European Regional Bureau Newsletter

12 January 2019 – 18 January 2019
https://www.Internetsociety.org/regions/europe/
Frédéric Donck (ERB)

Internet Access

Sweden: Rural municipality receives award for broadband best-practice

- The European Commission highlighted this week a partnership between telecoms operator Telia and Sunne, a rural municipality in west Sweden, as an "excellent example of investment into future proof infrastructure".
- The project replaced old copper networks with fibre and mobile networks, giving the municipality modern communication infrastructure with download speeds of up to 1 Gbps.
- Using different types of pre-existing infrastructures, including privately owned ducts, and, where applicable, water and sewer works were used for co-trenching. Fibre Internet services were brought to customers through an open portal with several service providers, allowing them to choose the most suitable plan.
- Alongside the digital infrastructure, the municipality launched with Telia an educational initiative "More Digital", to improve digital literacy among senior citizens.

Trust

EU: Brexit vote - uncertainty increases for data flows

- On Tuesday, British Members of Parliament massively rejected Prime Minister Theresa May's withdrawal deal on Brexit, throwing the talks about the country's anticipated exit from the EU into further confusion.
- Unless the UK government manages to now secure an extension from the other EU-27 countries, something France and Germany signalled was a possibility, the country will exit the bloc on the 29 March without a framework providing certainty for its businesses and citizens.
- The blanket legal basis governing the transfer of personal data out of the EU into the UK would also cease, and companies could be exposed to significant fines unless they put together the appropriate safeguards.

- GDPR standards would however survive. As a UK government paper from September 2018 stated, "the Data Protection Act 2018 would remain in place" even without an agreement for exiting the EU.
- But uncertainty remains "especially regarding smooth and secure data flows" said Thomas Boué, director general for Europe of the BSA Software Alliance, and industry group representing leading software companies, "in the absence of a transition period…entities operating across the Channel will face significant challenges to have legal alternative transfer mechanisms to transfer personal information in and out of the U.K. in place from day one".

EU: Election security, Facebook cracks down on Russian fake accounts

- Facebook announced on Thursday that it has taken down a network of pages covertly run by Russian state media organisation Sputnik.
- The Russian media organisation had coordinated a total of 289 pages and 75 accounts on the platform, followed by around 790,000 Facebook users.
- For Alex Stamos, Facebook's former chief security officer, this is important as it's the "first evidence [we've] seen that Russian overt propaganda organisations are also participating in covert amplification".

EU: "Beware of tech companies playing government" says Dutch MEP

- In an article published by Bloomberg, the Dutch MEP Marietje Schaake warns of the risks of large technology companies setting self-imposed cybersecurity standards.
- Governments and courts have been offloading their responsibilities to tech companies, with recent rulings at the European Court of Justice on the removal of websites from search results to respect "the right to be forgotten" being one example, and the NetzDG law in Germany being another, forcing companies to take hate speech, fake news and illegal content offline within 24 hours.
- By leaving the policing to the companies rather than to regulators and governments, MEP Schaake argues, "there's a great risk that the public interest will be captured by the private sector, and that norms will be made without transparency, accountability or the mandate of the people."
- The Dutch MEP says private initiatives, like codes of conduct, should be encouraged, but remain temporary constructs until governments are able to build powerful, enforceable rules.

EU: ITRE Committee votes to approve Parliament's AI & robots report

- On Monday, the Industry (ITRE) Committee in the European Parliament voted to approve MEP Ashley Fox's (ECR, UK) own-initiative report on a "comprehensive European industrial policy on artificial intelligence and robotics" by 49 votes to 1 and 4 abstentions.

- The report, which is non-binding, sends a political message to the European Commission about the Parliament's desired approach to AI and robots for the next legislature.
- The report urges Member States to develop new training programmes that focus on developing the skills of workers, especially in the industries most affected by automation so that they can seize job opportunities within the new jobs created by AI. The report is now expected to be voted on in plenary in February.

EU: ENISA releases new report on IoT security

- The EU's cybersecurity agency ENISA, released a report this week entitled "forest for the trees: an IoT security standards gap analysis" mapping the existing standards against requirements on security and privacy in the area of the Internet of Things (IoT).
- The report finds that there is no significant standards gap, every requirement can be met by an existing standard. The gap that exists in IoT device security is more the lack of a holistic treatment that accounts for the device's relationship to different ambient environments.
- In conclusion, manufacturers must combine a mix of security certification, assurance testing and validation, as well as market surveillance to guarantee the security of their product.

EU: "Europe's most hackable election", Commission raises concern over EU election

- This week, the EU's security commissioner Julian King told reporters at Politico about his concerns for the EU election on 23-26 May 2019. According to him, "given the dispersed nature and comparatively long duration of the EU elections" they present a tempting target to malicious actors. Steps therefore need to be taken to protect electronic voting infrastructure and tackle information.
- He further confirmed that there is evidence of hostile state interference in recent elections, without naming and shaming. To counter these malicious attempts, Commissioner King stated that "there will be much greater awareness and vigilance" pointing to work with electoral councils, cybersecurity authorities and platforms.

EU: First report of Europol's observatory function on encryption

- As part of the measures outlined by the European Commission in the 11th progress reports towards a Security Union, Europol and Eurojust established a joint observatory function with respect to encryption. Their first report is now publicly available.
- The report provides an overview of the current state of the encryption debate and the challenges and opportunities for law enforcement.
- It also provides a preview of what developments are likely to come, including quantum computing, artificial intelligence, 5G and steganography, the practice of hiding secret content and messages in otherwise non-secret mediums, for example, malware hidden in ordinary image files to control servers.

Germany: National cyber defence centre receives boost

- In the wake of a data leak that exposed the details of over 1,000 German politicians, government officials are revamping the country's "Cyber Defence Centre".
- The Centre was founded in Bonn in 2011 to help coordinate efforts by all German federal agencies in charge of cybersecurity, but with limited success say officials privately, reports Politico.
- As part of its changes, Berlin's Interior Ministry wants to establish a joint database listing cyber threats made available to agencies in Germany's 16 federal states, along with a 24/7 task force that can be deployed in case of a large-scale cyberattack.

Germany: Huawei ban under consideration

- The German government are examining whether it needs to restrict the use of Huawei equipment in its roll-out of 5G, said its Deputy Interior Minister.
- In a letter (in German) replying to an information request by a German MP, Günter Krings said: "The security of products offered by different telecommunication manufacturers and … the security of a future 5G network are of high relevance for the German government. This [consideration] will determine the direction of the German government when it comes to building up its future 5G network."