

Geneva Internet Platform


 Digital Watch
NEWSLETTER

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

DIGITAL POLICY TRENDS IN JANUARY

TRUMP'S FIRST 100 DAYS

Although the first month of the year was uncharacteristically quiet in terms of digital developments, all eyes were on President Trump's 100 days and the impact of his executive orders on global digital policy.

In particular, he left his mark on at least two main issues – net neutrality, and privacy – with further developments expected to unfold in the coming weeks.

The newly appointed chair of the US Federal Communications Commission (FCC) – Republican Ajit Pai – is expected to initiate a review of the Tom Wheeler's net neutrality rules he staunchly opposed. With a Republican majority on the Commission, this spells bad news for net neutrality proponents, and good news for the industry.

As for privacy, Trump's executive order on enhancing public safety limits privacy protection only to US citizens. This regulation could invalidate the Privacy Shield, which safeguards the privacy rights of EU citizens in transatlantic data flows.

The European Commission issued a statement that the Privacy Shield will remain, while in an interview in Malta, Euro-

pean Commissioner Vera Jourova said the EU needs reassurance from the USA.

New cybersecurity measures are expected in the coming days. More executive orders are expected to be signed, as stakeholders watch closely for potential implications for global digital policy.

IGF PREPARATIONS KICK OFF

No sooner had the IGF 2016 ended than preparations for the 2017 meeting kick-started. In January, stakeholders were invited to submit contributions on what worked last year, and what can be done to improve the overall IGF process this year.

The IGF community wrapped up its 2016 inter-session work with the publication of the final outputs of the Policy Options for Connecting and Enabling the Next Billion(s) initiative, and of the four best practice forums on gender, Internet exchange points (IXPs), Internet protocol version 6 (IPv6), and cybersecurity.

The next IGF, to be held on 18–21 December, can capitalise on the uniqueness of the host city – Geneva – which is the seat of many international and technical organisations covering more than 50% of international digital policy.

[Continued on page 3](#)

Panellists debating the future of work during the World Economic Forum Annual Meeting on 17-20 January. Read our report on the meeting on page 2. The impact of the digital economy on jobs is also one of the undercurrents affecting digital policy developments in 2017. [More on page 7](#)



Credit: World Economic Forum

IN THIS ISSUE

BAROMETER

The observatory looks at the global developments in January. Sustainable development, e-commerce, and legal issues were particularly prominent.

[More on pages 4 and 5](#)

LOOKING BACK AT 2016

In 2016, the digital policy year was marked by important developments affecting many issues. Read our round-up of the top 20 developments.

[More on page 6](#)

PREDICTING 2017

In 2017, we can expect unsettled weather, which will be stormy at times. But crisis opens new possibilities for sunny spells.

[More on page 7](#)

CROSSWORD

On the occasion of Data Protection Day, test your knowledge of the topic, your recognition of key words, legal instruments, and names of individuals who have left their mark.

[More on page 8](#)

Published on 31 January 2017, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Ana Andrijević, Stephanie Borg Psaila, Jovan Kurbalija, Marilia Maciel, Aida Mahmutović, Virginia (Ginger) Paque, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatović, Diplo's CreativeLab | The Brazilian version in Portuguese is available at dig.watch/newsletter | In addition to the Geneva Digital Watch newsletter, you can find in-depth coverage of developments on the GIP Digital Watch observatory (dig.watch) and join discussions on the last Tuesday of every month online, at local hubs, or at the Geneva Internet Platform (dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu

Le Numérique au Service de l'Humanité

The International Geneva Perception Change Project of the United Nations Office at Geneva, in collaboration with Fondation Eduki, organised a session dedicated to the Internet in the service of humanity, on 18 January 2017.[\[1\]](#) The event, presented as a press conference, focused on the use of the Internet in relation to humanitarian disasters, e-commerce, freedom of expression, and the work of the UN and its different partners.

Just-in-time course on Internet Governance

The course,[\[2\]](#) offered by the GIP and DiploFoundation from 23 January to 26 March 2017, assists permanent missions in Geneva in actively following the field of digital politics. While improving their knowledge of digital politics, participants will also gain the practical skills and knowledge required to follow current Internet-related processes, such as privacy and data protection, e-commerce, and cybersecurity. The course uses a blended learning technique, combining dynamic exchange in an online classroom with weekly lunchtime learning sessions at the GIP.

