

ISOC EUROPEAN REGIONAL BUREAU - EU issues overview

29 June-5 July 2013

Data protection

European Parliament to conduct PRISM inquiry

- On 4 July, the **European Parliament** adopted a [resolution on US surveillance programme](#), in which it calls for an **in-depth inquiry** to be conducted by the Parliament's [Civil Liberties Committee](#) (LIBE).
- LIBE will present a report on its findings by the end of the year in which it will **assess the impact of the alleged surveillance** activities on EU citizens' rights to privacy and data protection and examine the compatibility of the EU Member States' surveillance programmes with EU law.
- MEPs also called for:
 - Procedures to allow whistleblowers to unveil violations of fundamental rights and ensure their protection
 - The Commission and the Council to consider suspending the current Terrorist Finance Tracking Programme
 - Negotiations on a transatlantic trade deal not to water down EU data protection provisions
- **EU and US security and intelligence experts** will meet today (i.e. on 8 July), parallel to the launch of EU-US free trade negotiations, to [discuss the issue of surveillance](#), as the MEPs rejected an amendment to the resolution calling for the postponement of the trade negotiations.

Parliament Rapporteur calls for common EU-US data protection standards

- The European Parliament's Rapporteur on the proposed [EU data protection Regulation](#), **MEP Jan Albrecht** (Greens, Germany) has called for the **USA and EU to negotiate common data privacy standards**, parallel to the upcoming EU-US trade negotiations.
- Under the current EU provisions, companies operating in Europe are generally **prohibited from transferring data on EU citizens to the USA**, as the US data privacy legislation is not considered adequate. The exception to this rule is the so-called **EU-US safe harbour** framework.
- The **Lithuanian Foreign Minister**, whose country currently holds the Presidency of the Council, has voiced doubts that the discussed draft Regulation could adequately address the question of third countries' access to the EU data.

Germany: Procedure against Google's data processing practice

- The **Hamburg Data Protection Officer** has launched an **administrative procedure against Google** aimed at the company's data processing policies. The move is part of a coordinated EU-wide action led by CNIL, the French DPA, since October 2012.
- According to a [statement](#), Google's policies introduced in March 2012 do not comply with obligations regarding transparency related to the use and handling of data.
- The Officer has given Google the opportunity to respond by the middle of August. He may decide on further steps, including an order for Google to change its practices.

Open Internet

Turkey: Government uses Twitter to arrest protest organisers

- The administration of the **Turkish Prime Minister** has confirmed that the [government is using Twitter](#) and other social media platforms to **identify the organisers of demonstrations** that have turned into a nationwide movement.

- The country's Transportation and Communications Minister recently called for social media companies to cooperate closely with the authorities, underlining that Internet should not be misused as a tool for crime and violence. The authorities have also requested that social media providers open representation offices in Turkey for the government to have a direct interlocutor ensuring respect for Turkish law.
- In a recent press release, **Facebook** denied any possibility of disclosure of users' information to the Turkish government and expressed concerns over the future requests.

Copyright infringement

EU think tank wants balance in online copyright enforcement

- CEPS has published a [report on the Copyright in the EU Digital Single Market](#) in which it calls for the EU to **strike a balance between the copyright enforcement and the guarantee of fundamental rights**.
- The report underlines that **website blocking or removal** triggered by a copyright holder complaint should always apply the principle of proportionality with regards to the gravity of infringements.
- It adds that EU case law has recently demonstrated that the online enforcement measures should **not be unnecessarily complicated and costly for ISPs**.

Cybersecurity

EU: Parliament adopts tougher penalties for cybercrimes

- On 4 July, the [European Parliament](#) gave its approval to **draft Directive on attacks against information systems** that sets criminal penalties for perpetrators of cybercrimes.
- The Directive specifies prison terms for using **botnets** and attacks on critical infrastructure. **Legal persons will become liable** for offences committed for their benefit.
- It also states that **EU Member States** will be required to respond within eight hours to urgent requests caused by cyber-attacks.
- The formal adoption of the Directive by the Council is expected shortly. Once adopted, Member States will have two years to transpose it into national law.

Cybersecurity: update

- The European Network and Information Security Agency (**ENISA**) has launched a study covering the [use of cloud computing technologies](#) in the European public sector. The study aims at identifying common implementation approaches and **provide guidelines for securing cloud computing** infrastructure. The [survey](#) is open until 15 July.
- **The Czech Republic** has [updated its cybersecurity strategy](#) (until 2015). The strategy mainly focuses on an unimpeded access to services, data integrity and confidentiality of the Czech Republic's cyberspace.
- Following the adoption of the National Cybersecurity Strategy, **Hungary** has officially established the [National Cyber Security Coordination Council](#).
- The Centre for European Policy Studies (**CEPS**), a Brussels think tank, has published a [commentary](#) stating that cybersecurity needs a **global public-private partnership**. States should set up Computer Emergencies Teams and **private operators** should agree on **industry-wide codes of conduct** at regional and possibly global level to ensure the flow of information between operators and public authorities, according to the commentary. The document also stresses that there is **no viable alternative to the multistakeholder model** of governance and calls on regulators to ensure **net neutrality principles**.