

ISOC EUROPEAN REGIONAL BUREAU - EU issues overview

17 - 23 August 2013

Data protection

EU data protection watchdogs urge Commission to probe Prism

- The **Article 29 Working Party** (WP), composed of EU data protection authorities (DPA), **has sent EU Justice Commissioner Reding a [letter](#)** outlining concerns about the protection of EU citizens' data privacy following the revelations about the **US data surveillance programme**.
- The modalities of data access and location are the main issues at stake and the WP argues that the US laws should not apply to **data that is only in transit**, and is therefore not stored on servers on the US territory, reported MLex.
- In the letter, Jacob Kohnstamm, WP's Chairman, underlines that EU citizens need to benefit from protection guaranteed under European and International law, recalling the **limitations comprised in the so-called Safe Harbour Principles**.
- WP Members will also examine the [existence of similar programmes across the EU](#). **CNIL**, the French DPA, has already set up a **special working group** that examines access to French citizens' data by foreign authorities. The group should present its first report in September.

Cloud computing

EU should resolve regulatory challenges of cloud computing

- A year after the European Commission launched its **cloud computing strategy** ([Unleashing the Potential of Cloud Computing in Europe](#)), the question of whether and **how the EU should regulate cloud computing** has become more urgent in light of the US espionage scandal, some stakeholders argue.
- Several industry representatives have been warning the Commission against the adoption of **EU-centric policies that could hamper development in the sector**. Nevertheless, the Prism scandal has prompted the voice of those calling for a **separate EU cloud environment** that would guarantee protection of EU data.

Cybersecurity

Faulty hardware and software more disruptive than cyber-attacks

- The **European Network and Information Security Agency** (ENISA) has published the 2012 [Annual Incident Report](#) which maps incidents in the electronic communications sector that are reported to ENISA under the provisions of the [Framework Directive on common regulatory framework for electronic communications networks and services](#).
- According to the report, **Internet mobility** was the most affected sector in 2012.
- **Malicious actions accounted for 'only' 8%** of the reported incidents, although these incidents have a significant impact on a large number of users. Some **76% of incidents were caused by hardware or software failures**.

Cybersecurity update

- In **UK**, malicious activities of **hackers have affected one in five British Internet users**, according to a [recent survey](#) by University of Kent's Centre for Cyber Security.
- Some 6% of the users had their accounts (mail, social network or online banking) hacked more than once. The study also underlined that an **increasing number of cyber-attacks lead to substantial financial damage**.

- The Russian Defence Ministry intends to create a [separate branch of military forces](#) aimed at **combating cyber-attacks**. Their creation echo the concerns voiced earlier by the Russian President with regards to the **security of the Russian cyber sphere**. The move is part of the recently announced strategy that calls for **greater international cooperation in cybersecurity**, which could also be linked to the request that **all countries have control over the Internet Assigned Names and Numbers**.

General

ISPs do not deliver advertised connection speeds

- The **Commission is aware of discrepancies** existing between advertised Internet connection speeds and the actual service that is being provided, stated Commissioner **Kroes** in her [answer](#) to **MEP Marc Tarabella's** (Belgium, S&D) [question](#).
- The EU Commission is now considering to include **specific measures for ISPs on transparency** in the upcoming **Telecoms Single Market proposal**, stated Kroes.