Geneva Internet Platform
DigitalWatch
NEWSLETTER

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

# DIGITAL POLICY TRENDS IN OCTOBER

Developments in October presented a different kind of dynamics than in previous months. Cybersecurity was at the forefront for several reasons, as were the emerging technologies of the Internet of Things (IoT) and Artificial Intelligence (AI). The interplay between innovative technologies and security considerations was among the dominant themes, not least because of the unprecedented cyber-attacks that took place during the month.

## 1. IOT DEVICES USED IN MASSIVE DDOS ATTACKS

It is estimated that the global IoT market will grow to 27 billion devices by 2025. But to take advantage of the innovative solutions and unparalleled technological advances, security risks need to be tackled. This month's widespread attacks utilising Internet-connected devices are proof enough that IoT security is a pressing concern.

The distributed denial of service (DDoS) attack on 21 October, which infected hundreds of thousands of devices, rendered major websites inaccessible, including Twitter, PayPal, Netflix, Airbnb, Amazon, CNN, and several online journals. Security and video cameras, baby monitors, and video recorders that can connect to the Internet were some of the devices used in the attack.

The attack was directed at systems operated by Domain Name System services provider Dyn. Although the company fended off the first attack, it was under a second and third attack the same day.

This was not the first DDoS attack in October. Earlier this month, more than a million devices were used in attacks on a US security researcher and a French network service provider. What both attacks have in common is the unprecedented scale at which they happened.

The attacks bring IoT security into sharper focus, prompting countries to act. In the USA, the National Telecommunications and Information Administration (NTIA) launched an initiative aimed at ensuring that security vulnerabilities in IoT devices are mitigated through patches and security upgrades. In the EU, the Commission is about to propose new IoT-security legislation, to encourage companies to come up with a labelling system for Internet-connected devices that are approved and secure.

*Continued on page 3*

# US ELECTIONS AND DIGITAL POLICY

Millions of people are following the US Presidential election campaign very closely. Both candidates have addressed a large number of digital policy issues in their public speeches, from infrastructure and online taxation, to privacy and cybersecurity. Since the digital policies of the future US president will have a global impact, this issue provides a survey of the candidates' views on core digital issues.

*More on page 7*

# IN THIS ISSUE



Published on 31 October 2016. In addition to this newsletter, you can find in-depth coverage on the *GIP Digital Watch* observatory (http://digitalwatch.giplatform.org) and join live discussions on the last Tuesday of every month online, at local hubs, or at the Geneva Internet Platform premises | The Geneva Digital Watch newsletter is published by the Geneva Internet Platform and DiploFoundation | Design by Viktor Mijatovic, Diplo's CreativeLab | Contributors to this issue: Stephanie Borg Psaila, Foncham Doh, Tereza Horejsova, Jovan Kurbalija, Jacob Odame, Virginia Paque, Roxana Radu, Barbara Rosen Jacobson, Sorina Teleanu | Send your comments to digitalwatch@diplomacy.edu. The Brazilian version in Portuguese is available at http://digitalwatch.giplatform.org

## GENEVA DIGITAL DEVELOPMENTS

**ITU CWG-Internet meetings**

On 11 October, the ITU Council Working Group on International Internet-related Public Policy Issues (CWG-Internet) held a meeting dedicated to discussions and sharing of experiences and best practices on 'Building an enabling environment for access to the Internet' – a topic that was the subject of an online consultation between February and September 2016. The event started with a panel discussion setting the stage, and continued with an overview of the contributions from stakeholders to the online public consultation. Some of the key elements identified in the contributions were: free flow of information, open access to data, the importance of sustainable development, and the role of governments and regulators in building confidence and security in the use of the Internet. While there was support for these principles, views diverged on how they might be implemented. At the 8th meeting of CWG-Internet (13–14 October 2016), a new open consultation was launched on 'Developmental Aspects of the Internet', with contributions to be received by 4 January.

**ITU CWG Child Online Protection – 12th Meeting**

The ITU Council Working Group (CWG) on Child Online Protection met for a full-day discussion, on 10 October. The meeting included a high-level dialogue on child online protection, co-organised by the ITU and the Council of Europe, as well as an update of ITU's Child Online Protection initiatives and activities. The CWG furthermore discussed initial results of its online consultation on cyberbullying. Finally, member states and other participants shared their views and experiences with regard to the subject of the consultation.

