ISOC European Regional Bureau Newsletter

13 August – 19 August 2016
http://www.Internetsociety.org/what-we-do/where-we-work/europe

Data Protection

UK: Major data breach reported by accountancy firm Sage

- The **personal information of employees at 280 UK businesses** was reported to have been compromised by a perpetrator using an internal company computer login. The companies involved have been notified and advised to remain on alert. Sage stated it was treating this as a major priority.
- It remains to be seen whether the information has been stolen or simply viewed. If the Information Commissioner's Office (ICO) decides this is a case of negligence, Sage could undergo non-criminal enforcement, audit or even face criminal prosecution.

Antitrust

Russia: Antitrust decision forces Google to change Android distribution

- The Federal Antimonopoly Services (FAS) - the Russian competition authority - announced on 17 August that Google will have to **implement major changes in how it distributes applications via its Android mobile operating system in Russia.**
- FAS accused Google of breaching Russia's competition laws by restricting the ability of smartphone manufacturers to pre-install their apps on Android phones. Google has been ordered to change its terms and conditions and to inform all Android users in Russia that they can remove its apps.
- In a **statement,** the FAS requested Google to execute the changes within the designated period, which Russian **media** reported as being of eight days. Google can consider an appeal to a higher court.

EU Regulatory Framework

EU: New competition rules for telecom operators

- A confidential **document** of 400 pages reveals the European Commission's draft legal analysis on the **review of the regulatory framework for electronic communications**. It appears telecoms companies will face **additional rules on access to Internet networks** under changes to EU law.
- The leaked Impact Assessment indicates the Commission proposes to extend t**elecoms rules to cover online messaging services** - such as Skype and WhatsApp - to ensure they comply with privacy rules comparable to those for texts and calls.
- The European Commission will publish a draft law on data privacy aiming to ensure instant message and Internet-voice-call services face similar rules in terms of security and privacy to those regulating SMS

text messages, mobile calls and landline calls.

- Also under consideration is imposing a target for Internet speeds in all households in Europe to reach 100 megabits per second by 2025.
- The **Body of European Regulators of Electronic Communications (BEREC) will be given increased powers.** BEREC will review member states' approach to selling spectrum used in mobile communications and will monitor communications tools (such as WhatsApp) to ascertain whether are competition issues that need addressing.
- The final legal text is expected before the end of 2016.

Cybersecurity

US: Stolen malware files from group linked to NSA put up for auction

- A group of hackers operating under the name of Shadow Brokers announced its intention **to sell to the highest bidder malware files** it claimed to have obtained from a group linked to the US National Security agency (NSA).
- Security company Kaspersky named the company from whom the malware was reportedly stolen as the Equation Group, which has been linked to US security services.
- Wikileaks **tweeted** they also had access to the data and will make it public in due time.

US: Son of Russian MP faces US trial accused of hacking outlets in Washington

- Roman Seleznev - the son of Russian Liberal Democratic Party MP Valery Seleznev - is accused of a hacking scheme carried out between 2008 and 2014 targeting a number of American pizza restaurants.
- Seleznev – whose lawyers consider the arrest a "kidnapping" or an "illegal rendition" in violation of international law - is alleged to have obtained **€151 million** by hacking outlets in order to steal credit card data.

Australia: US computers remotely hacked by Australian authorities during law enforcement action

- Australian authorities remotely hacked a computer in Michigan to obtain a suspect's IP addresses as part of a child pornography investigation; the information obtained on US citizens was later handed to the FBI.
- It remains unclear whether Australian authorities obtained a warrant; while it is reportedly becoming an increasingly common practice to **pursue targets overseas by employing hacking tools**, the practice has encountered opposition from those claiming this act is **law enforcement hacking**.

Hate crime

UK: New team of specialist police will investigate online hate crimes

- Online hate crime and abuse will be the subject of a **newly-created team of police officers** who will support victims and help identify abuses. This pilot project will extend for a period of two years and cost **€1.9 million.**
- The team will be responsible for identifying the location of such crimes, allocate them to anappropriate force, and assist in the training of police officers and community groups in the identification of abuses.