

ISOC European Regional Bureau Newsletter

20 December 2014 – 9 January 2015

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

Data protection

EU: Germany, France and the UK hold up negotiations on the proposed Regulation, says Albrecht

- **MEP Jan Philipp Albrecht** (Greens, Germany), Rapporteur on the proposed Data Protection Regulation, warned that the differences in opinion between the European Parliament and Member States **could make an agreement on the reform impossible in 2015**.
- The MEP said that **Germany, France and the UK were holding up the negotiations**. While Germany has concerns with regards to how the proposal would impact its powerful regions, the UK remains opposed to the notion of a data protection Regulation, preferring a Directive instead. Moreover, France and Germany voiced concerns that smaller Member States, with less established data protection traditions, could decide on the matter.
- The **MEP supports Microsoft's efforts to avoid disclosing data stored in Ireland to the US** authorities. Jan Philipp Albrecht stated that US authorities should not be allowed to request data from companies headquartered in the EU.

EU: Discussions on possible new data retention rules marked by divisions

- Speaking at a meeting of the **European Parliament's Civil Liberties Committee** on data retention, Dominique Moore, Parliament's legal expert, stated that **EU lawmakers should lead the response to the court ruling** that last year **annulled the EU Data Retention Directive**.
- The ruling of the Court of Justice of the EU prompted governments to review their implementation of the original law. Lawmakers were warned that the national reviews of implementation could lead to the 28-state union winding up with **uncoordinated, diverging approaches**.
- The discussion showed that MEPs remain divided with regards to the necessity for law enforcement agencies having access to retained data.
- **MEP Timothy Kirkhope** (ECR, UK) stated that EU countries should follow the example of the UK, which quickly adopted a new data retention law to address the vacuum left after the EU ruling. **MEP Axel Voss** (EPP, Germany) underlined that new data retention provisions would need to be in line with the EU ruling. **MEP Birgit Sippel** (S&D, Germany) questioned the need for law enforcement access to retained data. She noted that the **collection and evaluation of data represents a burden for ISPs and telecoms companies**. **MEP Jan Philipp Albrecht** backed enshrining data retention into law.
- **Data retention is not listed in the Commission's work program for 2015**. However, a review of the so-called **e-Privacy Directive** that lays down privacy rules for telecom operators is on the Commission's list of upcoming legislative reforms. The Directive contains obligations for retaining electronic-communications data.
- **ETNO**, European Telecommunications Network Operators' Association, has called on the Commission to start a **transparent reflection on the subject of data retention** that would involve all interested parties.
- Generally speaking, the **industry's approach to data retention is twofold**: the need to **ensure that same rules apply throughout the EU** and that the **obligations do not translate into administrative**

and financial burdens.

- Telecommunication companies and **ISPs** **s are likely to push for compensation for compliance with data retention rules**, arguing that cost compensation would provide a safeguard to keep data retention effective and used only when necessary.

Finland: Information Society Code promotes overall confidentiality of electronic communications

- On 1 January, the **Information Society Code** that revises the country's electronic communications legislation passed into law. The Code has four main goals: simplifying existing rules; improving consumer protection; boosting information security; and creating a more equal telecoms market.
- The greatest potential of the Code comes from its **increased regulatory powers over the information society**. One of the new requirements is to ensure **confidentiality of communications rules** apply to all electronic communication distributors, including social media companies.
- The scope of legislation has increased to **cover companies based outside the EU but offering services in the country**. Thus, the Code's approach resembles the one taken by the proposed Data Protection Regulation.

Net neutrality

EU: Presidency will seek an overall compromise on the telecom package

- The Latvian Presidency of the EU announced that it will **seek an overall compromise** on the proposed telecom package that contains provisions on net neutrality.
- While in April 2014 the European Parliament passed the draft of the law which establishes strong net neutrality rules, **discussions at the Council level** seem to be heading in the opposite direction.
- MEP **Marietje Schaake** (ALDE, the Netherlands) voiced her concerns with regards to the Council's compromise suggestions. She also said that if the EU cannot establish a single market for telecoms, the planned establishment of a digital single market is even less likely, considering the complexity of issues.

