

ISOC European Regional Bureau Newsletter

9 – 15 January 2016

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

Data protection

EU: Article 29 WP will discuss EU-US data transfer arrangements on 2nd February

- The **Article 29 Working Party** (WP 29), umbrella organisation of the European data protection authorities, will gather in Brussels on 2nd February to discuss the **EU-US data transfers arrangements** following the annulation of the **Safe Harbour agreement**.
- According to a spokesperson of the **French data protection authority** (CNIL), the regulators have been **analysing the legality of other transfer mechanisms**, such as binding corporate rules within multinationals and model clauses businesses use to transfer data across the Atlantic, and aim to reach a **common position** at the upcoming meeting. **Johannes Caspar**, head of the Hamburg data protection authority, added that sanctions will be imposed on companies that transfer data using solely the struck-down agreement.
- The WP 29 urged the EU and US negotiators to agree on a new data transfer framework before the end of January. Earlier this week, the US are said to have submitted proposals on a new deal, including a letter by **Penny Pritzker**, US Secretary of Commerce, which explains commitments on the possible **oversight arrangements** for the new framework. Speaking at the CES tradeshow, **Edith Ramirez**, Chairwoman of the Federal Trade Commission, voiced her optimism stating that an **agreement** on a new transatlantic data transfers framework will be reached before the end of January.

EU: Proposal to reform ePrivacy Directive will be presented by the Commission in 2017

- A **proposal** to reform the **ePrivacy Directive** will be **presented in mid-2017**, the European Commission announced. The review which is part of the Digital Single Market Strategy will be supported by the results of a **public consultation** which will be launched this spring. **Rosa Barcelo**, head of sector for digital privacy at DG CNECT, stated that the **launch should be ready by the end of March**.
- **ETNO**, the European Telecommunications Network Operators' Association, stated that the revision of the ePrivacy Directive should be concluded by the time the implementation of the data protection Regulation is completed. It is expected for the Regulation to enter into force in early 2018.

Security/Cybersecurity

EU: IMCO Committee backs NIS and adds a provision limiting further requirements for digital companies

- With 34-to-2 votes in favour, the European Parliament's **Internal Market Committee** (IMCO) on 14 January approved the proposed **Network and Information Security Directive** (NIS).
- **MEP Vicky Ford** (ECR, UK), Chair of the Committee, announced that **one addition has been made** to the published text. The addition concerns the **article on security requirements and incident notifications** for digital services providers (15a) and is designed to ensure a unified set of rules across the EU. The added paragraph **limits the possibility for Member States to impose further security or**

notification requirements on digital service providers.

France: Amendment on encryption ban struck down

- The **French Parliament** held discussions this week on the **proposed digital bill** to which over 400 amendments were tabled. The so-called **CL92** amendment, which would require equipment manufacturers to incorporate backdoors to their encryption systems, was withdrawn due to the opposition from **Axelle Lemaire**, French Secretary of State in charge of digital.
- **Explaining** her decision, Secretary Lemaire, who has repeatedly voiced her support to encryption, was quoted as saying that the provision is **contrary to the new mission of the French data protection authority (CNIL) which is to promote encryption**.

Global: Activists urge heads of states to respect safety and security online worldwide

- In a **letter** published on 11 January, **AccessNow**, a coalition of activists, organisations and companies, **warned leaders across the world** against the risks of agreeing to laws, mandates or secret agreements wherein encryption or other **secure communication tools are bypassed or undermined**.
- The authors argued that **any exception to provide the strongest available security** of communication tools will be a slippery slope towards more insecurity, more complexity and more criminality online.
- **The call comes in the wake of terrorist attacks** which have led governments in France, the United Kingdom, United States, as well as in India and China, to consider legislation which would allow backdoors to encrypted technologies for enforcement authorities or weaken encryption otherwise.

EU: MEPs denounce lack of information with regards to Council's intelligence and data sharing plans

- At a debate organised by the European Parliament's **Justice and Home Affairs Committee**, several MEPs accused Member States of avoiding the question of **intelligence and data sharing arrangements**.
- Speaking at the debate, **H.P. Schreinemacher**, Director Strategy and Analysis of the Netherlands National Counter Terrorism and Security, who represented the Dutch Presidency of the EU, stated that the Council's stance with regards to passing on stored information can be summarised as **collect, check and connect**. The Presidency hopes to make progress on a common definition and standardisation in using the information systems at the upcoming informal EU Council meeting (25 – 26 January), Schreinemacher added.
- **MEP Judith Sargentini** (Greens, the Netherlands) requested more information about how data sharing would work in practice. **MEP Sophie in't Veld** (ALDE, the Netherlands) added that the Council of the European Union is not consistent and said that there should be more debate about **independent and democratic oversight**.

Net neutrality

Europe: The Council of Europe presents net neutrality guidelines

- In a set of **network neutrality guidelines** issued on 13 January, the **Council of Europe (CoE)**, the intergovernmental regional group of 47 states, said that **Internet traffic should be treated equally**, without discrimination, restriction or interference irrespective of the sender, receiver, content, application, service or device.
- Acknowledging that **Internet traffic management**, which is used by ISPs to deal with peak demand on networks, is justifiable in some cases, the Council warned that it could also result in blocking, discrimination or prioritisation of specific types of content, applications or services. Therefore, the guidelines argued that traffic management should only be allowed to comply with an order from a court or a regulatory authority, when needed to **preserve network integrity and security**, or to prevent or **address network congestion**. Once implemented, traffic management should not be maintained longer than necessary and should be subject to regular review.

- With regards to the so-called **zero-rating**, which is not included in the EU net neutrality rules, the CoE said that preferential treatment should only be allowed if it does not affect the affordability, performance or quality of users' access to the Internet.
- The guidelines also include provisions on **protecting and promoting the right to freedom of expression** and **the right to privacy** related to network neutrality. The CoE underlined that any restrictions on freedom of expression must fit under rules of the European Convention on Human Rights and other rules, arguing that the principle of network neutrality reinforces the exercise of the right to freedom of expression, as Article 10 of the Convention applies **not only to the content of information but also to the means of its dissemination**.
- As for **accountability**, the guidelines said that in their policy frameworks, states should **ensure the accountability of Internet service providers with regard to respect for network neutrality principle**.

General

Global: 60% of the global population remains without access to the Internet

- In the **World Development Report 2016: Digital Dividends**, the **World Bank** argued that the benefits of digitisation of society on growth, jobs and services have mainly benefited the developed countries.
- The World Bank proposed **two actions** to allow technology and the Internet **to boost inclusion and innovation** across the world. The first action strives to make the Internet universal, affordable, open and safe. The second action focuses on stronger regulations to ensure competition amongst business and adapting skills to the needs of the digital economy.
- **Kaushik Basu**, World Bank Chief Economist, explained that despite the current success of digitisation, 60% of the global population, meaning **four billion people, are still without access to the Internet**.