CSTD 2016–2017 Inter-Sessional Panel

At its 2016–2017 inter-sessional panel on 23–25 January,[\[3\]](#) the UN Commission on Science and Technology for Development (CSTD) discussed innovative approaches to support the implementation of the sustainable development goals (SDGs), and the role of science, technology, and innovation in ensuring food security by 2030. Members of the Commission also looked at the progress made in the implementation of the outcomes of the World Summit on the Information Society (WSIS), at regional and international level, paying particular attention to the linkages between the WSIS process and the 2030 Agenda for Sustainable Development.

Second meeting of the CSTD Working Group on Enhanced Cooperation

The second meeting of the CSTD Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (WGEC),[\[4\]](#) on 26–27 January, was dedicated to discussions on two broad questions: (1) What are the high-level characteristics of enhanced cooperation? (2) Taking into consideration the work of the previous WGEC and the Tunis Agenda for the Information Society, particularly paragraphs 69–71, what kind of recommendations should be considered? Participants focused on the first question and identified a set of high-level characteristics that enhanced cooperation should present, including being transparent, inclusive, result-oriented, and responsive to innovation, and giving consideration to underrepresented groups. There were divergent views on the role of non-governmental stakeholders in the policy process, and on whether new mechanisms are needed. The next meetings are expected to take place in May and October.

ITU Cybersecurity Workshop: Cybersecurity and Risk Assessments in Practice

The workshop,[\[5\]](#) on 27 January, explored the practical implications of assessing cybersecurity risks at national level, in large organisations, and at the level of critical infrastructures. After a broad discussion on top security threats in 2017 and beyond, participants exchanged information and experiences regarding strategies, tools, and methodologies used for assessing cyber risks within their entities. The role of standards and standardisation organisations in managing cybersecurity vulnerabilities and risks was also discussed.

WORLD ECONOMIC FORUM LOOKS AT THE FUTURE OF THE DIGITAL ECONOMY

The 47th WEF Annual Meeting, which took place in Davos-Klosters, Switzerland, on 17–20 January,[\[6\]](#) brought together leaders from across business, government, international organisations, academia, and civil society, to discuss several digital policy issues.

The future of the digital economy was an overarching theme for many sessions, exploring aspects such as the digital transformation of industries, the fourth industrial revolution and its implications (in areas such as gender equality and jobs), the need for shared norms and rules for the digital economy, and trust-based collaboration among stakeholders. Security and crime in the digital era were part of the discussions. During the meeting, WEF launched a report on *Advancing Cyber Resilience: Principles and Tools for Boards*,[\[7\]](#) which outlines a series of principles and tools for companies to tackle cybersecurity risks and ensure the resilience of their information infrastructures.

The advancements in the field of Internet of Things (IoT) and artificial intelligence (AI) were also discussed, as participants explored policy implications and outlined the need for principles

and standards to ensure that IoT and AI products bring benefits to society as a whole, while minimising the risks. Trustworthy online information, a topic that has attracted a lot of attention lately, was also discussed, with a focus on possible modalities for balancing freedom of expression with the need to educate users on how to differentiate between real and misinformation.

WEF participants took the opportunity to launch new initiatives and agree on future actions. In one example, major financial service providers, global IT and telecom companies, and UN entities agreed on six principles on public-private cooperation aimed at facilitating digital cash payments in crisis-affected populations.[\[8\]](#)

As has been the case at many other high-level events recently, the Agenda for Sustainable Development also featured high in Davos. World leaders discussed the challenges of globalisation and the increasing anti-globalisation trends. Many of the debates revolved around the need to identify modalities for reforming the governance of globalisation processes,[\[9\]](#) with a view to making them better suited to contribute to global growth and development.

DIGITAL POLICY TRENDS IN JANUARY

Continued from page 1



The IGF can also capitalise on the vibrant digital research scene involving CERN (the European Organization for Nuclear Research), the EPFL (École polytechnique fédérale de Lausanne), and the University of Geneva.

CYBER-SAGA BETWEEN THE USA AND RUSSIA CONTINUES

A new report by the US intelligence services, published in early January, concludes with 'high confidence' that the Russian President was behind an influence campaign aimed at the US Presidential election. Russia has denied these accusations. Meanwhile in Russia, three cybersecurity specialists connected to the Kremlin were arrested over allegations that they were spying for Washington.

The ongoing tension between the USA and Russia marked the beginning of the year, sparking more concern over the ability of the two countries to resolve their cyber-tensions. It remains to be seen whether the new US administration will make a difference.

SETTING THE SCENE FOR 2017

The predictions for 2017 are based on a backdrop that is influencing digital policy developments, one that will test long-standing notions related to Internet development.

Over the last two decades, globalisation and the growth of the Internet have been closely related. Looking ahead, the crisis of globalisation will have an unavoidable impact on the Internet: if the crisis leads to further restrictions in the movement of

people, capital, and goods across national borders, the same is likely to happen with Internet traffic – in addition to a more fragmented Internet which could affect many segments of society.