EU: Study warns EU lawmakers against prematurely regulating net neutrality

- A recently published **report on network neutrality** said that **EU lawmakers are running the risk of premature regulation** as they seek to finalise the EU net neutrality provisions. The fast pace of technological change should be carefully assessed for the EU not to implement an overly rigid regulation, the report warned.
- The study for the Parliament's Committee on Internal Market and Consumer Protection, written by J. Scott Marcus, a consultant at German research institute WIK, concluded that **most fears about violations of net neutrality are overblown**. Instead of regulating, legislators should **favour market-based solutions**.
- Underlining **scarcity of incidents**, the study argued that it is difficult to assess the effectiveness of the current regulatory framework that would justify the necessity to implement a new law.

Open Internet

Turkey: Draft bill would allow website shutdown without court order

- The **Turkish government announced** it is considering a **bill that would grant powers to block a website** without a court order if it is considered as threatening national security and public order. The Prime Minister and Communications Minister will be given the power to make such decision.
- While the website could be shut down immediately, Maritime Affairs and Communications Minister Lütfi Elvan said that a court order would have to be filed within 24 hours. The judge would have 48 hours to decide on the matter; otherwise the prohibition will be automatically lifted.
- The draft also envisages **penalties and fines for not cooperating** amounting to up to \$215,000.

Russia: New data location law and censorship efforts

- **US tech giants** such as Facebook, Google Twitter and Intel have been at odds with the Russian government after a recent **series of legislative measures and censorship orders** aimed to limit Internet freedoms.
- Russia's new law on personal data, signed by President Putin on 31 December 2014, requires that all **data of Russian citizens is stored within Russia's borders**, starting from 1 September. This law followed a series of legal steps, including a mandatory register of all Russian bloggers with a number of followers above a certain threshold.
- On top of the new law on personal data, the government requested that Internet platforms do not promote protests in favour of **Alexei Navalny**, an opposition leader arrested for alleged fraud. Despite early compliance, all US platforms ignored Russian orders to remove events, videos and tweets promoting Russian protests against holding Navalny in prison.
- The Navalny case, along with similar tensions between Twitter and the Turkish government in 2014, underline the growing **difficulty of running a social media business** in an environment in which freedom of speech is limited.

Cybersecurity

Germany: Pro-Russia group says it hacked German government websites

- A website associated with **pro-Russia hackers calling itself CyberBerkut** claimed to be responsible for an **online attack** that occurred on 7 January, **bringing down the main German government websites** for several hours. The hackers demanded that the German government stop financial and political support to the current leadership of Ukraine.
- Moreover, the hacker group has also **made public documents** it said contain private email exchanges between Ukrainian officials, and papers on military cooperation between the US and Ukraine.

Copyright

EU: Commission to propose a review of the copyright framework in 2015

- **Copyright reform will be the first new digital initiative to be proposed in 2015**, Digital Economy Commissioner **Günther Oettinger** **tweeted** before the Christmas break.
- After a meeting with the MEPs of the Parliament's Committee on legal affairs (JURI), the Commissioner clarified that any new **proposal on copyright will not be an extension of existing national rules** but new regulation. However, he reassured his audience that the **Commission's proposal will cover only those areas where national rules no longer work**.
- The Commission has not yet decided whether it will propose a new Directive, leaving some discretion to Member States in transposing it to national rules, or full harmonisation through a Regulation.

General

EU: Latvian Presidency puts emphasis on digital

- The **Latvian Presidency** of the Council of the EU has published its **work programme**, presenting its work priorities for the next six months.
- Underlining the opportunities given by information technologies, the Presidency reiterated that the development of the **Digital Single Market** is among its top priorities.
- While establishing the single market, special attention will be given **to increasing safety and security in the digital environment**. The establishment will be based on an overall **strategy**, and supported by a **strong data protection** framework (the proposed Data Protection Regulation) and **enhanced cybersecurity** (the proposed Network and Information Security Directive).