IEEE

GLOBAL INTERNET POLICY MONITOR

Read summaries of significant recent internet technology policy activities around the world

2 August 2017

Synopsis

Scroll to read full summaries with links to news articles.

ENISA has this week called upon the **EU** to expand its remit as it aims to take a leading role in the bloc's emerging **cybersecurity** programme.

The **European Court of Justice** has ruled that the data sharing agreement between the **EU** and **Canada** violates the EU's **data privacy protections**, in a ruling similar to that which derailed the **US-EU Safe Harbour** in 2015.

In the **US** a bipartisan alliance of Senators has launched new legislation to increase security standards for **IoT** devices.

A report from the **Government Accountability Office** has found security flaws in the **cybersecurity** guidance issued by the **Department of Defense**, with specific mention made to the Pentagon's advice on **IoT** security.

The House of Representatives **Energy and Commerce Committee** has called for evidence from leading technology companies, **Alphabet Inc**, **Facebook**, **Comcast**, **Amazon** and others as it considers future changes to **net neutrality** in the **USA**.

Following a crackdown on **VPNs** by the **Chinese Government**, **Apple** has removed its VPN apps from the Chinese version of its App store.

A new report by the **Internet Society** has found that **Cybersecurity** has become the number one concern for internet users in the **Asia-Pacific** region.

Veritas Technologies has reported that companies in **Europe** and **Asia** are over emphasising their compliance with **GDPR** ahead of its introduction, finding that only 2% of the 900 respondents it surveyed were fully compliant.

Dr Tobias Feakin the Australian Ambassador for **Cyber Affairs** has told the RSA Conference in Singapore that more should be done to fight against both domestic and international **controls of the internet**, calling instead for the international community to develop a free, open and secure internet.

Russia has banned the use of **Virtual Private Networks** as the Government seeks to block access to unlawful content on the internet.

Communications Ministers from each of the **BRICS** countries have met in Hangzhou, **China** to discuss further cooperation in **digital transformation** and **cybersecurity**. The roundtable event was also attended by leading communications and technology companies from each of the five countries.

ITU has published its 2017 report detailing its analysis of the facts and figures of global information and communication technology use. The report identifies the increase in **internet access**, with notable increases in the number of young people accessing the internet.

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

2 August 2017

Table of Contents

Europe

Internet governance

31.07.17

Euractiv

New EU digital Commissioner adds cabinet members

The EU's new Commissioner for digital issues Mariya Gabriel has begun to assemble her cabinet team, with several noteworthy appointments, including Carl-Christian Buhr, currently a director at CERT-EU, as deputy head of cabinet.

"Less than one month after taking office, the newest EU Commissioner, Mariya Gabriel, has filled several spots in her cabinet.

Gabriel's head of cabinet is Lora Borissova, a Bulgarian official who previously worked at the EU External Action Service. Gabriel, who was an MEP until she was confirmed earlier this month as the newest Commissioner, was head of the Bulgarian delegation in the European Parliament's centre-right European People's Party."

Cybersecurity

28.07.17

EU cybersecurity exercise focuses on 'quasi-democratic' country and anti-globalisation group

The EU Council has announced that a range of cybersecurity exercises will be launched in September and October for EU and NATO member countries to test their cyber skills.

"An EU exercise to test countries' ability to react to cybersecurity attacks will focus on threats from terrorist organisation, "a quasi-democratic country" and anti-globalisation groups.

The series of made up attacks will be simulated as part of a competition this September and October. A spokeswoman for the Council of the EU, one of the institutions organising the events, said all EU member states will take part in at least part of the exercise. It will run from 1 September until 11 October. NATO member countries can also compete."

01.08.17

Euractiv

EU agency asks Commission to 'avoid fragmentation' in new cybersecurity plans

ENISA has called on the EU to work harder to combine both civil and military responses to cyberattacks in a 20 page document calling for a new cohesive approach to cybersecurity.

"The EU needs to step up its cooperation between civil and military cybersecurity authorities when member states are attacked by hackers, according to the EU cybersecurity agency ENISA.

The Athens-based agency asked the European Commission for a bigger role in responding to cybersecurity breaches. Part of that role would mean working more with the military when hackers attack more than one EU country. Those cybersecurity breaches can potentially become an EU competency, according to a document that the agency sent the EU executive, which EURACTIV has obtained."

02.08.17

Government Computing

ENISA bids to lead EU cybersecurity programme

ENISA has this week called upon the EU to expand its remit as it aims to take a leading role in the bloc's emerging cybersecurity programme.

"The European Union Agency for Network and Information Security (ENISA) wants to become the EU's centre of expertise for cyber security.