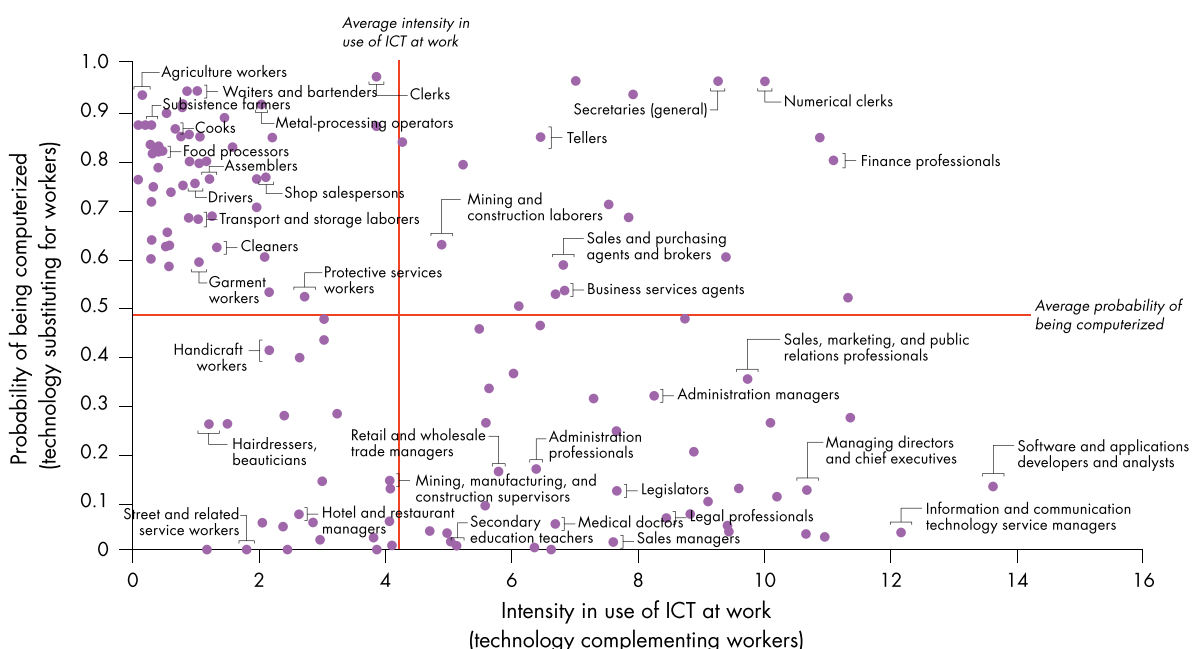
Jobs and employment, which will be high on political agendas in 2017, are directly affected by the digital economy. An increase in digital technology is often interpreted as leading to fewer available jobs.

According to the World Bank's 2016 *World Development Report*, jobs held by hotel and restaurant managers are less likely to be automated, while financial professionals are most likely to be replaced by computers. The digital industry, will increasingly come under pressure to contribute to solving the social costs of fast digital developments.

The adage that the Internet changes the way we live, work, and entertain has become a daily reality. Gadgets are evolving from interesting to essential devices, affecting our daily routines and deeper cultural patterns.

Discussion on the social impact of the Internet must be carefully balanced. While our goal might be to address the negative aspects (reduction of social cohesion and solidarity, less critical thinking), we may end up undermining numerous positive digital developments.

It is against this backdrop that digital policy is expected to develop in 2017. More on page 7. Turn to pages 4-5 for more digital policy developments in January.



The World Bank's 2016 *World Development Report* illustrates the impact of technology on jobs. Credit: World Bank

DIGITAL POLICY: DEVELOPMENTS IN JANUARY

Global IG Architecture



increasing relevance

The IGF community wrapped-up its 2016 intersessional work, with the publication of the final outputs of the Policy Options for Connecting and Enabling the Next Billion(s) initiative, and of the four best practice forums on gender, IXPs, IPv6, and cybersecurity. Preparations for the 2017 cycle have already started, as stakeholders have been invited to submit contributions on how to improve the IGF process.

