

# ISOC European Regional Bureau Newsletter

30 July – 5 August 2016

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

## Privacy Shield

### EU-US: Privacy Shield fully operational as of 1 August

- It is now possible for companies to sign up to the Privacy Shield with the US Department of Commerce who will assume the role of verifying compliance of a company's privacy policies with the data protection standards of the Transatlantic data-sharing agreement.
- EU Justice Commissioner Věra Jourová and US Commerce Secretary Penny Pritzker stated that the new pact is **good for citizens and businesses** on both sides of the Atlantic. It provides Europeans with the reassurance that their personal data will be protected by participating US companies and that companies' commitments to the agreement are enforceable under US law.
- The announcement was coupled with a citizen's guide to provide individuals with transparent information on how the privacy of citizen's data are guaranteed and what remedies are available. The US will work closely with Europe's independent data protection authorities to ensure the efficiency of the present framework.

## Data Protection

### Global: Yahoo investigating claims of "mega-breach" affecting 200 million of its accounts

- Yahoo is investigating claims that the same hacker behind the data breaches at MySpace and LinkedIn could now be behind the Yahoo breach. **Usernames, passwords and dates of birth are being sold** for EUR1,615 to a marketplace on the dark- web.
- Earlier this month, Yahoo was sold to the American telecoms giant Verizon for a total of nearly 4.5 billion euro.

## e-Privacy

### EU: Commission publishes first results of the e-Privacy public consultation

- On 4 August, the Commission made public the preliminary findings of the public consultation concerning the review of the e-Privacy Directive.
- **83 per cent** of individuals and civil society organisations saw a clear **added value in drafting specific privacy rules for the electronic communications sector** to ensure the confidentiality of electronic communications.
- **76 per cent considered the scope of the rules should be broadened** to cover over-the-top service providers (OTI) when they offer communications services such as instant messaging. 76 per cent of these groups also said the e-Privacy Directive has to a limited extent achieves its objectives to ensure

full protection of privacy and confidentiality of communication.

- There was a disagreement over cookies with 77 per cent of citizens and 70 percent of public authorities believing that information service providers should not be allowed to prevent access to their services if users decline to download cookies.
- 38,5 per cent of responses came from citizens and more than a quarter of responses came from Germany, followed by the UK and Belgium.

## Internet access

### Global: Mobile broadband penetration in the OECD area rises to 90.3 per cent

- A report published on 2 August by the Organisation for Economic Co-operation and Development (OECD) revealed more than nine high-speed wireless Internet subscriptions for every 10 people across the OECD area. There has been a 7 per cent increase in mobile broadband penetration since last year.
- The report bases its analysis of broadband markets on five categories: penetration, usage, coverage and geography, prices, services and speeds.

## Telecoms

### EU: Telecom regulators meet to analyse over half a million consultation responses

- Telecoms regulators from across the EU met on 2 August to **assess more than 500,000 responses** to the public consultation on net neutrality.
- The recent publication by the European Telecommunications Network Operators' Association (ETNO) and GSMA reveals strong opposition to some fundamental statements. Indeed some suggested amendments are aiming to delete paragraphs concerning free speech from net neutrality rules. It all comes after a number of associations of journalists expressed their concern that net neutrality violations are a **threat to online freedom of speech and media pluralism**. They consider strong net neutrality rules, including a ban on zero-rating, are necessary to ensure everybody has an equal opportunity to be heard online
- The Body of European Regulators of Electronic Communications (BEREC) will publish **new rules expected for 30 August**.

### Turkey: Internet watchdog Telecommunication Directorate (TIB) will be shut down

- President Recep Tayyip Erdoğan announced on 2 August that the Telecommunication Directorate (TIB) will be closed, asserting that it is heavily infiltrated by Gulen supporters (the group which is widely blamed for the failed coup of 15 July 2016). President Erdoğan's statements were widely picked up by the media. Soon after, Prime Minister Binali Yıldırım said that TIB would not be replaced by another institution.
- The TIB website appears to be shut down at the moment but it's parent organisation, the Information and Communications Technologies Authority (BTK), is still functioning.

## Cybersecurity

### Russia: "Professional" cyber-attack targets a number of government bodies

- The Russian Federal Security Service (FSB) declares a "cyber-spying virus" was found in the network of approximately 20 state organisations, scientific and defence companies, including critical infrastructure.

- The malware enabled to follow what was being typed by monitoring keyboards, take screenshots and switch on cameras and microphones within the targeted computers. They have not yet declared who is believed to be behind this attack.
- The reported attack follows security breaches of the Democratic Party computers in the US, which some media outlets speculated as having originated in Russia.

**Global: Ransomware threat increases to the point of affecting 40 per cent of attacked businesses**

- Security firm Malwarebytes surveyed 500 companies in four countries (Canada, Germany, UK and the US) and found **one-third of victims lost revenue as a result of ransomware**. Almost 40 per cent of all businesses experienced an attack over the past year and ended up paying the ransom.
- The most affected industries are **healthcare and financial services**.

## Hate crime/online radicalisation

**Global: Tech giants join efforts in the fight against online extremism**

- Google's parent company Alphabet, with help from Facebook and Twitter, has partnered with the Institute for Strategic Dialogue, a London-based think tank, to explore the use of online advertising tools to **counter extremist propaganda**.
- Alphabet has funded a series of videos with a range of anti-extremist messages to run on Facebook, Twitter and Alphabet's YouTube. The aim was to understand what sort of messages resonated and could be rolled out more broadly to **prevent radicalization**.
- Organizers worked on how to better target its messages during on Twitter, YouTube and Facebook for users in the U.S., U.K. and Pakistan. The results were published in a study on 1 August.
- Social media marketing tools can be highly effective at identifying key target audiences for organisations working to tackle radicalisation.
- However, social media marketing is very much "a new science". The two **biggest challenges** for NGOs disseminating content using marketing tools are the **frequency** with which advertising tools and platforms change, and apparent **inconsistency and inaccuracy** relating to the figures reported.