

ISOC European Regional Bureau Newsletter

8 October – 14 October 2016

<http://www.Internetsociety.org/what-we-do/where-we-work/europe>

Internet Access

EU: Free Flow of Data initiative and e-Privacy Directive to suffer potential delays

- The **Free Flow of Data initiative communication** – originally scheduled for release on 30 November – is expected to be delayed to January 2017. Legislative proposals are expected to follow-up the communication by summer 2017 and address topics such as liability and data ownership.
- The publication of the **e-Privacy Directive** - also expected 30 November – is similarly expect to be **postponed until after Christmas** according to a Commission spokesperson.

EU: Tele2 AB secures €125 million EIB loan

- **Sweden and the Netherlands will receive a €125 million loan from the European Investment Bank to set up high-speed mobile Internet.** The support will go to Tele2 AB, responsible for deploying the technology in both countries.
- Sweden plans to achieve universal 4G access by 2019; the Netherlands is striving to achieve a similar target for 4G coverage by 2018.

EU: Launch of ECIPE's Digital Trade Estimates

- The **European Centre for International Political Economy (ECIPE) released a database on the regulatory hurdles countries and their businesses encounter to trade data on 12 October.**
- The database - covering 13 policy areas identified in 65 countries, including all EU Member States - covers online transactions, data flow, standards, intellectual property, and investment, amongst others.
- The database reveals Member states have a total of approximately 500 legal restrictions on the movement of data across borders imposed upon companies. Member States with the most restrictions include Germany (44 restrictions), France (38), Denmark (23) and Italy (23).
- The European Commission will ask Member States to justify their restrictions, particularly in fields such as healthcare and taxes.

EU: Parliament discusses European Communications code

- MEPs from the Industry, Research and Energy (ITRE) Committee received a presentation by Claire Bury, Deputy Director-General of DG Connect, on **the European Commission's recent proposal for a directive establishing a European Electronic Communications Code.**
- The European Electronic Communications Code aims to streamline telecoms rules currently spread over multiple legislative pieces to enable a favourable environment for companies to invest in future-proof high-quality network infrastructures. The idea behind the present code would be to ensure connectivity for all.
- MEPs supported the **need to develop an EU Internet infrastructure, especially the roll-out of 5G wireless networks and the introduction free Wi-Fi hotspots in public places across Europe,**

although certain MEPs - Martina Werner MEP (S&D, Germany), Seán Kelly MEP (EPP, Ireland), Dan Nica MEP (S&D, Romania) - questioned whether the initial €120 million allocated to the plan would suffice. Overall, MEPs welcomed the Commission's plans, but stressed the need to prioritise implementation and remain cautious against promising too much.

- Meanwhile, the Internal Market and Consumer Protection's (IMCO) Committee's Digital Single Market Working Group **also met on 12 October to assess the proposals and their impact on European consumers and the internal market.** Discussions – involving academics, MEPs, European Commission, and key stakeholders - centred on the nature of the type of regulatory environment required to deliver innovation while protecting end-users.

EU: Updates on the Satellite and Cable Directive

- **Lidia Geringer de Oedenberg MEP (ALDE, Poland) was confirmed as rapporteur for the Satellite and Cable Directive;** she will also be shadow rapporteur on copyright, and has previously expressed her support for copyright to primarily protect artists. In parallel, **Therese Comodini Cachia (EPP, Malta) was confirmed as the rapporteur for the copyright file.**
- The European Commission had previously published a **study on the functioning of the EU Satellite and Cable Directive** as part of the REFIT process, offering an overview of the EU broadcasting sector, assessing cross-border availability of broadcasters' online services as well as an analysis of national legal frameworks and licensing practices in the sample Member States.
- The study found the directive to be successful in eliminating copyright related barriers for satellites to communicate cross-border to the public - emphasising the success of the Country Of Origin (COO) principle in eliminating copyright-related barriers to cross-border licensing.

EU: Public Consultation on European Interoperability Framework revision

- The European Commission published the **results of the public consultation on E-services.** The results showed most **citizens use digital public services provided by their country's administrations and prefer online services over post, phone calls or physical presence.**
- Nearly 40 per cent of citizens, 70 per cent of academia and 60 per cent of businesses consider **public services should be fully digitalised.**

EU: Potential compromise over cross-border data flows in TiSA

- The European Commission may have struck a deal to allow EU data to be transferred to other countries in the Trade in Service Agreement (TiSA) via **a clause guaranteeing international data flows into a trade agreement with 22 countries outside the EU, including the U.S. and Australia.**
- The compromise would ensure the EU's stricter data protection laws cannot be overturned by the trade agreement.

