

ISOC European Regional Bureau Newsletter

6 – 12 February 2016

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

Security/Cybersecurity

EU: ENISA warns against limiting the use of cryptographic tools

- The **European Network and Information Security Agency** (ENISA) has published a **paper** analysing several aspects of **crypto regulation** and their difficulties from a technical perspective. In the paper, ENISA highlighted that a **policy limiting the use of cryptography in products can damage IT industry**.
- In the wake of terrorist attacks, law enforcement authorities and intelligence services submitted requests to create means to circumvent communication protection measures. ENISA warned that limiting the use of cryptographic tools will **create vulnerabilities that can in turn be used by terrorists**, and lower the trust in electronic services.

UK: Committees criticise the proposed Investigatory Powers Bill

- The **Intelligence and Security Committee** (ISC) of the UK Parliament published its **Report on the Draft Investigatory Powers Bill** in which it criticised the proposal for failing to deliver clarity. MP Dominic Grieve, Chairman of the ISC, stated that the draft appears to have suffered from a lack of sufficient time and preparation. According to Grieve, those working on the legislation have not always been clear as to what the provisions are intended to achieve.
- In the report, the ISC **recommended major changes**. With regards to equipment interference (hacking), the report urged the lawmakers to **bring all IT operations under the same legislation**, with the same authorisation process and the same safeguards. The ISC also recommended that Class Bulk Personal Dataset warrants be removed from the legislation, as more targeted actions are available. As for communications data, the report underlined that the approach to the examination should be consistent, with same safeguards being applied to all data irrespective of how it has been acquired.
- Furthermore, the ISC recommended that the **draft needs to be strengthened with provisions on privacy protection** as an overarching approach to data protection is currently missing.
- In its report, **Joint Committee on the Draft Investigatory Powers Bill**, which is composed of peers and Members of Parliament, made **86 recommendations**, arguing that the British Home Secretary Theresa May has **not proved a need to store Internet connection records**.
- The Joint Committee argued in favour of more **explicit protection for encryption and safeguards against backdoors**.

EU: Respondents consider cybersecurity as priority area for ICT Standards Plan

- According to the **preliminary results** of the public consultation on the adoption of a **Priority ICT Standards Plan** the European Commission published on 5 February, respondents singled out **cybersecurity** as one of the top areas requiring common standards in order to achieve a Digital Single Market.
- The preliminary results show that the majority of respondents agreed on the **importance of setting**

priorities for standardisation. The respondents rated the areas of action put forward by the European Commission as follows: cybersecurity (17%); Internet of things (14%); data based services and applications (11%); cloud computing (10%); eHealth (9%); fifth-generation communications (8%); digitalisation of European industry, smart transport systems & smart cities (7%); smart transport systems (6%).

Data protection

EU: Google to start applying the right to be forgotten to all its websites

- According to media **reports**, Google will **expand the application of the right to be forgotten** to all its websites when accessed from an EU Member State. The move is said to address objections raised by EU national data protection watchdogs with regards to the company's implementation of the 2014 right to be forgotten ruling.
- Google had **previously objected to wide application** of the right to be forgotten underlining that it could have a negative impact on the free flow of information.
- A person close to the company said that Google will delist the search results subject to the right to be forgotten from all its websites when a user conducts a search from the country where the removal request was submitted. The search results will be **filtered based on a user's IP address**.
- European data protection authorities have been informed about the upcoming change, media reported.

France: CNIL requests Facebook to comply with data protection rules

- **French data protection authority (CNIL)** announced that according to the results of its audit, Facebook fails to comply with several provisions of the French data protection act. The issues identified include the **collection of data concerning the browsing activity** of Internet users who do not have a Facebook account; collection of data related to, among others, religious and political views without user consent; collection of data on account holders which is used for targeted advertising; and personal data transfers under the Safe Harbour which is invalid. Facebook has been given **three months to comply**.
- **The Belgian, German (Land of Hamburg), Spanish and Dutch data protection authorities** are carrying on with their investigations at the national level and within an international administrative cooperation framework, CNIL announced.

EU: ECOFIN Council rubber-stamps the political agreement on General Data Protection Regulation

- On 12 February, the **Economic and Financial Affairs Council (ECOFIN)** **confirmed** the political agreement reached on the **General Data Protection Regulation** with a view to an early second reading adoption.
- The text of the Regulation will now go forward for an early second reading **adoption by the European Parliament which is likely to take place in March**.

Safety

EU: 25% of EU Internet users experienced security related problems in 2015

- On the occasion of the **Safer Internet Day** (9 February), the latest **figures** released by Eurostat confirmed that there are significant differences among EU Member States with regards to the share of Internet users who experienced security related problems.
- In 2015, fewer than 15% of Internet users experienced security related problems in the Czech Republic (10%), the Netherlands (11%), Slovakia (13%) and Ireland (14%), while 42% of Internet users experienced problems in Croatia, 39% in Hungary, 36% in Portugal and 34% in Malta.
- Catching a virus or other computer infection (e.g. Trojan horse or worm) was the main problem experienced for those Internet users who had security related issues. In the EU, 21% of users caught a

virus or other computer infection resulting in loss of information or time. The share of Internet users having caught a virus was highest in Croatia (41%), followed by Hungary (36%), Portugal (33%), and France (29%), while fewer than 10% of internet users caught a virus or computer infection in the Netherlands (6%), the Czech Republic (8%) and Slovakia (9%). Except for Croatia, the share of Internet users who caught a virus resulting in loss of information or time dropped in all Member States in 2015.

- **Security concerns kept some EU Internet users from doing certain activities.** In 2015, almost 1 in 5 users did not shop online (19%) or did not carry out banking activities (18%), while 13% of users did not use the Internet with a mobile device via wireless connection from places other than home.

Copyright

EU: Culture Commissioner calls for clear definition of copyright application to online content distribution

- In a guest **blogpost** published on the blog of Commission Vice-President Ansip, **EU Commissioner for Culture and Education Tibor Navracsics** presented his priorities for the upcoming overhaul of the EU copyright framework. The Commissioner highlighted that **fair remuneration of copyright holders** should be a top priority.
- In order to ensure fair remuneration, Navracsics suggested for the Commission to **clearly define how copyright applies to online distribution of content**.