**ITU CWG-WSIS – 29th Meeting; first physical open consultation for WSIS Forum 2017**

The first physical meeting of the WSIS Forum 2017 Open Consultation Process was held at the ITU Headquarters, on 12 October. It specifically addressed issues related to the thematic focus and format of the Forum. The meeting discussed additional elements, such as a hackathon, TEDx, and the topic of virtual reality for sustainable development. The event took place in the context of the 29th meeting of the ITU Council Working Group on WSIS (CWG-WSIS), held on 12 and 13 October. This meeting featured, among others, discussions on activities and projects related to the implementation of WSIS action lines, as well as updates on sustainable development goals (SDGs) related activities.

**What's the problem with TTIP?**

This session, held on 18 October at the Graduate Institute of International and Development Studies, covered issues at stake regarding the Transatlantic Trade and Investment Partnership (TTIP) from a legal and economic perspective. The controversy around the TTIP stems from a number of sources. Some panelists insisted on the fact that the TTIP would not solve some major issues in Europe including the problem of job growth and Europe's disadvantages in terms of size and market power in comparison with the USA. Other speakers stressed the importance of building a strong cooperation between the USA and Europe, but also with developing countries that are growing economically, militarily, and technologically. The application of the Investor-State Dispute Settlement (ISDS) within the TTIP was also highlighted during the discussion, even though its necessity remained contested.

## EVENT REPORT

# INTERNET AND DEVELOPMENT: A REALITY-CHECK

How can we create a more inclusive Internet? What are the practical steps we can take to expand global connectivity?

These were some of the questions addressed at 'Internet Inclusion: Global Connect Stakeholders Advancing Solutions'. The event was attended by leaders from some of the Internet's main organisations and businesses, in Washington on 5 October.

Last year, the international community took on a historical commitment through the adoption of the SDGs, with the Internet having a central role in reaching them all.

It is generally assumed that the Internet boosts development. However, although evidence of the Internet's inherent power is growing, the assumption of the Internet being an engine for development does not apply automatically. Development is also too complex to be reduced only to access to the Internet.

The Internet can make a real impact if we address the gap between possibilities and realities in an open, collaborative and constructive way, and at all levels of governance. All of the Internet's stakeholders hold a piece of the puzzle:

- **Expanding infrastructure:** The private sector needs to invest for the infrastructure to provide Internet access and to create and host services, leaving governments to prioritise areas with high costs or low demand.
- **Fostering skills and entrepreneurship:** A skilled technical community is necessary to deploy and operate access and content infrastructure. It is also necessary to develop human capacity so that there are entrepreneurs, developers and others to create content and services, and the innovative new business and delivery models built on them.
- **Developing a supportive governance system:** Good governance is needed to set the principles and rules of an enabling environment for a local Internet ecosystem, and specific policies to promote infrastructure investment and human capacity. Governments can also deploy their own content and services and encourage people to make the most of the Internet.

Promoting an Internet that supports the SDGs is not only technical, or only policy, or developmental; it is all of the above.

*Excerpt of a blog post published by DiploFoundation and the Internet Society in the Huffington Post. Read the full version.*

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

# DIGITAL POLICY TRENDS IN OCTOBER

*Continued from page 1*

As in most areas, cybercrime evolves at a faster pace than policy. Creating and maintaining a strong, up-to-date, regulatory environment to ensure the security of IoT devices will present a tough challenge for policymakers.

## 2. MORE BILATERAL CYBERSECURITY AGREEMENTS

States are increasingly concluding bilateral agreements on cyber issues, particularly on cybersecurity. In 2016, over 20 bilateral arrangements were concluded, most of which involved the USA. The arrangements range from dialogues and frameworks for cooperation, to cyber agreements with formal commitments.

The latest is India and Russia's formal cyber agreement, signed on the margins of the 8th BRICS (Brazil, Russia, India, China and South Africa) Summit. The agreement will tackle cybercrime and combat cyber-terrorism, and will include matters of defence and national security.

