicated to Internet governance and digital policy. Keep track of the latest developments, upcoming and past events, actors active in each policy field, instruments and resources, and much more.



The observatory in numbers

900+	digital policy updates added during 2016
43	issues represented on the observatory
14	expert curators and 20 assistant curators forming part of the team
10	*Geneva Digital Watch* newsletters published in 2016
7	processes followed by the observatory
3	major just-in-time reporting initiatives completed in 2016

The ***GIP Digital Watch observatory*** – at dig.watch – provides a comprehensive and neutral coverage of the dynamic field of digital policy.

The observatory:
- maintains a comprehensive live summary of the latest developments in digital policy.
- provides an overview of issues, actors, and ongoing processes.
- maintains a live calendar of upcoming and past events, and public consultations.
- provides access to the latest research and data on Internet policy.
- is enriched by quantitative research.
- provides just-in-time reporting from digital policy events.

It draws from the strengths of its partners' assets: the resources DiploFoundation has developed over the last 15 years, the Geneva Internet Platform's international reach, and the Internet Society's network of Chapters that help shape localised content.

The observatory is an initiative of the Geneva Internet Platform operated by DiploFoundation – in partnership and with the support of the Internet Society.