Members and observers of the CSTD Working Group on Enhanced Cooperation gathered for the group's second meeting to discuss the characteristics of enhanced cooperation in Internet governance, and possible modalities for achieving it. [More on page 2.](#)

Sustainable development



increasing relevance

At its 2016-2017 Inter-Sessional Panel, the CSTD looked at how the implementation of the SDGs could be supported by innovative approaches, and discussed further linkages between the 2030 Agenda for Sustainable Development and the outcomes of the WSIS process. [More on page 2.](#)

The *Inclusive Growth and Development Report 2017*, published by WEF, underlined the slow growth and rising inequality at global level, and suggested several policy and institutional approaches that could contribute to more sustainable and inclusive growth and development. Among the recommendations, enhancing access to Internet services and infrastructure and maximising the growth and employment potential of Internet-enabled trade were seen as particularly important. [More on page 2.](#)

The first UN World Data Forum was marked by the launch of the *Cape Town Global Action Plan for Sustainable Development Data*. The plan calls for recognition of the fact that national statistical systems are essential to the full implementation of the Agenda 2030, and proposes a series of objectives and actions for addressing key statistical capacity building needs.

Security



same relevance

In the USA, a report published by intelligence services concluded, with 'high confidence', that 'Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election'. The expert community, however, commented that the report does not provide sufficient information for attributing, with high certainty, the attacks to the Russian authorities.

Cellebrite, an Israel-based company that offers services of breaking into protected mobile phones (including to governments and law enforcement agencies around the world), confirmed a breach of its servers. The event has sparked concern that the company's encryption-breaking technology could be sold to the highest bidder.

The US Federal Trade Commission (FTC) filed a lawsuit against Taiwan-based computer networking equipment manufacturer D-Link for failing 'to take reasonable steps to secure its routers and Internet Protocol (IP) cameras, potentially compromising sensitive consumer information'. D-Link denied the accusations. A report released by the Ponemon Institute has revealed that around 80% of IoT applications and 71% of mobile applications are not tested for vulnerabilities, raising security concerns.

The Federal Security Service in Russia announced that major commercial banks in the country were targeted by a massive cyber-attack by hackers in November last year. A report from security firm Risk Based Security reveals that the year 2016 set new records in terms of data breaches: there were 4,000 data breaches reported over the year, exposing over 4.2 billion records.

E-commerce & Internet economy



increasing relevance

Colombia has passed new rules that impose a 19% value added tax on Internet services paid by credit card, primarily targeting over-the-top (OTT) services such as Netflix, Uber, Spotify, and AirBnB. In Canada, the government is considering imposing a so-called Netflix tax on digital services bought from foreign companies over the Internet.

In the UK, thousands of eBay and AirBnB users are being pursued by the British tax office for not declaring their earnings through the 'sharing economy'. The government of Indonesia has started an investigation into Google's tax practice, accusing the company of owing the state more than \$25 million in taxes.

Digital rights



same relevance

At the conclusion of their 12th Human Rights Dialogue (in Brussels on 10 January), the African Union and the EU expressed their commitment to promoting and protecting freedom of expression and the right of access to information in the digital age. The European Court of Human Rights has ruled that security concerns are not a sufficient reason to deny a prisoner Internet access, as this represents a violation of the prisoner's right to freedom of expression.

The European Commission has proposed a new set of privacy rules, also applicable to Internet companies. Turkey has announced plans to develop a domestic search engine and email service compatible with its national culture and values while a new regulation in Vietnam will enable the Ministry of Information and Communications to demand that content providers take down or block content representing 'ill-intended and toxic' information.

David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of expression, has warned that age-verification checks introduced by the UK government to prevent children from accessing online pornography could 'give the government access to information of viewing habits and citizen data', which would breach international law.

Jurisdiction & legal issues



increasing relevance

In the Microsoft case, the court's ruling over data held in Ireland stands, after the US Court of Appeals for the Second Circuit denied a rehearing of the case.[↗](#)

Uber and the Roads and Transportation Authority (RTA) in the Emirate of Dubai have signed an agreement[↗](#) under which the company will be able to use 14,000 vehicles through its app 'as per the laws governing the operation of taxis and limousines in Dubai emirate'.

The Committee on Legal Affairs in the European Parliament has adopted a report[↗](#) outlining recommendations for the introduction of 'civil law rules on robotics'. The report, published in draft version in May 2016, proposes the elaboration and adoption of an EU 'legislative instrument' to tackle legal questions related to the development of robotics and AI.

In China, the government has launched a campaign aimed at shutting down providers of services such as virtual private networks and content delivery networks, which do not have authorisation 'to run cross-border operations'. These services are often used to bypass Internet restrictions in China.[↗](#)

Infrastructure



same relevance

The government in Cameroon ordered an Internet shutdown to the country's two main English-speaking regions, after Anglophone teachers, lawyers, and students went on strike over alleged bias in favour of Francophones.[↗](#) The regions have been without Internet since mid-January.