Last month, Canada and China also started a series of negotiations for a possible bilateral agreement on cybersecurity, which is expected to tackle cyber-espionage, data theft, and state-sponsored attacks.

We can expect more bilateral cybersecurity agreements in the next few months, as states continue to finalise ongoing arrangements while they embark on new talks to tackle heightened concerns over cyberconflict and the use of ICTs by terrorists.

## 3. TACKLING CHALLENGES RELATED TO ARTIFICIAL INTELLIGENCE

As with IoT, the field of AI is also evolving quickly. It presents opportunities for areas such as health, education, energy, and the environment, and is expected to make significant progress in exhibiting broadly applicable intelligence, even surpassing humans in the performance of certain tasks.

Due to its rapid progress, AI presents new social, ethical, and legal concerns, which authorities have started to evaluate. Among the main concerns are the implications of AI for jobs, skills, and the economy. For example, skills will need to be matched with the needs of a particularly specialised field. The resulting inequality and the likelihood of job losses will also need to be tackled.

The US administration has outlined its strategy for promoting AI research and development, while the UK parliament has asked the government to take proactive measures. Both note, however, that it may be too early to consider sector-wide regulations. *More on page 6.*

## 4. ACCESS TO INTERNET INTERRUPTED

Elections and politically driven motivations were at the heart of three incidents where access to the Internet and to certain Internet applications was interrupted.

WikiLeaks editor-in-chief Julian Assange, who has been ensconced at the Ecuadorian embassy in London for over four years, had his Internet connection partially restricted to stop WikiLeaks interfering with the US election. US officials claimed that Ecuador was pressured to do so by the US government. WikiLeaks recently leaked e-mails from John Podesta, a high-ranking official within Hillary Clinton's presidential campaign.

In a different case, Montenegro blocked Viber and WhatsApp during the country's parliamentary election on 16 October. The service was reinstated after the polling stations closed. The ban was widely criticised as a move to silence opposition, even though the country's Agency for Electronic Communications and Postal Services said that the ban was intended to keep users from receiving 'unwanted communication'. The agency said that mobile users asked for protection from such communication, and the ban 'turned out to be the only option to prevent the distribution of unwanted communication'.

While interference with elections is frowned on and for good reason, measures need to be balanced with the right to freedom of expression. In the US case, online activities get an international dimension: the banning of Assange's activities from the Ecuadorian embassy in London and the alleged involvement of Russian entities.

In Montenegro's case, the main challenge is to apply the traditional election silence practice (24 or 48 hours prior to elections) to the online space. In the pre-Internet era, election silence would have involved the banning of political events and of broadcasting campaigns via TV, radio and other public media. In the Internet era, it is much more difficult to enforce the election silence practice since social media is used for both public promotion and private communications. Many countries will face this challenge of enforcing election silence in the online space.

In a third case, Internet shutdowns in Turkey cut off millions of citizens, following protests against the detention of Diyarbakir's mayor and co-mayor over terrorism charges. The impact of Internet shutdowns is also financial, and can cost countries billions in gross domestic product (GDP), a Brookings report has concluded.

## 5. FREE BASICS CONTROVERSY REIGNITED

Facebook's intention to launch Free Basics in the USA has been a surprise move. The controversial initiative, which provides access only to selected websites rather than the entire Internet, raised red flags in India and Egypt last year, despite being available in more than 40 countries.

Facebook's aim is to connect low-income and rural US citizens. The same plan, however, was rejected by India's Telecom Regulatory Authority after months of intense discussions. The authority had declared that the service violates net neutrality principles.'

The introduction of Free Basics in the USA has re-ignited long-running debates between those who see such services as essential in connecting underserved populations, and those who claim that such services breach net neutrality principles.

The US case, however, is quite particular. Although the country has strong net neutrality rules in place, the rules do not mention zero-rating. Such practices are therefore scrutinised by the Federal Communications Commission (FCC) on a case-by-case basis. In fact, the FCC is probing Internet providers Comcast, T-Mobile, and Verizon over such practices – a process which has already taken many months, and which net neutrality activists are pushing to be resolved 'without delay'.