The agency currently helps the EU and its member states be better equipped and prepared to prevent, detect and respond to information security breaches. Now, as the EU attempts to beef up its cyber security response to attacks, ENISA wants to be the Union's go-to cyber player."

02.08.17

Security Brief Europe

UK SMBs estimate average cost of cyberattack more than £730,000

A report by Webroot focused on small-to-medium sized businesses (SMBs) in the UK, USA and Australia has found that on average UK SMBs lose more than £730,000 as a result of cyberattacks.

"A new report has revealed many small-to-medium sized businesses (SMBs) in the UK are operating under a false sense of security.

The evolving cybersecurity landscape of 2017 thus far has presented SMBs with a host of new threats to their clients, data and bottom line."

Privacy

26.07.17

Euractiv

EU court's blow to Canada deal marks new hurdle for data laws

The European Court of Justice has ruled that the data sharing agreement between the EU and Canada violates the EU's data privacy protections, in a ruling similar to that which derailed the US-EU Safe Harbour in 2015.

"An EU data sharing agreement with Canada is illegal because it violates privacy rights, the European Court of Justice said Wednesday (26 July), marking a new legal blow to the bloc's data deals.

The top EU court's opinion on a draft passenger name record deal with Canada is the latest setback for the European Commission's data rules—after it knocked down data retention laws and in 2015, the safe harbour agreement allowing companies to transfer personal data to the United States."

31.07.17

SC Media

Human rights organisations declare EU-US privacy shield invalid

Amnesty International and Human Rights Watch have called on the EU to abandon the EU-US privacy shield, arguing that US surveillance undermines any attempts to protect citizen's privacy in data exchanges.

“Two leading human rights organisations have called for an end to EU - US Privacy Shield, saying that US surveillance practices render it invalid. Amnesty International and Human Rights Watch addressed the European Commission in a letter on 26 July.

According to the groups, “the United States of America (United States) does not ensure a level of fundamental rights protection regarding the processing of personal data that is essentially equivalent to that guaranteed within the European Union (EU)”. In short, that the safety of European data cannot be ensured.”

01.08.17

SC Media

Rudd reaps tech industry backlash for proposal to undermine encryption

The UK’s Home Secretary Amber Rudd has received significant criticism ahead of her visit to Silicon Valley for her position on encryption backdoors that would allow law enforcement access to encrypted messaging services.

“UK home secretary Amber Rudd faced a barrage of criticism after she warned social media and companies - ahead of attending the inaugural Global Internet Forum to Counter Terrorism in San Francisco - that the Government may introduce laws to clamp down on extremist content if companies do not take action themselves.

She drew particular criticism from civil rights groups and the tech industry for her comment, reported in the Telegraph, that "real people" don't need end to end encryption and that messaging apps like WhatsApp should ditch it and do more to help the authorities deal with security threats. This ‘help' is understood to mean backdoors for the authorities – as well as not allowing suspected terrorists access to their services.”

02.08.17

Computing

Most GDPR-compliant organisations are actually not

Veritas Technologies has reported that companies in Europe and Asia are over emphasising their compliance with GDPR ahead of its introduction, finding that only 2% of the 900 respondents it surveyed were fully compliant.

“Many of the companies that claim to be ready for the GDPR do not actually comply with its regulations, a study by Veritas Technologies has found.

31 per cent of the 900 respondents across Europe and Asia told Veritas that their organisation already matches the "key requirements" of the GDPR; however, when questioned further they were found to lack understanding and are unlikely to actually comply. Only two per cent appear fully ready for the incoming legislation."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

01.08.17

The Hill

Senators offer bill to boost security of internet-connected devices

A bipartisan alliance of Senators has launched new legislation to increase security standards for IoT devices.

“A bipartisan group of senators unveiled legislation Tuesday to bring more security to internet-connected devices, often referred to as the "internet of things."

Sens. Mark Warner (D-Va.), Steve Daines (R-Mont.), Cory Gardner (R-Colo.) and Ron Wyden (D-Ore.) introduced the "Internet of Things Cybersecurity Improvement Act of 2017.”

Cybersecurity

27.07.17

The Hill

IRS fails to resolve dozens of information security deficiencies, GAO says

The GAO has criticised the IRS for failing to resolve a number of data security issues that places sensitive financial data at risk of cyberattacks.

“The IRS's ability to protect sensitive financial and taxpayer data is limited by its failure to resolve numerous information security deficiencies identified by the Government Accountability Office (GAO).

The continuing “control deficiencies” are identified in a new GAO auditreleased Wednesday that sheds light on the slow progress the IRS has made on information security despite, its reliance on computer systems to support its operations and store sensitive data.”

28.07.17

The Hill

[House panel asks agencies for docs from Russian cyber firm]

The House Science, Space and Technology Committee has requested reports from a range of US federal agencies relating to Kaspersky Lab after it has fallen under increased scrutiny for alleged ties to Russian Intelligence.