The Marshall Islands have faced several weeks of Internet blackout, due to problems with an undersea fibre optic cable. While phone and Internet communications have been switched to satellite, authorities have limited access to email and important facilities like airports, emergency services, etc.[↗](#)

ICANN and the US government have agreed[↗](#) to terminate the Affirmation of Commitments (AoI), a 2009 document which outlined, among others, ICANN's commitments to openness and transparency, and regular community reviews of its work. These commitments are now incorporated into the revised ICANN by-laws.

Net neutrality



increasing relevance

The net neutrality rules adopted by the US FCC in 2015 might be at risk, as the Commission's newly appointed chairman is expected to initiate a review.[↗](#) Meanwhile, in a report outlining the results of a policy review conducted in 2016,[↗](#) the FCC expressed concerns over AT&T's and Verizon's zero-rating services, seen as presenting significant risks to consumers and competition.

The Telecom Regulatory Authority in India (TRAI) has launched a new public consultation on net neutrality,[↗](#) asking for input from stakeholders on the core principles of net neutrality and practices that might be seen as violating these principles.

New technologies (IoT, AI, etc.)

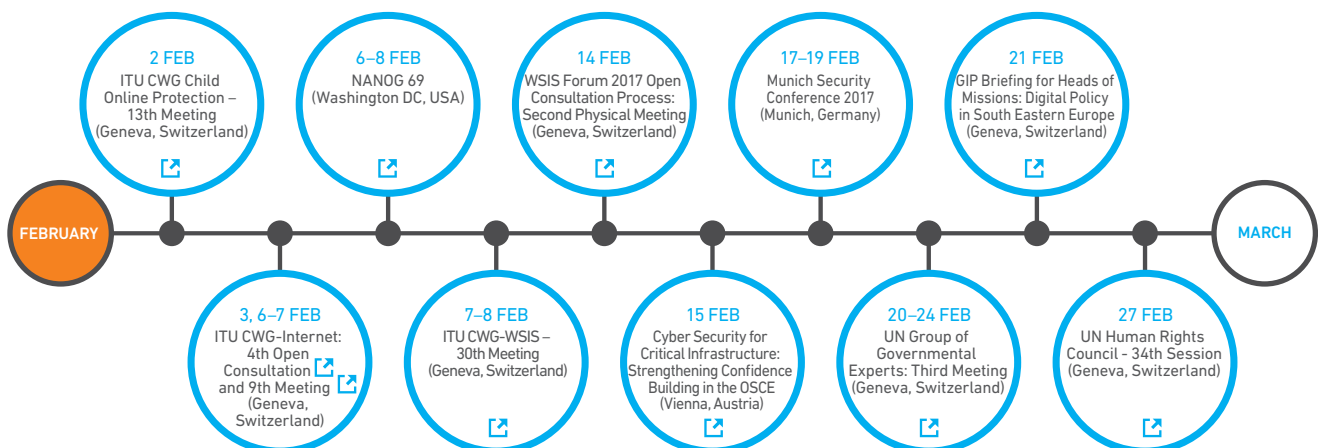


same relevance

In the USA, four senators have reintroduced[↗](#) a draft bill aimed at ensuring 'appropriate spectrum planning and interagency coordination to support the IoT'. In parallel, the country's Department of Commerce (DoC) has issued a *Green Paper on Fostering the Advancement of the IoT*,[↗](#) outlining several principles aimed at guiding any future DoC activities in this area. The paper was accompanied by the launch of a public consultation[↗](#) inviting comments on potential roles for the government in sustaining IoT development.

The European Telecommunications Standards Institute has launched[↗](#) an Industry Specification Group on cross-sector Context Information Management for smart cities applications and beyond, to work on the development of specifications and protocols for smart cities interoperability.

AHEAD IN FEBRUARY



For more information on upcoming events, visit dig.watch/events

LOOKING BACK AT DIGITAL POLICY DEVELOPMENTS IN 2016

The digital policy year in 2016 was marked by several important developments, covering issues ranging from privacy and data protection to cybersecurity, and from jurisdiction to the IoT and AI. In this review, we look at the top 20 developments.

1. Cyberpeace: between Cold War and *détente*. Several developments illustrated the securitisation of cyberspace: from the cyber tension between the USA and Russia, [to](#) NATO declaring cyberspace as an operational domain. [to](#)

2. Apple/FBI case brings privacy, security, encryption, and surveillance into sharper focus. Apple's refusal [to](#) assist the FBI in unlocking a cell phone [to](#) triggered intensive debates.

3. Tech companies enhance encryption for users. In the aftermath of the Apple/FBI controversy, tech companies sought to enhance or tighten encryption, with the aim of protecting users' right to privacy.