In order to ensure that Free Basics in the USA does not suffer the same fate as in India and Egypt, Facebook is first engaging in discussions with the White House. Given the imminent elections, it will be interesting to see how the opposing positions of the two Presidential candidates on net neutrality will play out after the elections.

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


Indian citizens protesting against the introduction of Free Basics in India last year. *Credit: www.thehansindia.com*

# DIGITAL POLICY: DEVELOPMENTS IN OCTOBER

## Global IG Architecture

same relevance

Leaders of BRICS countries have emphasised the need to enhance international cooperation against terrorist and criminal misuse of ICTs. The Goa Declaration, adopted during the 8th BRICS Summit on 15–16 October, also recognised the 'leading role of states' in ensuring the stability and security in the use of ICTs, and reaffirmed that the Internet is a global resource.

Preparations for December's Internet Governance Forum meeting are under way. The schedule is now available.

## Sustainable development

same relevance

During its annual debate, the Second Committee of the UN General Assembly (UNGA) called for efforts to bridge the digital divide between and within countries, rural and urban areas, and genders. A side event organised by the UN Department for Economic and Social Affairs (UNDESA) highlighted the role of ICTs in achieving the 2030 Agenda and the potential of ICT policies and their 'analog complements', such as strengthening regulations and ensuring accountable institutions.

## Security

increasing relevance

Two DDoS attacks, utilising many Internet-enabled devices, rendered major websites inaccessible. More than a million devices were used in attacks on a US security researcher and French network service provider. The second attack was directed at systems operated by Domain Name System services provider Dyn, which suffered three attacks in one day; the attacks affected Twitter, PayPal, Netflix, Airbnb, Amazon, CNN, and several online journals.

India and Russia signed a bilateral cybersecurity agreement which will tackle cybercrime and combat cyberterrorism. Canada and China have also started a series of negotiations for a possible bilateral agreement on cybersecurity, which is expected to tackle cyber-espionage, data theft, and state-sponsored attacks. Meanwhile, the US Intelligence Community officially blamed the Russian government for recent cyber-attacks.

The Group of Seven (G7) agreed to a set of cybersecurity guidelines for banks. The guidelines instruct governments to cooperate in continually monitoring and updating cybersecurity systems, both for the governments themselves and the companies they regulate. They also encourage banks and financial institutions to share information about their cybersecurity challenges.

## Privacy & other human rights

increasing relevance

In the UK, the Investigatory Powers Tribunal (IPT) ruled that the fact that access to the datasets of private data had not been subject to sufficient supervision between 1998 and 2015, and that private data were collected from unwitting residents, violated the right to privacy under the European Convention on Human Rights. In the USA, the FCC approved new privacy rules to ensure that broadband providers obtain consumers' permission to collect data.

The Court of Justice of the EU ruled that the dynamic Internet protocol (IP) address of a website visitor constitutes personal data, if the website operator has the legal means of identifying the visitor with additional information held by the Internet access provider. The Court also ruled that a website operator may have a legitimate interest in storing certain personal data relating to visitors in order to protect itself against cyber-attacks.

UN Special Rapporteur on the freedom of opinion and expression David Kaye presented his report on Promotion and protection of the right to freedom of opinion and expression to the UN General Assembly, in which he noted that 'there is no question that governments worldwide are wielding the tools of censorship'.

The European Parliament approved new rules aimed at ensuring that public sector websites and mobile applications are more accessible to people with disabilities.

## Infrastructure

increasing relevance

Rapid developments are being made in the fields of IoT and AI; the recent cyber-attacks utilising IoT devices has now brought security into sharper focus.

In the USA, the NTIA launched an initiative aimed at ensuring that security vulnerabilities in IoT devices are mitigated through patches and security upgrades. In the EU, the Commission is about to propose new IoT-security legislation to encourage companies to come up with a labelling system for Internet-connected devices that are approved and secure.

When it comes to AI, the US administration has outlined its strategy for promoting AI research and development, while the UK parliament has asked the government to take proactive measures.

