ISOC European Regional Bureau Newsletter

26 November – 2 December 2016
http://www.Internetsociety.org/what-we-do/where-we-work/europe

Internet Access

EU: Telecoms priorities of the Maltese presidency of the Council

- A **memo** published by the Maltese outlined priorities for its forthcoming presidency, including **concluding the wholesale mobile roaming review;** progressing the European Commission **plan to expand wireless Internet access;** reach political agreement on **cross-border parcel delivery** and finalise discussions on the use of the **470 MHz to 790 MHz band of spectrum.**

EU: Cloud service providers agree data protection code of conduct

- After months of talks, **Cloud companies agreed on a code of conduct to secure data protection on 30 November** to reinforce consumer trust. The Code includes joint commitments to **better secure IT systems, data centres and cloud infrastructures**.
- The aim is to ensure high standards of data protection and to encourage companies to better protect their cloud-base IT systems from hackers or other forms of data breaches.
- The Code aims also to reassure consumers and help cloud companies prepare for the General Data Protection Regulation (GDPR) due to come into effect on May 2018.
- The European Commission was in charge of coordinating discussions and will announce the Code during the coming weeks. Companies are also expected to sign up to the code over the next weeks; thereafter, German non-profit association **SRIW** will take over the management.

EU: Nine Member States combine efforts to bring the EU into the digital age

- Ministers from a **"Digital Nine"** comprising Belgium, Denmark, Estonia, Finland, Ireland, Luxembourg, the Netherlands, Sweden and the UK met in Brussels to discuss issues related to geo-blocking, free flow of data and business taxes.
- The group announced its **willingness to make conscious efforts on digitization** declaring they would be prepared to start a digital single market among themselves and other interested parties should progress at EU-level be insufficient.

EU: Council agrees on draft regulation banning unjustified geo-blocking

- The European Council **agreed** a **draft regulation** on 28 November t**o ban unjustified geo-blocking between Member States.** The draft will become the Council's common position upon which negotiations with the European Parliament will begin.
- This constitutes the first major Digital Single Market (DSM) proposal agreed by Member States and seeks to remove discrimination based on customers' nationality, place of residency or of establishment. The regulation – which will apply to commercial offers and transactions between Member States but excludes activities such as financial, audio-visual, transport, healthcare and social services – means that traders will not be able to discriminate between customers on prices or general terms and conditions and will be unable to block or limit access to their online interface.

- European Commission Vice-President Andrus Ansip **welcomed** the Council's common position and encouraged negotiations with the Parliament to ensure the agreement is completed under the Maltese Presidency of the EU.
- Germany, Austria and Luxembourg led a minority protest during the ministerial gathering in Brussels, claiming the draft would interfere with antitrust enforcement and is contrary to the current rule allowing courts to settle cross-border disputes.
- Parliament's position on geo-blocking is expected in the spring of 2017.

Trust

EU: 400,000 Deutsche Telekom customers left without Internet access

- **A hack on Deutsche Telekom's hardware** affected Internet access, phone connections and TV reception 20 November onwards.
- 900,000 customers were initially affected but this fell to 400,000 after security measures were taken, including issuing software updates and asking affected customers to disconnect their routers.
- In a **statement,** Deutsche Telekom explained some customers experienced temporary problems and fluctuations in the quality of their Internet access, while others were unable to connect at all.
- Initial investigations found no geographical pattern and an attack on routers by external parties was not excluded.

EU: European Commission cyberattack was politically driven

- According to a European Commission investigator, the cyberattack institution suffered on 24 November **was not state sponsored but was of a political nature.**
- A distributed denial of service attack caused Internet access to be disrupted for hours. It remains unclear who was behind the attack although no data was breached. No more information has so far been made public.

EU: Sensitive information on terrorism left unprotected at Europol

- Europol - the EU's police and cybercrime agency - **left information related to terrorism investigations publically accessible.** The incident occurred as a result of a former Europol employee taking home documents and copying them to a hard drive connected to the Internet but unprotected by a security system or password.
- Europol had known about this case since September and informed Member States and the European Commission; it declared the dossiers were not accessed by anyone apart from journalists from the Dutch radio program **Zembla** but was unable to guarantee this.
- The files – amounting to some 700 pages - contained telephone numbers of people involved in terrorism investigations, dating back over a decade.
- Europol Director Rob Wainwright attended a **special meeting** at the European Parliament on 28 November to discuss the agency's role in information sharing and ensuring security. MEPs debated parliamentary oversight over Europol for two hours. No mention was made to the data vulnerability case. The Liberal group (ALDE) have **asked** Mr Wainwright and Security Commissioner Julian King to provide further details on this omission.
- A **Joint Parliamentary Scrutiny Group** is being set up together with national MPs to scrutinise Europol; it is expected to enter into force on 1 May 2017.

EU: Member State Coalition opposes Commission's plans for cross-border data flows

- **Sixteen countries** - led by Poland, and including Belgium, Denmark, the Netherlands, Slovenia and Sweden - stated their strong **opposition to national laws restricting the transfer of data across borders** when concerning health or tax information.

- The group considers such laws cause unnecessary additional costs for companies and prevent governments from moving their services to cloud storage in other Member States – **costing the EU €8 billion each year.**
- France and Germany meanwhile are supportive of maintaining current data movement restrictions – with Axelle Lemaire French State Secretary for Digital Affairs, stating her position in Brussels in November.
- The European Commission strategy for cross-border data flows was intended to be presented on 11 January but it appears increasingly likely the Commission will issue a communication containing broad suggestions, with possible legislation being tabled later in the year.

EU: Parliament adopts transatlantic deal on exchange of personal data for law enforcement purposes

- **The European Parliament adopted the law enforcement data sharing deal,** known as the **"umbrella agreement",** on 1 December. The agreement introduces protective measures for personal data processed from the EU to the US for investigations or prosecutions.
- The agreement was adopted with 481 votes in favour, 75 against and 88 abstentions and will be implemented by the new US administration. The European Commission assured the Parliament the agreement would only go into effect if the forthcoming Trump administration puts in place the requested safeguards for privacy.
- Final arrangement will be agreed in Washington at a ministerial meeting between EU and US representatives on 5 December.

UK: Over 150,000 people sign UK parliament petition to repeal "Snooper's Charter"

- As of 2 December, more than 150,000 people had signed a **UK parliament petition** to repeal the new UK surveillance laws, the **Investigatory Powers Act.**
- The Act provides UK intelligence and law enforcement agencies with wide-sweeping surveillance powers, allowing for the monitoring and analysis of citizens' communications, regardless of whether they are suspected of any criminal activity. Security services will have the right to hack into computers, networks, servers and mobile devices and surveil data gathered from devices in bulk.

Other

UK: Telecom regular orders BT split

- Telecoms regulator **Ofcom has ordered BT to legally separate from its Openreach division**, which is currently responsible for running the UK's broadband infrastructure. A formal notification to the European Commission is in the process of being prepared ahead of the separation process.
- Ofcom **considers** BT has failed to offer voluntary proposals to address competition concerns on their ability to favour its retail business when making investment decisions in Openreach. Its preference is for Openreach to become an independent company and to have control over its branding and budget allocation.