4. Measures are introduced to combat violent extremism online. Companies worked on deleting social media accounts, [and](#) filtering content, [while](#) the issue was discussed by the UN Security Council, [the G7,](#) [and](#) BRICS. [to](#)

5. Cybercrime increasingly exploits vulnerabilities. Cyber-attacks increased and became more sophisticated, ranging from theft of user information [to](#) exploitation of zero-day flaws [and](#) cyber-espionage. [to](#)

6. DDoS attacks bring IoT security into sharper focus. Large attacks utilising smart devices [generated](#) discussions on the responsibility of vendors for the security of their products, and on the need for standards.

7. Artificial intelligence: new applications and growing concerns. As progress continued (e.g. self-driving cars, [applications](#) for automatic detection of hate speech online [to](#)), policymakers started exploring more carefully the social, economic, and ethical implications.

8. SDGs and Internet access permeate digital policy discussions. Several discussions solidified the view that efforts to connect the unconnected contribute to attaining the SDGs. Innovative solutions for increasing universal access attracted more attention.

9. Debates on data governance increase after a series of data breaches Issues of data protection and security have risen on the political agenda, and governments are increasingly adopting data localisation rules.

10. Privacy Shield is adopted; framework replaces Safe Harbour. The new EU-US Privacy Shield for transatlantic exchanges of personal data [was](#) challenged in court. [to](#)

11. Courts rule on privacy, and data retention. Judgments shaped the application of users' right to privacy, in cases involving employers access to employees' communications, [and](#) general data retention by Internet providers. [to](#)

12. Continuation of restrictions to Internet services. Restrictions to Internet services worldwide raised concerns over freedom of expression. The UN Human Rights Council called on countries to refrain from such measures. [to](#)

13. New guidelines on net neutrality emerge alongside fresh debates on zero rating. In the EU, stronger net neutrality rules were introduced. [In](#) the USA, Facebook initiated talks with the government over Free Basics, [while](#) the service was banned in India. [to](#)

14. Digital revolution fosters economic growth. This message was stressed at the G20 Leaders' Summit, [and](#) underlined by UNCTAD when launching the eTrade for All initiative. [to](#)

15. New guidelines for the sharing economy were issued by the European Commission. [to](#) addressing concerns over the uncertainty of rights and obligations arising from the sector. Courts were asked whether Uber is a transport service provider or a digital platform.

16. Apple ordered to pay Ireland €13 billion in taxes; other companies hit by new investigations. In motivating its order, the European Commission argued that the Apple-Ireland agreement involved unlawful state aid. [to](#)

17. Court cases tackle intellectual property rights. Google's Java case was a major win for proponents of the fair use principle. [In](#) the EU, new copyright proposals [were](#) met with mixed reactions.

18. Fake news and filter bubbles make the headlines. In the context of the US Presidential election, the role of intermediaries in the spread of false news attracted attention. [Should](#) they be de facto regulators of content?

19. Microsoft case delineates extent of jurisdiction. A US court ruled that the government could not use a search warrant to force Microsoft to turn over e-mail communications stored in Ireland. [to](#)

20. IANA stewardship transition is completed. Despite last-minute developments, the stewardship of the IANA functions was transitioned from the US government to the global Internet community. Work on enhancing ICANN's accountability continued throughout the year. [to](#)

FORECAST FOR 2017: UNSETTLED WEATHER, STORMY AT TIMES, WITH SUNNY SPELLS

The political and economic turbulence ahead will lead to unsettled weather. But crises open new possibilities. Digital growth is expected to accelerate, and to further test the 'techno-absorption capacity' of modern society. Set against a backdrop of the globalisation crisis, the impact of the digital economy on jobs, and the impact of the Internet on society, how exactly will digital policy developments be influenced? What follows are the top predictions for 2017.

Cyber geopolitics: between conflict and cooperation

The cybersecurity discussion will focus more on the vulnerabilities of modern society and possible ways to overcome cybersecurity risks. The topic will surface in debates on national security, the fight against violent extremism, and ensuring the personal security of Internet users. At international level, cybersecurity will feature prominently on the agendas of the G7, the G20, and other high-level events.