Microsoft announced plans to open data centres in France, in 2017, to enhance the provision of cloud services across Europe. According to Microsoft, the continuous investment in regional cloud services is intended to respond to European businesses' needs to comply with data sovereignty and security regulations.

## Net neutrality

increasing relevance

Facebook is in talks with US government officials over the possible launch of the Free Basics service in the USA. The service would aim to connect low-income and rural US citizens. Several groups have asked the FCC to prohibit abusive data caps and zero-rating plans 'without delay'.

The Dutch parliament has adopted a revised net neutrality law, aimed at bringing the country's legislation in line with the relevant EU regulation adopted in 2015. Telecom operators, however, see the law as being too severe, and in conflict with EU rules.

## E-commerce & Internet economy

same relevance

A UK employment tribunal has ruled that Uber drivers are employees and should have workers' rights. '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'. The Lithuanian parliament has formally recognised ridesharing services such as Uber and Taxify. Estonia, Latvia, Finland, and Denmark are expected to follow suit.

Facebook has paid £4.2 million to the British tax authorities. The company ceased to route advertising sales through Ireland from 1 April, which will most likely lead to a large increase in tax payable to the UK authorities.

MasterCard will enable the verification of card holders by facial recognition. Users will be able to make payments without the need for PINs or passwords. This technology is available in 12 markets in Europe and is expected to expand in 2017.

## Jurisdiction & legal issues

same relevance

The US Department of Justice has petitioned the Court of Appeals for the Second Circuit in New York for the Microsoft case to be reheard. In July 2016, the District Court ruled that Microsoft cannot be ordered to provide authorities with the contents of a user's e-mails stored on servers outside the USA.

Google.fr and Wikipedia were inaccessible in France after being wrongly added to ISP Orange's terrorism blocking list.

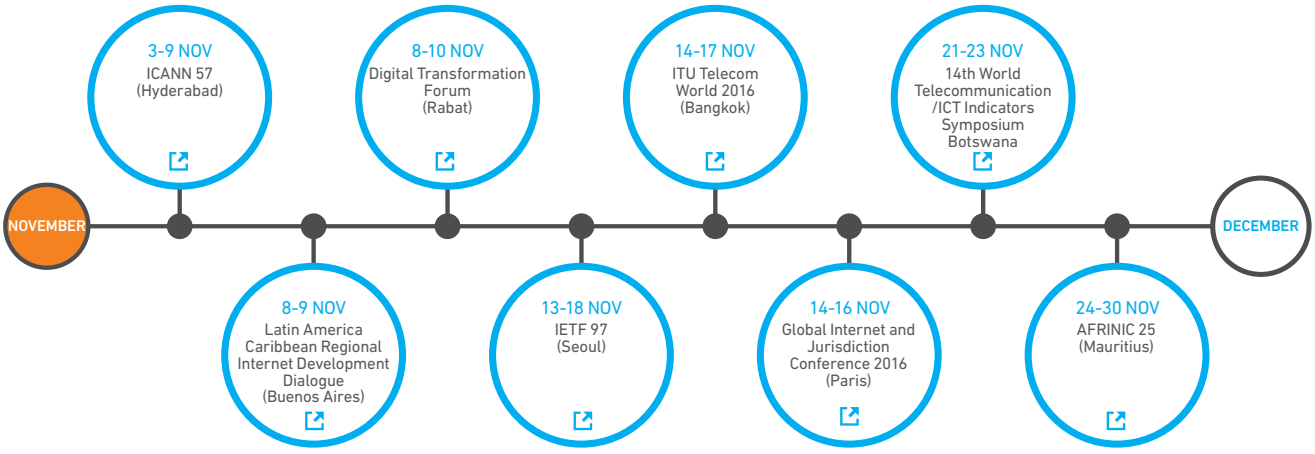
Ecuador blocked Julian Assange's Internet access to prevent WikiLeaks interfering with the US elections. In Montenegro, the regulator ordered telecom operators to prevent access to WhatsApp and Viber on election day, allegedly following users' complaints over 'unwanted communication'. Shutdowns also took place in Turkey amid unrest. The cost of Internet shutdowns can run into billions in GDP, a report has concluded.

