

European Regional Bureau Newsletter



14 April 2018 – 20 April 2018

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

Frédéric Donck

Internet Access

EU: POLITICO's Q&A with Roberto Viola

- Politico conducted an interview with European Commission's Director General for Communications Networks, Content and Technology, Roberto Viola, on the EU telecoms reform (the European Electronic Communications Code).
- Director-General Viola stressed the importance of 5G and of the Gigabit Society. He repeated the Commission estimate that €500 billion of investment is needed to realize a fully connected society, with 90% of this coming from private funds.
- In relation to the push from the Parliament to reduce intra-EU calls tariffs, he said that recent evidence from BEREC indicated that it wasn't clear that there was a big problem. He suggested that transparency of prices was a first step that could be taken.
- On net neutrality, Viola said that Europe's rules were ok and there was no need to change the rules. He said the change in the position of the US had not changed the EU's stance on this. He claimed that Europe was "a benchmark in the world" on this issue.

Trust

Global: US and UK accuse Russia of "malicious" cyber-offensive

- In a joint alert on April 16, security officials from the US and UK [blamed](#) the Kremlin for mounting a "malicious" Internet offensive aimed at espionage, stealing intellectual property and laying the basis for an attack on infrastructure.
- In the joint statement, the two parties said the cyber-attack was not targeting solely the UK and the US, but the entire world.
- Moscow has repeatedly denied using cyber weapons.

EU: Council of Ministers on malicious cyber activities

- On April 16, the Council adopted [conclusions](#) on malicious cyber activities, which stress the importance of a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply.
- The Council expressed its serious concern about the increased "ability and willingness of third states and non-state actors to pursue their objectives by undertaking malicious cyber activities".

EU: Facebook users outside the EU will unlikely be protected by the GDPR

- According to a recent article by Reuters, as from May 25, when the General Data Protection Regulation (GDPR) will enter into force, Facebook users outside the EU will not fall under the new rules, reducing the company's exposure to the GDPR.
- Facebook users outside the US and Canada, are currently governed by terms of service agreed with the company's international headquarters in Ireland. As from next month, this will no longer be the case.
- Under the GDPR, companies which are proven to have breached the new provisions could be fined up to 4% of global annual revenue.

EU: Legislators discuss data protection and privacy

- On April 18, the European Parliament in plenary sitting discussed data protection and citizen's privacy as a line of defence against election manipulation, with the Bulgarian Presidency of the Council EU and the European Commission.
- During the debate, the importance of the General Data Protection Regulation (GDPR) was repeatedly emphasised, with the Parliament also urging the Council to allow the negotiations on the e-Privacy Regulation to move forward.
- On the Facebook-Cambridge Analytica scandal, Commissioner Jourová [argued](#) the case shows that “protection of personal data can have a major impact on our democratic societies, on our elections.”
- Monika Panayotova, Deputy Minister for the Bulgarian Presidency Council EU, announced that on May 16, EU leaders are expected to discuss the need for transparent practices and full protection of privacy and personal data on the part of social networks and digital platforms.
- Meanwhile, the European Parliament EPP Group (Christian-Democrats) leader, Manfred Weber, sent a [letter](#) to Mark Zuckerberg, inviting him to appear personally before EU lawmakers.
- In related news, the White House cyber coordinator Rob Joyce has [criticised](#) the GDPR, which he said undercut the WHOIS database, “a key tool for identifying malicious domains on the Internet,” which he claimed would not be compliant with the new law.

EU: EU's e-evidence proposal released

- On April 17, the European Commission unveiled a [proposal](#) on e-evidence consisting of a Regulation on cross-border access to and preservation of electronic data held by service providers, and a Directive requiring service providers to appoint a legal representative within the EU.
- The e-evidence proposal would allow European police and judicial authorities to file requests for electronic evidence directly with tech companies across the EU. The proposed Directive aims at facilitating police's direct access to bank account information in another country.
- DIGITALEUROPE [welcomed](#) the proposal, calling on the co-legislators to deliver a framework that can “serve as a basis for the Commission to negotiate agreements on behalf of the EU and its Members.” The Computer & Communications Industry Association (CCIA) also [reacted](#) to the proposal, welcoming its objectives and encouraging further improvements.
- More critical has been the European Civil Digital Rights (EDRi), which [argued](#) the proposal “turns service providers into judicial authorities,” allowing companies to handle citizens' data, and putting fundamental rights at risk.

EU: Industry signs Cybersecurity Tech Accord

- On April 17, 34 leading tech and security companies, including Microsoft and Facebook, pledged to stand up to governments that launch cyberattacks, signing the [Cybersecurity Tech Accords](#).
- Besides preventing governmental cyberattacks, the firms also agreed to collaborate on stronger defense systems and protect against tampering of their products and services.
- The signatories committed to building new partnerships with industry, civil society and researchers to improve the security and resilience of cyberspace

EU: Article 29 WP releases statement on encryption

- The Article 29 Working Party (WP29) at its April plenary released a statement on [encryption](#) and its impact on the protection of individuals with regard to the processing of their personal data in the EU.
- The WP29 stressed the fact that strong encryption is required to ensure a secure, free flow of data between citizens, businesses and governments. Encryption is considered to be a fundamental tool to guarantee confidentiality and integrity of data.
- Backdoors and master keys are deemed to undermine encryption and damage citizens making their data vulnerable.

EU: Commission Vice-President Ansip addresses RSA Conference 2018

- On April 18, European Commission Vice-President Andrus Ansip delivered a [speech](#) on cybersecurity at the RSA Conference 2018, in San Francisco.
- VP Ansip argued that transatlantic cooperation on cybersecurity will help to maintain secure and open data flows between the two regions, which are “the world's highest.”
- He also stressed the importance of the Privacy Shield and said that the EU is closely following the Federal Trade Commission's investigation into the Cambridge Analytica case.

EU: Security Commissioner Julian King on cyber threats to digital democracies

- On April 18, the European Commissioner for Security, Julian King, addressing the Centre for European Policy Studies, [highlighted](#) the need to build resilience, security and stability in cyberspace.
- He stressed the important role played by the EU Network and Information Security Agency, ENISA, whose mandate will be reinforced and which will also be responsible for establishing and running the envisaged EU-wide cybersecurity certification framework.
- Commissioner King also mentioned the final report of the High-Level Expert Group on Fake News and Disinformation Spread Online, which outlined that online platforms and social media should sign up to a voluntary Code of Principles and good practice to tackle the issue.