

ISOC EUROPEAN REGIONAL BUREAU - EU issues overview

15 - 21 June 2013

Data protection

PRISM incites tougher EU stance on data protection

- In a [debate](#) with the EU Justice Commissioner Reding, the members of the European Parliament's **Civil Liberties Committee** urged the EU to implement strong legislation to protect EU citizens' personal data, following the possible scope of the US surveillance of European data.
- **Commissioner Reding confirmed** that during her recent meeting with the US Attorney General Eric Holder, the EU and the US agreed to **set up a transatlantic expert group** to address the PRISM case. The first meeting of the group should be held in July.
- **MEP Veronique Mathieu** (EPP, France) urged **for a swift adoption of [the proposed Data Protection Regulation](#)**.
- **MEP Sophia in't Veld** (ALDE, Netherlands) called on the EU to maintain a strong position against the USA, stressing that the EU should reinforce the data protection proposal with regards to the **data transfer safeguards**. Commissioner Reding supported this point and stated that the **new rules should apply to all companies operating in the EU** regardless of the country of their headquarters.

Parliament's LIBE Committee postpones its vote

- The European Parliament's **Civil Liberties Committee** (LIBE) will not vote on the proposed overhaul of the European data protection framework before October, postponing its vote yet again, stated MEP Jan Philipp Albrecht, Rapporteur on the dossier.
- The delays are said to make it unlikely for the legislation to be approved before the European Parliament's next elections that will take place in May 2014.

France: Google is being given three months to adapt its privacy policy

- On 20 June the **French data protection authority CNIL** [ordered Google to comply](#) with data protection rules within three months. This follows the **investigation into Google's privacy policy compliance** with European data protection legislation launched in February 2012 by the **Article 29 Working Party (WP)**, under the auspices of CNIL, and pursuing the recommendations made to Google in October 2012.
- The formal notice sent to Google found that the company has **not implemented WP's recommendations** and that its practice prevents users from knowing how their data is being used, processed, retained and how they can control it.
- As part of the international administrative cooperation, data protection authorities from Germany, Italy, the Netherlands and the UK are conducting their own investigations. The Spanish authority has already announced that it is opening a sanction procedure against Google.

Open Internet

UK: ISPs to warn users accessing child pornography websites

- In order to deter customers from accessing paedophile sites, **two main British ISPs** (BT and TalkTalk) are to [issue warnings to users who try to access the incriminated websites](#) that have been identified by the Internet Watch Foundation.
- The moves follow recent calls by Prime Minister **David Cameron** for Internet search engines to do more to **eradicate child pornography**.

France: Court orders Twitter to disclose user's information

- A ruling of the County Court of Paris from 24 January ordered **Twitter to disclose the credentials** of the authors of racist and anti-Semitic tweets. The case brought to the court by several associations claimed that the incriminating pseudonymous **Twitter postings broke the French law against racism**. Twitter decided to appeal against the ruling.
- In its recent ruling, the [French court rejected Twitter's appeal](#), stating that the company did not provide an 'easily accessible and visible' way to notify the company of illegal or suspicious tweets, and did not 'justify its refusal to comply with the ruling'. Thus, Twitter is to hand over the requested account details.
- In addition, the complaint has recently started a new legal action against Twitter [seeking €38.5m in compensation](#).

Copyright infringement

France: User sentenced to have its Internet access suspended

- A district court in the Parisian region has sentenced an **Internet user to have his Internet access suspended for two weeks**, in the first case applying the 'three strikes' antipiracy law, the so-called Hadopi.
- However, the user, who was repeatedly warned about illegally downloading copyrighted material, may escape the suspension charge, as the implementation of the ban is said to be impossible. According to ZDNet, the French legislation stipulates that users' **Internet access may not be fully suspended** as the user must remain able to send and receive emails.
- Moreover, the recently published report on copyright online commissioned by the French government - [Rapport Lescure](#) – proposed easing France's three-strike antipiracy policy and ending court's possibility to order the cut of Internet access. The Hadopi law was put in place in 2009.

Russia: Proposed bill could allow out-of-court website closure

- A [draft Russian bill on copyright infringement](#) would allow a copyright holder to **file a lawsuit against the hosting company** owning servers with pirated content or providing links to such. Should the provider not remove the incriminating material within three days, the whole website will be blocked until a court decides on the matter.
- The members of the State Duma have endorsed the proposed bill. The final vote on the measure is expected in the coming days.

Net neutrality

German government confirms plans for net neutrality regulation

- **Philip Rösler**, German Federal Minister of Economy has confirmed that the German government is planning a [regulation that would ensure net neutrality](#).
- This legislation should be **approved before the term of the current Parliament** (September), he added. The hearings on the matter are planned for July.

Cybersecurity

Proposed Cybersecurity strategy criticised by ENISA and EDPS

- The office of the **European Data Protection Supervisor (EDPS)** has published its [opinion](#) on the proposed **EU cybersecurity package** ([Directive](#) for a harmonised security network across the EU and Communication on a [Cybersecurity Strategy of the European Union](#)), underlining that cybersecurity is not to be taken as an excuse for **unlimited processing of personal data**.

- According to the opinion, the **proposal does not offer sufficient guarantees** with regards to data protection, and the Commission's proposal fails to take into account the roles of other proposed regulations ([Data Protection Regulation](#) and [eTrust Regulation](#)) thus limiting effectiveness of the proposed cybersecurity strategy.
- **Jörgen Samuelsson, Chair of ENISA's Management Board**, has criticised the proposed one-size-fits-all approach to cybersecurity. During a public hearing on 18 June in the European Parliament's Internal Market and Consumer protection Committee (IMCO), he stated that an EU-wide approach should be based on **coordination and information exchange** rather than detailed legislation.
- IMCO is the leading committee on the proposed Directive and its draft report is expected by the end of the month, with a possible adoption in committee in November.

ENISA update

- The [Regulation](#) governing the functioning of ENISA, the European Network and Information Security Agency came into effect on 19 June, giving the agency a new mandate for the seven years to come and expanding its duties.
- [ENISA's duty to protect European cyberspace](#) is to be based on the agency's collaboration with **Member States' Computer Emergency Response Teams (CERTs)** and on a **strong collaboration with Europol's European Cybercrime Centre (EC3)**. The agency is also to support cybersecurity exercises (such as Cyber Europe 2012), research, development, and standardisation of EU risk management and electronic products, networks and services.
- On 20 June, ENISA's [Electronic Communications Reference Group \(ECRG\)](#) organised the first teleconference offering the participants (European providers of electronic communications networks and services) the possibility to **collaborate and discuss about the security and resilience issues the ISPs face**. The ECRG is a shared platform enabling ENISA to gather information from the European electronic communications stakeholders and to address the questions of security measures, incident reporting, data protection, botnet mitigation and interconnection security.
- ENISA has also published the results of its mapping exercise that confirmed that the [inventory](#) of **Computer Emergency Response Teams (CERTs)** now includes **209 CERTs across Europe**, which is 12 more than at the end of 2012. CERTs, established by EU Member State governments and other public or private sector bodies, provide responses to emergencies affecting vital computer networks or information systems.