## IANA Transition

same relevance

The IANA functions contract between ICANN and the US government expired last month, and the stewardship of the IANA functions transitioned to the global Internet community on 1 October. Meanwhile, the Attorney Generals of Arizona, Oklahoma, Texas, and Nevada – who had filed a last-minute suit to prevent the transition from going forward – filed a notice of voluntary dismissal, dropping their lawsuit against the US government.

## AHEAD IN NOVEMBER




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

# ARTIFICIAL INTELLIGENCE – TOO SMART TO IGNORE

**The field of artificial intelligence has seen significant advances over the past few years, in areas such as smart vehicles and smart buildings, medical robots, and communications. These advances are expected to have implications in several policy areas (economic, societal, education, etc.), and governments are increasingly considering them.**

AI is now on the radar of policymakers, and new reports have shed light on the policy issues associated with it. In October, the US National Science and Technology Council released a report on Preparing for the Future of Artificial Intelligence and a National Artificial Intelligence Research and Development Strategic Plan.

In the UK, the parliamentary Committee on Science and Technology published a Report on Robotics and Artificial Intelligence. Earlier this year, the Committee on Legal Affairs in the European Parliament (EP) released a draft report with Recommendations to the Commission on Civil Law Rules on Robotics (expected to be discussed in plenary in January 2017). The following main policy issues are covered in these four documents.

### Economic and social

AI systems have significant potential to lead to economic growth. They can increase the efficiency of production processes, improve the quality of existing products and services, and also generate new ones, leading to the creation of new markets. However, concerns have been raised regarding possible disruptions that AI could bring to the labour market.

There are views that automated systems will make some jobs obsolete, and lead to unemployment. Other consider that AI advancements will generate new jobs, to compensate for those lost, without affecting overall employment rates. All analysed documents call for further monitoring of job trends to better understand the risks and opportunities brought by AI. They also underline the need to adapt education and training systems to new digital skills requirements. Governments are called upon to take action aimed at increasing the size, quality, and diversity of the workforce in AI.

### Safety and security

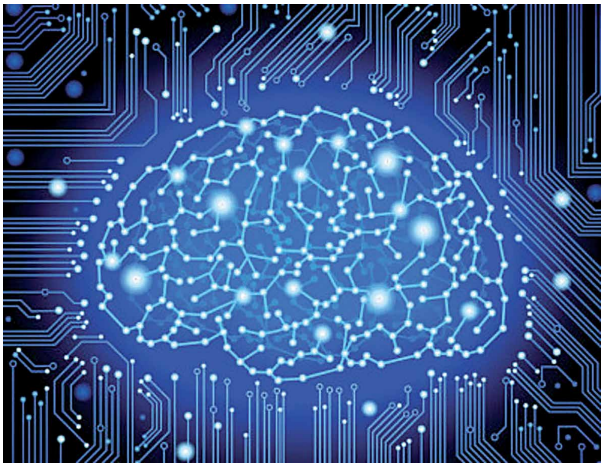
AI applications in the physical world (e.g. in transportation) bring into focus issues related to human safety, and the need to design systems that can properly react to unforeseen situations, and have minimum unintended consequences. AI also has implications for cybersecurity. On the one hand, there are cybersecurity risks specific to AI systems. For example, critical systems that embed AI need to be secured to potential cyber-attacks. On the other hand, AI applications in cybersecurity are expected to play an increasingly important role in both defensive and offensive cyber measures.

### Privacy

AI systems work with enormous amounts of data, and this raises concerns regarding privacy and data protection. The analysed documents emphasise the need for AI applications to ensure data security and protect privacy and confidentiality. The EP draft report further calls for the development of standards for the concepts of privacy by design, privacy by default, informed consent, and encryption in AI systems.

### Ethics

As AI systems involve judgements and decision-making, concerns have been raised regarding ethics, fairness, justice, transparency, and accountability. The risk of discrimination and bias in AI decisions is such a concern. One way of addressing this issue is to combine ethical training for AI practitioners with the development of technical methods for designing AI systems in a way that they can avoid such risks (i.e., fairness, transparency, and accountability by design).



