

ISOC European Regional Bureau Newsletter

18-24 January 2014

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

Data protection

EU: DPAs increasingly sceptical about the proposed data protection overhaul

- Speaking at a data protection conference in Brussels, Wojciech Wiewiórowski, **Polish Data Protection officer** stated that the **overhaul of the EU data protection framework is losing the support of national data protection authorities** (DPAs). DPAs which previously supported the proposed Regulation, are rethinking their position as over recent months EU Member States have failed to make progress on the proposal, Wiewiórowski said. With all the topics still undecided, the problem lies in the proposed text and not in the political will of the parties involved, he stated.
- **Paul Nemitz**, Director of the European Commission's justice department, said that he does not perceive any technical problem with the proposal that cannot be overcome. The adoption of the report is more important than its quality, added Nemitz.
- The so-called '**one-stop-shop**' mechanism is said to be among the most controversial provisions of the proposal. The mechanism allows companies operating across the EU to be regulated by one authority, instead of 28 national authorities.
- While the **European Parliament's Civil Liberties Committee**, which is leading the work on the dossier, has already approved its set of amendments, EU Member States are yet to amend the proposal. Once EU Member States make their amendments institutional negotiations would begin.
- Previously, a legal advisor to the European Council said that a system with a lead authority would not be a good system for protecting citizens' fundamental rights.
- Attending the Council meeting, **EU Justice Commissioner Reding** appeared not to expect an agreement before the European elections (22-25 May). The Commission, leading parliamentarians, the Greek Presidency and the future Italian Presidency are said to have agreed upon a **road map** that could allow the reform to be adopted before the end of the year.

EU: Diverging views on how to ensure do-no-track mechanism

- A recent debate in the European Parliament revealed the diverging views on the enforcement and self-regulation of the so-called Do-Not-Track standard (DNT) which allows users to determine whether websites can track their browsing history.
- So far the **World Wide Web Consortium**, which has been working on a global DNT, has failed to define a common approach.
- Considering the privacy issues linked to the tracking of Internet activity, the European Commission is looking into the possibility of embedding a DNT standard in legislation.
- **Robert Madelin, Director General at DG Connect**, voiced his scepticism of legislative enforcement of this principle, underlining that **self-regulation could better respond** to evolving technologies.
- On the other hand, a representative of the European Commission also said that self-regulation would not guarantee the proper functioning of DNT.

Amid snooping revelations, Microsoft proposes to shield foreign users' data

- In reaction to the revelations about **US data snooping**, Microsoft has announced that it is to **allow its foreign customers to have their personal data stored on servers outside the US**.
- The company's general counsel has underlined that users should know whether their data are subjected to certain laws and access of governments in a third country, thus having the ability to make a choice as to where their data resides. For instance, a European client could choose to have the data stored on the company's Irish servers.
- While privacy campaigners have welcomed the move, warnings came from several Internet companies regarding a **possible fragmentation of the Internet** which could turn into regional or national systems.

Net neutrality

EU: IMCO vote reinforces conditions for specialised services

- With 35 votes for and one vote against, the **European Parliament's Internal Market and Consumer Affairs** committee has **adopted its final compromise amendments to the proposed Connected Continent package**.
- Under the adopted amendments, the proposed provisions on the so-called **specialised services** that would allow **ISPs** to strike deals for faster transmission of certain content, **have been made more stringent**, as other specific conditions for conclusions of contracts on those services have been introduced to the proposal.
- The amendments propose **stricter rules for the use traffic management tools**. These would be almost exclusively usable for transient network congestion and specific court orders. The application of traffic management measures shall be subject to **periodic review**, reads the amendment.
- **MEP Christian Engström**, (Group of the Greens/European Free Alliance, Pirate Party, Sweden) has welcomed IMCO's vote stating that it was an important step in protecting a free and open Internet.
- The **Industry, Research and Energy Committee** is set to vote on the amendments on **24 February**.

Cybersecurity

EU: Internet society provider excluded from the scope of the proposed cybersecurity Directive

- The **Internal Market Committee of the European Parliament has adopted a draft report** on the proposed **network and information security Directive (NIS)**. **MEP Andreas Schwab** (EPP, Germany), the Rapporteur on the dossier, has been mandated to start negotiations with the Council. The bill would oblige operators of 'critical infrastructure' to notify national authorities when their networks are seriously compromised.
- The text adopted strips out obligations on social networks, cloud-computing providers and other web services to report hacking attacks and other security incidents. According to the report, **the reporting should only be done on a voluntary basis**.
- The possibility of **imposing sanctions** on companies who lack adequate safeguards against cybersecurity threats has been weakened. Sanctions should only be imposed when a company has intentionally failed or neglected to fulfil its security obligations.
- The **cooperation between the competent authorities** in the field of network and information security is to be strengthened, with EU Member States obliged to assign single points of contact for cross-border cooperation. The Commission's original proposal merely stipulated that the competent authorities in each state should cooperate on cybersecurity safeguards.
- The draft report has strengthened data protection obligations when a cybersecurity incident notification involves personal data.
- The report will be voted in the **plenary session of the European Parliament in March** (10-13 March).

Cybersecurity needs to be brought back to real world

- While remaining a wide concept that lacks a clear definition, cybersecurity needs to be governed by rules that encompass a system of checks and balances, guaranteeing accountability, stated **MEP Marietje Schaake** at a think-tank's recent conference. Schaake has warned that the latest debates on cybersecurity have been marked by increased perception of cybersecurity as a military term, which could ultimately lead to a legal system that lacks democratic oversight. She called for cybersecurity matters to be brought back into day-to-day life.
- Speaking at the same conference, **Robert Madelin** underlined the necessity for the **EU to be cyber-ready**. Following an analysis of threats and Internet usage, the EU should steer digital legislation in order to guarantee that the **same levels of protection apply off and on-line**.

Data protection

Germany: Attack threatens a fifth of the German population

- The **German Federal Office for Security (BSI)** has announced that some 16 million email users in Germany have had their **passwords and other details stolen**.
- According to the office, millions of computers have been affected with a program enrolling the devices on to a network from which data could be stolen.
- The scale of attack equates to almost a fifth of the German population being at risk. A specialised website where people can check if their email accounts have been compromised has been set up by the BSI.