Encryption: security and privacy

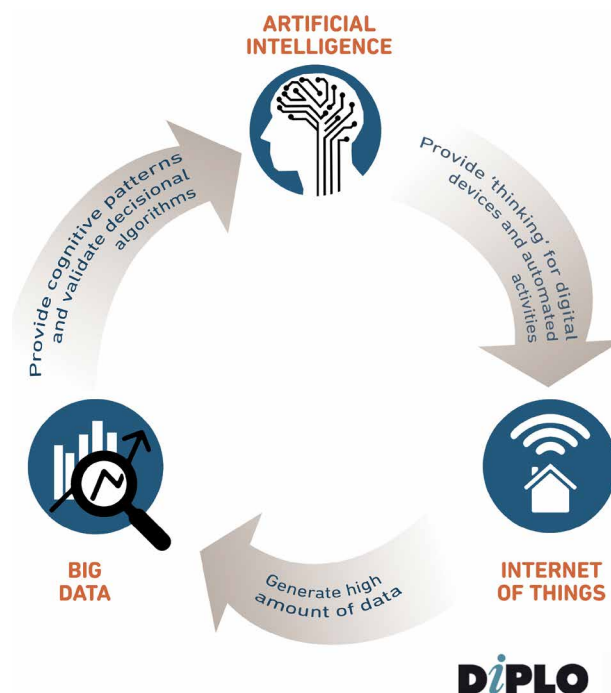
Last year's Apple/FBI controversy gave rise to many dilemmas surrounding the balance between privacy and security. These dilemmas are expected to resurface this year, and, sooner or later, stakeholders will need to reach a compromise. Public-private partnership could be a compromise arrangement which would ensure the protection of public interest and avoid heavy regulatory pressure on the Internet industry.

Content policy, fake news, and violent extremism content

Combating violent extremism online will remain high on the policy agenda in 2017. In addition, a solution will be sought to the question of 'fake news', oscillating between holding Internet companies responsible and focusing more on improving social media literacy among Internet users.

Powerful interplay: AI – IoT – Big data

As the interplay between AI, IoT, and big data is likely to be further strengthened in 2017, governments and the private sector will continue to explore implications (and possible solutions) in areas such privacy and security, social and economic consequences, ethics, and accountability.



The interplay between the three technology sectors of AI, the IoT, and data is likely to be further strengthened in 2017.

Data governance and data localisation

Two trends are likely to dominate in 2017. First, data governance will need to be addressed in a more comprehensive way, since a solution aimed at one area may directly affect other aspects. Second, we can expect further pressure on data localisation requirements, with increased costs for Internet businesses.

Digital trade and the Internet economy

Digital trade, as an engine of economic growth, could be a way of containing the protectionist wave expected in 2017. This could be best illustrated in the EU, where the digital single market may have wider strategic relevance: if further harmonisation is achieved, this may help to reverse the current anti-integration tide in the EU policy space.

ICANN after the IANA transition

For years, ICANN-related issues have been at the top of the policy agenda. This is unlikely to be the case in 2017, as the IANA stewardship transition is not likely to be reversed by the new US administration. ICANN's main focus in 2017 will be on the new generic top level domains. A potential controversy could be triggered by the question of jurisdiction of US courts over ICANN.

Digital policy shaped by court decisions

In 2016, courts played an increasingly important role in shaping digital policies. This development is likely to accelerate in 2017 with national and regional courts filling digital policy gaps and addressing questions of cybercrime, content removal, role of intermediaries, freedom of expression, protection of personal data, and mandatory data retention requirements, to name a few.

Connecting the dots among digital policy silos

In 2017, many activities will focus on mapping common elements and identifying 'boundary spanners' that will create linkages between different digital policy silos. These include, among others, the CSTD Working Group on Enhanced Cooperation, the WSIS Forum, the WTO Public Forum, and the IGF.

Digital realpolitik: from values to interests

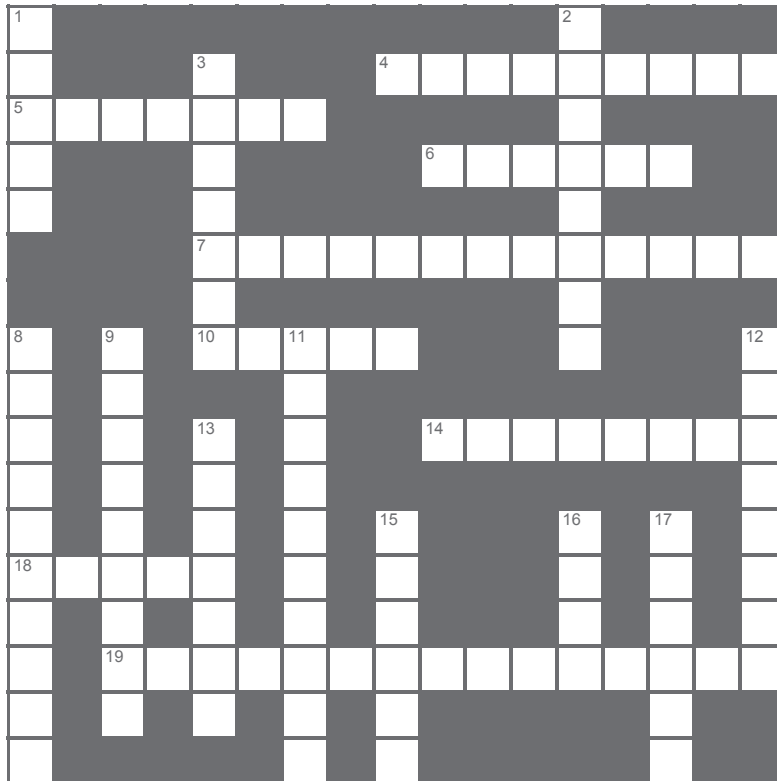
The global shift to realpolitik could trigger several major consequences in the digital policy field. Realpolitik may politicise issues dealing predominantly with technical aspects such as digital standards. It may also challenge the inclusiveness principle that has been introduced in the digital policy ecosystem over the past few decades, and may create a shift from global discussions towards bilateral deals and plurilateral arrangements. On the positive side, realpolitik may deflate digital policy bubbles and contribute towards creating a basis for more solid and sustainable technological development.