*Credit: Tej3478, CC BY-SA 4.0, via Wikimedia Commons*

### Legal

One overarching question is whether AI-related challenges (especially regarding safety, privacy, and ethics) call for new legal and regulatory frameworks, or whether existing ones can be adapted to address them. US and UK documents take a cautionary approach: it might be too soon for AI sector-wide regulation, and adapting current frameworks is seen as the most suitable approach for the time being.

Additionally, the UK report calls for the creation of a Commission on AI, tasked with identifying principles for the development and application of AI, providing advice to the government, and fostering public dialogue. The EP draft report notes that 'the current legal framework would not be sufficient to cover the damage caused by the new generation of robots.' It therefore calls for an EU directive on civil law rules on robotics, and for a guiding ethical framework for the design, production, and use of robots. It further suggests the creation of a European Agency for robotics and AI, to provide technical, ethical, and regulatory expertise to support the EU and its member states.

### International cooperation

As the US reports note, the policy implications of AI have also attracted the attention of intergovernmental organisations such as the United Nations, G7, and the Organisation for Economic Co-operation and Development (OECD). Governments seem to increasingly believe that AI would benefit from international cooperation in promoting research and development, and identifying suitable responses for related challenges.

In the USA, the government is called to develop a strategy on international engagement related to AI, and to cooperate with other stakeholders in the development of AI standards. The EP draft report calls for international harmonisation of technical standards, mainly to avoid risks of market fragmentation. It also encourages cooperation in setting regulatory standards, under the auspices of the UN.

*An expanded version of this article is available on DiploFoundation's website. The GIP Digital Watch observatory is keeping track of developments in the field of AI. Follow the latest updates on Convergence and Internet of Things.*

# US ELECTIONS AND THE CANDIDATES' STANCE ON DIGITAL POLICY

**Millions of people are following the US Presidential election campaign very closely. The decisions of the next US President will have a bearing on the future of the Internet, among many other areas. The position expressed by the candidates affects the way the electorate will vote. It can also help practitioners foresee developments and changes.**

Both candidates have addressed a large number of digital policy issues in their public speeches, from infrastructure and online taxation, to privacy and cybersecurity.

Hillary Clinton's overarching vision on Internet policy has been expressed in the Initiative on Technology and Innovation. She believes that IG 'should be left to the global community of engineers, companies, civil society groups, and Internet users, and not to governments', therefore expressing commitment to the multistakeholder approach.

Both candidates have paid significantly more attention to cybersecurity, as one of the key challenges that the next president will face. Both have promised to use a strong hand against terrorists, in particular the Islamic State of Iraq and the Levant (ISIS).

When it comes to citizens' rights, Clinton has called for a balanced approach between liberty and security; yet she does not take a clear stance on encryption. Trump has openly said he would restore some of the National Security Agency's (NSA) spying programmes.

The following is a synopsis of the nominees' position on some of the main digital policy areas.

*Read our blog post, and follow our dedicated page on the GIP Digital Watch observatory to keep track of the candidates' position.*