The Netherlands: Dutch parliament votes to establish tighter net neutrality rules

- **A parliamentary vote held on 11 October will ban platforms from offering free data for selected services and impose stronger net neutrality rules.** The Dutch Net Neutrality law received widespread agreement with 66 members in favor, and 9 against.
- Telecom trade associations, including GSMA and ETNO, expressed their disappointment; mobile carriers such as T-Mobile will be particularly affected as they offer services to stream music on commercial data packages and are free of data limits (zero-rating). Critics of zero-rating consider this practice prioritizes some services over others, threatening the open nature of the Internet.
- European telecoms regulators' organization BEREC published guidance on net neutrality in August and authorized the use of zero-rating - but only for non-commercial purposes. The Dutch Authority for Consumers and Markets announced it would investigate T-Mobile's new music service, "Freedom Music" to ensure it does not unfairly disadvantage competition.

EU: ECJ bans sales of copies of copyrighted software

- The **European Court of Justice ruled that citizens will not be allowed to sell copies of legally purchased software unless granted permission by the copyright owner.** The matter was referred to the European Court of Justice by the Riga Regional Court after two Latvian citizens were accused of selling copyrighted copies of Microsoft programmes online in 2004, in which Microsoft lost sales of €265,514.
- The ECJ ruled that original software sold on a physical medium could be resold if under unlimited user license.

Trust

Global: G7 Cyber Expert Group agrees to support financial cybersecurity

- A **non-binding agreement will set common strategies to strengthen online infrastructure, combat cyberattacks and coordinate a rapid response system to mitigate damages.**
- The framework is not a formal treaty, nor does it impose new regulations on companies. Instead, cybersecurity is treated as a risk management factor, laying out proper governance, risk-assessment and recovery mechanisms for companies.
- The present agreement comes after each member country formed an opinion about the current state of its cyber defences; the results were put together at the **G7 meeting in May** involving financial ministers and central bankers in Japan.
- The framework presents a set of eight principles applicable to both small private firms and large federal agencies. The G-7 cyber working groups meets periodically to review the agreement's progress and deliberate on improvements.

EU: Survey reveals European companies and unprepared and unaware of the cost of a data breach

- The **Continental Europe Cyber Risk Report 2016** published by the insurance broker Marsh & McLennan revealed a **lack of awareness and ownership of cyber risk.** 60 per cent of companies across Europe do not know how much an attack would cost them, and approximately the same amount had not envisaged a plan to cover the impact of a cyberattack.
- The report analyses the attitude of organisations towards the threat posed by cyber risks, mechanisms in place to manage them and the use of cyber insurance as a means of risk transfer. Concerns over cyber threats are increasing as IT departments continue to be the main (68 per cent) responsible in cases of such attack. The study revealed a lack of ownership of the cyber risks by the board and an increase in the procurement of cyber insurance with 47 per cent of respondents already covered by a policy or planning to acquire one in the next year.

UK: New guidelines aimed at Internet trolls

- Under the new **Crown Prosecution Service guidance, incitement to online harassment, derogatory hashtags and the posting of humiliating images could lead to prosecution in England and Wales.**
- Alison Saunders, Director of Public Prosecutions, stated that the Internet is "not an anonymous place where people can post without any consequences". The public policy statements on hate crime will be subject to **public consultation.**

UK: Police website remain insecure

- A **report** published by the Centre for Public Safety revealed **only one in four UK police and affiliated websites complied with the highest standards of online security.**
- Further, up to 25 per cent of British police websites were found to lack any form of automatic secure connection, leaving sensitive data vulnerable to being intercepted.

France: TV5 claims Russia behind huge cyberattack

- In April 2015, TV5's website and social media accounts were victim of a huge cyberattack, whereby the perpetrators used **highly targeted malicious software to destroy the TV network's systems.**
- In the immediate aftermath of the attack, a group called Cyber Caliphate - claimed responsibility for the attack on behalf of Islamic State - but TV5 believes **the attack was carried out by Russian hackers.**
- The attack resulted in a significant financial cost of €5 million in the first year, followed by over €3 million per year for new, extra protection.