

ISOC EUROPEAN REGIONAL BUREAU - EU issues overview
30 March – 5 April 2013

Data protection

Coordinated enforcement action launched against Google

- Following an **investigation into Google's privacy policy** instigated in 2012 by the Article 29 Working Group (the body of EU data protection authorities – DPAs), French DPA [CNIL](#) has confirmed that the [concerns](#) raised over possible breaches have not been addressed.
- Therefore, DPAs from Britain, Germany, France, Italy, Spain, and The Netherlands are to force Google to correct the alleged breaches in the **first coordinated procedure** by EU Member States against a private company on privacy.
- The probe identified the following shortcomings with regards to Google's compliance with EU data protection rules:
 - 'Google provides insufficient information to its users (including passive users), especially on the purposes and the categories of data being processed'
 - 'Combining personal data on such a large scale creates high risks to the privacy of users'
 - 'Google failed to provide retention periods for the personal data it processes'

Update on discussion on EU data protection reform

At a recent event on data protection, EU Justice Commissioner Viviane Reding warned that **pseudonymous data** are to be subjected to the same data protection provisions as any personal data in the proposed Data Protection Regulation. In a [document](#) recently presented by the **Irish Presidency** of the Council, pseudonymous data was underlined as a possible way to decrease perceived administrative burdens on companies.

EU Member States to defend data retention at the EU Court of Justice

- Following a complaint against the Austrian telecoms law on data retention lodged by an Austrian telecommunication company employee, as well as by more than 11,000 individuals, the Constitutional Court of Austria has asked the EU Court of Justice for clarifications on the compatibility of the EU's [data retention provisions](#) with the EU Chart of Fundamental Rights.
- EU Member States have stated they will **defend the Directive** before the Court, as the Austrian referral is said to call the law's validity into question.
- The Data Retention Directive has been criticised for giving the Member States too much power regarding the definition of key provisions, e.g. the period for which the data must be retained.

Cybersecurity

Germany: BITKOM opposes wider reporting obligations regarding cyber attacks

- IT industry association **BITKOM** has sent a [response](#) to the Federal Interior Ministry regarding its [proposal](#) for a **law to increase security of information technology systems**. This would require '**significant IT security incidents**' to be reported to the Federal Office for ICT Security (Bundesamt für Sicherheit in der Informationstechnik).
- BITKOM objects to the lack of clarity in this obligation, which it believes would increase **administrative burdens on large ISPs**, as they are subject to thousands of cyber attacks every day. BITKOM President Dieter Kempf points out in a related [press release](#) that successful attacks do not necessarily cause much damage if they are spotted and tackled early.

Netherlands: Minister sets out role for ISPs in tackling botnets

- In a [letter](#) to the Second Chamber (Tweede Kamer) of the Dutch Parliament, Minister for Security and Justice Ivo Opstelten has given an overview of an **investigation into the Pobelka botnet**, which attacked Dutch and German computers between February and September 2012. The investigation was led by the cybersecurity section of the National Coordinator for Antiterrorism and Security (NCSC).
- The botnet targeted financial transactions made over the Internet, principally by targeting sensitive data inputted via web browsers. The investigation did not find any evidence linking the botnet to a state source.
- Opstelten writes that it will require considerable efforts for the NCSC to inform owners of affected information systems, and this shall be done **in cooperation with ISPs**. He also writes that he will launch a **consultation** with all relevant public and private actors on fighting botnets, including with ISPs.

Open Internet

Russian consumer watchdog demands shutdown of 1,500 websites

- Russian consumer rights agency Rospotrebnadzor has [asked for the blacklisting](#) of over 1,500 websites containing information on suicide, in line with **new provisions on child's protection** against harmful information. More sites could be affected, as the agency confirmed its Internet scrutiny continues.
- Contrary to previous practice, the new law enables state bodies to block Internet resources **without court approval**.
- Earlier, Rospotrebnadzor stated that some Internet companies (e.g. Google, YouTube etc.) refused to cooperate in blocking what is judged as harmful content.
- Several analysts have argued that the law may open the door for far-reaching **Internet censorship** should the blacklist start banning sites for political reasons.

Net neutrality

France: ISP limits access to YouTube

- The service provider Free is at the centre of controversy around net neutrality, as it has been **limiting consumer access** to YouTube, arguing that the service consumes a high amount of its **bandwidth**.
- Xavier Niel, Free's CEO confirmed that the situation will escalate unless **Google starts paying appropriate compensation** to Free.
- A similar conflict between Google and Orange was resolved, thanks to Orange's considerable leverage and international presence. Free, which is much smaller, is counting on its **customers to put additional pressure** on Google.
- Even though, the problem was flagged to the **French Telecoms Regulation Authority** (ARCEP) in September 2012, the authority has not yet reacted.

Net neutrality/Data protection/Internet governance

France: Senate report calls for greater EU involvement in digital sphere

- The French Senate has published a [report](#) on the EU digital sphere, in which it argues that the EU should take a more **proactive stance** to ensure good conditions for the EU Internet industry to prosper, e.g. on **net neutrality** and **data protection**.
- Regarding **cloud computing**, one issue identified is the obligation for **American ISPs** to comply with requests by the US authorities, even though these **could breach EU data protection provisions**.

- The report calls on the EU to clearly define provisions on **the right to be forgotten**, warning against a wide use of the Commission's delegated acts that are part of the proposed Regulation.
- The report also calls for the **creation of European Digital Council** to guarantee a **comprehensive framework** for cybersecurity, data protection and net neutrality.