| | Hillary Clinton | Donald Trump |
|---|---|---|
| Telecommunications infrastructure | Supports development of 4G and faster adoption of 5G networks. Wants to establish the Infrastructure Bank that will serve as a competitive grant programme to give cities, regions, and states incentives to undertake actions that foster greater access to high-speed Internet for their residents at affordable prices. | Promises to rebuild the US infrastructure, without clear commitments. |
| Cybersecurity | During the first Presidential debate, Clinton warned that cybersecurity and cyber-warfare are among 'the biggest challenges facing the next president'. As declared in her Initiative on Technology and Innovation, she will support efforts to enhance cybersecurity, invest in cybersecurity technologies, public-private partnerships, information sharing, and the adoption of best practices. | During the first Presidential debate, Trump said that 'we should be better than anybody else, and perhaps we're not... The security aspect of cyber is very, very tough. And maybe it's hardly do-able.' |
| Encryption | Called for a 'Manhattan-like project' to help law enforcement break into encrypted communications. Also said that the USA has to 'balance liberty and security, privacy and safety'. Avoids controversy while supporting security and privacy. Backed Apple's position on encryption. | Called on supporters to boycott Apple unless it agreed to comply with the FBI's order to break encryption. |
| Privacy and data protection | Supports efforts such as the US-EU Privacy Shield to protect data movement across borders. Rejects the false choice between privacy interests and keeping Americans safe. | No general stance on privacy issues, but has committed to specific points, such as to close the loopholes in the federal privacy law to ensure that students' personal information remains private. |
| Economic issues | Opposes the Trans-Pacific Partnership (TPP) trade agreement made with 11 other nations along the Pacific Rim. TPP may have a major impact on e-commerce. It remains to be seen if and how her proposal to enforce trade laws could apply to online trade (e.g. creating a chief trade prosecutor, and tripling the number of trade enforcement officers). | Also opposes the Trans-Pacific Partnership accord. He criticised Amazon for not paying taxes, and believes the tech company is harmful for commerce. |
| Development | According to Clinton's campaign, she wants to 'ensure that technology is a force for broad-based growth, reducing social and economic inequality, and securing American leadership on the global stage.' | In an open letter to Trump, technology sector leaders claim that Trump would be 'a disaster for innovation. His vision stands against the open exchange of ideas, free movement of people, and productive engagement with the outside world that is critical to our economy – and that provide the foundation for innovation and growth'. |
| Content policy | Wants to close off parts of the Internet (mainly social media) to combat ISIS. Clinton says that the only solution is to engage American technology companies in blocking or taking down militant websites, videos, and encrypted communications. | Also wants to close off parts of the Internet (mainly social media) to combat ISIS. Technology companies have expressed concern. In their open letter, they claim that Trump would obstruct the free and open exchange of ideas. |

# THIS MONTH IN INTERNET GOVERNANCE HISTORY

From the first transatlantic cables and the creation of the World Wide Web (WWW), to legislation and court rulings that shaped digital policy, the historical timeline of the Internet and Internet governance is as interesting as it is remarkable. The *GIP Digital Watch* observatory is tracking the developments that shaped IG history. Here, we take a look at the main developments that took place in October.

Visit the observatory and follow us on Twitter and Facebook for more anecdotes.

**29 October 1969**
The first successful message on ARPANET was sent from the University of California, Los Angeles (Boelter Hall 3420), and delivered to Stanford Research Institute. ARPANET was an early packet-switching network and is considered the technical foundation of the Internet.

**October 1971**
The first e-mail was sent by Ray Tomlinson, who also implemented the use of @ for e-mail addresses which he considered was the least-used character on the keyboard.

**31 October 1990**
Tim Berners-Lee finalised three WWW technologies: HyperText Markup Language (HTML), the formatting language for the Web; the Uniform Resource Identifier, commonly known as a URL; and the Hypertext Transfer Protocol (HTTP), which allows for the retrieval of linked resources from across the Web.

**24 October 2003**
The Number Resource Organization (NRO), the coordinating body for the five regional Internet registries (RIRs), was established. The RIRs manage the distribution of Internet number resources, including IP addresses.

**17–19 October 2004**
The term Web 2.0 (using software and applications that allow the user to interact with web pages, and to do things, rather than just observe) took off when the first Web 2.0 conference was hosted in 2004.

**4 October 2006**
The non-profit media organisation Sunshine established WikiLeaks, which went on to publish thousands of classified documents, including details of the US NSA's surveillance operations.

**30 October – 2 November 2006**
The first Internet Governance Forum took place in Athens, Greece. The 8th IGF, in Bali, Indonesia, also took place in October (22–25 October 2013).

**6 October 2015**
The Court of Justice of the European Union declared the Commission's Safe Harbour decision invalid, striking down a long-standing agreement for the transfer of personal data from Europe to USA. It would be later replaced by the EU-US Privacy Shield in 2016.

**27 October 2015**
The European Parliament voted against amendments to what could have been stronger net neutrality rules in Europe. They also voted for the elimination of roaming charges.

**1 October 2016**
The IANA functions contract between ICANN and the US government came to an end, and the stewardship of the IANA functions transitioned to the global Internet community.

**21 October 2016**
The world experienced one of the largest DDoS attacks in history utilising smart devices. *More on page 4.*