Adapted from Dr Jovan Kurbalija's *Digital Politics in 2017: Unsettled Weather, Stormy at Times, with Sunny Spells*. Read the full text for a more comprehensive overview of these predictions. The text also describes the context for the 2017 developments in more detail, and lists the main events to watch out for.

TEST YOUR KNOWLEDGE ON PRIVACY AND DATA PROTECTION

The 11th anniversary of Data Protection Day (also known as Privacy Day, outside Europe) fell on 28 January. Initiated by the Council of Europe (CoE) as the date the Data Protection Convention - or Convention 108 - was opened to signature, it is currently marked in 47 European countries, and the United States, Canada, and India. The initiative is focused on raising awareness about privacy through education.

Complete our crossword and test your knowledge of Privacy and Data Protection, recognising key words, legal instruments, and names of individuals who have left their mark.



Across

- 4 A digital _____ is used as a method of authenticating the identity of individuals on the Internet. (9)
- 5 A _____ private network allows users to create a secure network connection over a public network, such as the Internet. (7)
- 6 A term used to refer to an individual who uses advanced computer skills to penetrate into or misuse computers. (6)
- 7 The whistleblower who, in May 2013, leaked top secret information about the NSA's surveillance activities. (6,7)
- 10 Identity _____ is the act of stealing another individual's personal information to impersonate the victim, often for financial gain. (5)
- 14 The _____ Charter is the nickname given to the UK's Investigatory Powers Act 2016. (8)
- 18 The abbreviation for a protocol for secure and private communication over a computer network which is increasingly deployed by Internet companies. (5)
- 19 A term which describes the principle of keeping personal data private or restricted to authorised persons. (15)

Down

- 1 The International Covenant on _____ and Political Rights is one of the main global legal instruments for the protection of privacy. (5)
- 2 A term used to describe a software code that gives access to a program or service, circumventing normal security protections. (8)

- 3 A data _____ is the term used in legislation to describe an individual to whom the data relates to. (7)
- 8 An Austrian lawyer and privacy activist who requested the Irish data protection watchdog to investigate Facebook's European privacy practices leading to the invalidation of the Safe Harbour framework. (3,7)
- 9 Family/last name of the first-ever Special Rapporteur on the right to privacy. (9)
- 11 The process of converting information or data into a code, in order to prevent unauthorised access. (10)
- 12 A 2014 resolution of the UN General _____ calls upon member states to 'respect and protect the rights to privacy, including in the context of digital communications'. (8)
- 13 A person must be specifically asked for it, if their sensitive personal data are to be processed. (7)
- 15 The Privacy _____ is the name of the new framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. (6)
- 16 Acronym for a controversial US draft bill which aimed at expanding the ability of the US law enforcement to combat online copyright infringement and online trafficking in counterfeit goods. (4)
- 17 A privacy _____ is a document that clearly defines the way a party gathers, uses, discloses, and manages a customer or client's data (Hint: The text that many users usually skip to read by clicking 'Next') (6)

Across: 4 Signature, 5 Virtual, 6 Hacker, 7 Edward Snowden, 10 Theft, 14 Snoopers, 18 HTTPS, 19 Confidentiality.
Down: 1 Civil, 2 Backdoor, 3 Subject, 8 Max Schrems, 9 Carnataci, 11 Encryption, 12 Assembly, 13 Consent, 15 Shield, 16 SOPA, 17 Policy.



Subscribe to GIP Digital Watch updates at www.giplatform.org/digitalwatch