ISOC European Regional Bureau Newsletter

24 September – 30 September 2016
http://www.Internetsociety.org/what-we-do/where-we-work/europe

Internet Access

EU: European Commission instructs 19 Member States to cut the cost of broadband Internet

- A number of Member States (Austria; Belgium; Bulgaria; Croatia; Cyprus; the Czech Republic; Estonia; Finland; France; Greece; Hungary; Latvia; Lithuania; Luxembourg; the Netherlands; Portugal; Slovakia; Slovenia and the UK) have been ordered by the Commission to implement **national rules to ensure the reduction of the cost of deploying broadband Internet by 30 per cent.** The request follows a formal notice from March addressed to those who had failed to transpose the measures into national legislation. They will now have two months to introduce the rules or else they could be referred to the European Court of Justice and be made to pay financial sanctions.

EU: European Commission publishes rules on fair use policy

- The revised draft of the rules on 'fair use' have been **published** in the context of limiting roaming charges. The implementing act is due to be adopted by the European Commission on 15 December 2016.

Trust

EU: New Cloud Code of Conduct

- Over 20 European cloud infrastructure companies have agreed to a new voluntary **code of conduct to protect data stored on their servers.** The code prohibits companies managing data centers to profile customers' personal data for marketing, advertising or activities of a similar nature, including the resale of such information to third parties.
- In parallel, the European Commission has also been working on a **code of conduct** to reinforce security standards for cloud software providers. The code was expected to be launched in September but has suffered from a delay.

EU: New rules to prevent dual-use technology exports falling into wrong hands

- The European Commission proposed a **Regulation** on 28 September for the **control of exports of dual-use products.** The text introduces **restrictions on exported products such as anti-virus software or tools for the monitoring of computer networks.**
- Sales were already prohibited in countries like North Korea. The new trade regulation will now introduce limitations to the sale of surveillance software in countries known for human rights abuses.
- The **industry has expressed concer**n over how strict the limitations will be. Companies such as Symantec called for a balanced approach between human rights and technology. DigitalEurope

expressed worry about the chilling effect this proposal may have on European tech manufacturers.

Global: Yahoo hack from a European perspective

- The data breach announced on 22 September affecting over 500 million users raised questions over whether Yahoo complied with European data protection standards. In a **statement** by the British Information Commissioner's Office, Yahoo was asked to provide details on the hack and the impact on UK citizens.
- According to a new **report** from the digital security firm InfoArmor, cyber criminals appear to have been behind the attack. Researchers **consider the group of Eastern European professional criminal hackers, "Group E", were responsible.** This conclusion was reached after analysing part of the compromised accounts, as well as other information concerning the 2014 attack.
- On 22 September, Yahoo published **guidelines** on how to protect online accounts. Under the current Data Protection Directive, there is no obligation to notify data breaches. This will change once the new General Data Protection Regulation is in place as of mid-2018.

EU: Ransomware the leading cyber threat in Europe

- Europol's annual Internet Organised Crime Threat Assessment **reports** a change in the way cybercriminals operated during the past year. **Ransomware**, when a computer is locked down and unlocked in exchange for ransom, **has become the leading cyber threat in Europe.**
- Amongst the targets were CEOs and top politicians, with the key business sectors under threat being e-commerce and the sharing economy. Other trends include the theft of data as a commodity, complex malware attacks on ATM cash machines, the use of encryption tools and the darknet by criminals.
- The report shows different forms of cybercrime such as online sexual exploitation, cyberattacks performed by youngsters, professionals and terrorists. It has lately become increasingly common for hackers to sell cybercrime as a service to criminal groups.

Switzerland: Stricter surveillance laws to monitor Internet traffic

- A new surveillance law expanding the government's monitoring powers for security received the support of 65.5 per cent of Swiss voters. Consequently, the Swiss government will be allowed to use drones and intercept computers in other countries.
- So far Swiss police and intelligence agencies have had limited investigative tools when compared to other countries. Activities such as telephone tapping and email surveillance were previously banned regardless of the circumstances. From now onwards these kinds of surveillance will be allowed only with the prior approval by a federal court and only with regard to the highest-priority cases.

Other

EU: Digital Assembly 2016

- "Putting the Digital Single Market at the heart of Europe" was this year's theme for the **Digital Assembly** held in Bratislava on 29 September. It was an opportunity for stakeholders to exchange ideas on issues such as e-commerce and online platforms, the digitalization of Europe, Internet of Things and ePrivacy, amongst others.

- On Thursday start-ups presented in Bratislava a 60-page long **manifesto** to Commissioner Oettinger focused on encouraging the growth of SMEs in the EU. The document will be passed on to DG Connect and DG Grow for evaluation. “The goal is to go from start-up to scale-up,” Oettinger declared.