

# European Regional Bureau Newsletter



20 October 2018 – 26 October 2018

<https://www.Internetsociety.org/regions/europe/>

[Frédéric Donck \(ERB\)](#)

## Internet Access

### GLOBAL: Digital Commissioner Ansip talks connectivity in India

- The European Commission's Vice President for the Digital Single Market Andrus Ansip flew to New Delhi to deliver a keynote speech on the future outlook of the EU and India on telecoms, digital and ICT.
- He [stressed](#) the EU's common ground on privacy and high data protection standards, while saying India was an important partner in the development of 5G connectivity.
- Vice President Ansip welcomed India's progress in drafting a national data protection law, one that will "hopefully pave the way for greater data flows between the EU and India" he said.

### EU: The EESC warns that future digitalisation projects must be inclusive

- The European Economic and Social Committee (EESC), a consultative institution of the EU, stressed that the "digital dividend" resulting from EU-funded digital projects must be more evenly distributed.
- The report constitutes the official opinion of the EESC on the Digital Europe programme, a programme of digital measures contained within the EU's next long-term budget (2021-2027).
- Authored by Norbert Kluge (Scientific Director at the Hans Böckler Foundation) and Ulrich Samm (Professor of Plasma Physics at Heinrich-Heine University Düsseldorf), the report [supports](#) the Parliament's proposal to increase the budget for digital skills from €700m (7.6% of the total) to €830m (9%), as well as measures promoting R&D, and supporting ethical research into AI.

### EU: Negotiators make progress on .eu legislation

- Member States in the Council of the EU [agreed](#) this week on a joint negotiating position on proposals to revise the governance rules of the .eu top-level domain.

- The first .eu regulation was adopted 16 years ago, but the EC argues that tougher competition in the domain name space calls for an update. The new rules render the governance of the .eu domain more transparent, setting up a multi-stakeholder group to advise the EC on its implementation and extends the rights to register a .eu domain to citizens living outside the EU.
- With almost 4 million registrations, the .eu top-level domain is one of the largest international country code top-level domains (ccTLDs).
- This Council will now negotiate with the European Parliament to reach a final text.

## Trust

### GLOBAL: Online trust is waning, says global report

- A new [report](#) published by the Center for International Governance Innovation (CIGI) and IPSOS find that over half of Internet users around the world are more concerned about their online privacy than a year ago.
- Based on the results of a survey of 26,000 people in 25 countries, the report found that roughly two-thirds (63%) of respondents feel social media companies have too much power. Meanwhile a large majority (81%) cite their fear of cybercriminals as the main reason for their loss of trust online.
- Online privacy concerns vary by region with Middle East/African countries recording the highest percentage of concerned individuals, followed by Latin America, BRICS, North America, and only then, Europe on par with respondents from Asia-Pacific. Taken by country, the most concerned respondents were from Kenya, Tunisia and Egypt, and the least concerned about online privacy were from China, Great Britain and Germany.

### EU: Leaders call for cyber sanctions regime

- EU leaders at the European Council summit last week [agreed](#) to start work on outlining a new cyber sanctions regime to deter hostile countries from malicious cyber activities.
- The EU's External Action Service, the Commission and Council will now start work on sketching out the practical details of a future sanctions regime to respond to and deter cyberattacks.
- Leaders claimed they were resolved "to further enhance the EU's internal security and our ability...to detect, prevent, disrupt and respond to hostile activities of foreign intelligence networks."
- Europe's leaders stopped short of naming Russia as the perpetrator of cyber-attacks against EU Member States. The UK and the Netherlands had pressed for the introduction of strong language on Russia in the Council Conclusions but opposition led by Italy prevented the move.

### EU: Europol and ENISA team up on security in the Internet of Things

- Law enforcement officials from Europol joined cyber experts from ENISA this week to share their outlook on security in the Internet of Things at a joint conference (Oct 24-25) in the Hague.
- The conference [concluded](#) that law enforcement authorities must go beyond defence and incident response but should be able to investigate and prosecute criminals more easily if they are abusing connected devices.
- More work is needed on digital forensics in relation to IoT and although police are already using connected devices like smart cameras, bodycams, and sensors in firearms, the conference participants agreed policing authorities must still upskill on data and privacy protection.
- Building on its work with Interpol, ENISA will prepare additional reports on security in the IoT with a study in late 2018 on Good Practices for Security of IoT in smart manufacturing, and in 2019, a similar report on smart cars.

### EU: Digital giants declare they are ready to restore trust

- At the [International Conference on Data Protection](#) organised this week in Brussels, the CEOs of Apple, Facebook and Google all declared that they were ready for more legislation on privacy.
- The conference entitled “Debating Ethics: Dignity and Respect in Data Driven Life” was opened by Giovanni Buttarelli, the European Data Protection Supervisor, who [said](#) humanity was at a “50-50” moment, a tipping point where half of the world’s population was connected to the Internet.
- In the keynote speeches that followed, Tim Cook, Apple CEO, agreed that privacy was a “fundamental human right” but warned of Internet companies over-reliant on data, saying “our information is being weaponised with military efficiency”, and by video message, Facebook’s Mark Zuckerberg and Google’s Sundar Pichai, each assured an audience of data protection officials that their companies were taking steps to ensure a safe, online environment.

### EU: Data protection officials set out new principles for AI

- Data protection commissioners from across the globe gathered in Brussels this week and adopted a [resolution](#) on AI with six principles laying out how the technology can be developed and governed ethically.
- The “International Declaration on Ethics and Data Protection in AI”, authored jointly by the French, Italian and EU data protection authorities, endorsed AI that is designed according to the “fairness principle”, with accountability, transparency and intelligibility, applying principles of privacy by default and design, protects individual privacy rights, and prevents unlawful biases or discriminations.
- Commenting on the discussions leading up to the adoption of the resolution, Isabelle Falque-Pierrotin, France’s privacy commissioner, said two issues are dividing the opinions of data protection regulators: whether data subjects should always have the right to know whether it is an algorithm or a human-led process handling their data, and secondly, whether data subjects always have a right to human intervention in algorithmic decision-making.

- The International Conference of Data Protection and Privacy Commissioners also served as an opportunity to publish resolutions on [e-learning platforms](#), and efforts to improve [collaboration between DPAs](#).

#### **USA: Trust in large Internet companies varies greatly**

- Amazon and Google are among the most trusted institutions in the United States, while Facebook is among the least, finds a [report](#) from the Baker Center for Leadership and Governance.
- The results highlight the disparity in trust levels among different companies, with respondents answering that they had more confidence in Amazon and Google than in universities, NGOs, courts, state government, the press. At the bottom of the table, among the least trusted institutions in the country, are Facebook, political parties and the US Congress.