"A House panel has asked nearly two dozen government agencies for documents on Russian-origin cybersecurity firm Kaspersky Lab.

The House Science, Space and Technology Committee made the request to 22 different government agencies in letters that were released by the committee on Friday."

01.08.17

CNBC

Gaps found in Pentagon guidance on Internet of Things devices, overall cybersecurity

A report from the Government Accountability Office has found security flaws in the cybersecurity guidance issued by the Department of Defense, with specific mention made to the Pentagon's advice on IoT security.

"A government agency has found there are gaps in the Department of Defense's policies on new Internet-capable devices such as smart TVs and also suggests cybersecurity efforts "can be strengthened."

"Unless DoD improves the monitoring of its key cyber strategies, it is unknown when DoD will achieve cybersecurity compliance," the Government Accountability Office said in a report released Tuesday."

01.08.17

SC Media

Prankster tricks Whitehouse cybersecurity advisor into thinking they're Jared Kushner

Homeland Security Adviser Tom Bossert has been tricked by a phishing attack into disclosing his personal email address to a person impersonating White House Advisor and son-in-law to President Trump, Jared Kushner.

“A U.K.-based hacker managed to phish and spoof the accounts of a number of White House officials tricking other officials into believing they were conversing with colleagues.

In one incident, the self-described “email prankster” managed to fool Homeland Security Adviser Tom Bossert, who advises on cybersecurity, into believing he/she was President Donald Trump's son-in-law Jared Kushner and convince him into disclosing his personal email address.”

Privacy

01.08.17

The Hill

Senate bill would ease law enforcement access to overseas data

A new bill titled “The International Communications Privacy Act” has been introduced in the Senate to provide law enforcement with greater powers to access US data held in foreign servers.

“Senators introduced bipartisan legislation Tuesday that would create a legal framework allowing law enforcement to access Americans' electronic communications in servers located in other countries.

The International Communications Privacy Act from Sens. Orrin Hatch (R-Utah) and Chris Coons (D-Del.) would also require law enforcement to notify other countries of such data collection on their citizens in accordance with their laws.”

Internet Inclusion

31.07.17

Reuters

Republicans want tech input on U.S. net neutrality legislation

The House of Representatives Energy and Commerce Committee has called for evidence from leading technology companies, Alphabet Inc, Facebook, Comcast, Amazon and others as it considers future changes to net neutrality in the USA.

“A U.S. congressional committee on Monday asked for input from Google parent Alphabet Inc (GOOGL.O), Facebook Inc (FB.O), Comcast Corp (CMCSA.O), Amazon.com Inc (AMZN.O) and other major companies on a proposed rewrite of

rules governing consumer internet access, according to an email reviewed by Reuters.

Last week, the House of Representatives Energy and Commerce Committee's chairman asked the chief executives of those three companies, as well as AT&T Inc (T.N), Verizon Communications Inc (VZ.N), Netflix Inc (NFLX.O) and Charter Communications Inc (CHTR.O) to testify at a Sept. 7 hearing on the future of net neutrality rules. None of the companies have agreed yet to testify."

02.08.17

The Hill

Senate panel advances bill to boost federal cyber scholarships

The Senate Commerce, Science and Transportation Committee has given its support to a bill that would increase federal funding for cybersecurity scholarships provided by the National Science Foundation.

"A Senate committee on Wednesday advanced legislation that would update and expand an existing federal cybersecurity scholarship program for students pursuing degrees in cyber fields.

The bipartisan bill, sponsored by Sens. Roger Wicker (R-Miss.) and Tim Kaine (D-Va.), would expand a cyber scholarship-for-service program run by the National Science Foundation in an effort to bolster the nation's cybersecurity workforce."

Pan-Asia

Internet governance

31.08.17

SC Media

Apple pulls VPN apps from China App Store

Following a crackdown on VPNs by the Chinese Government, Apple has removed its VPN apps from the Chinese version of its App store.

“China's crackdown on virtual private networks (VPNs) has pushed Apple to remove some VPN apps from the China App Store.

The ExpressVPN iOS app was nixed from the store, the company said in a Sunday blog post.”

Cybersecurity

31.07.17

Times of India

India vulnerable to cyber crime, must upgrade defence: Study

A new study from IIT Kanput has found that India needs to increase its cybersecurity defences in order to protect its increasingly digital economy.

“Demonetisation and the subsequent push for digitisation has escalated risks relating to cyber crime and India needs to urgently upgrade its defences by setting up a cyber security commission on the lines of the Atomic Energy and Space Commissions, according to an IIT Kanpur study shared with Parliament's committee on finance.

Noting that the government has initiated a number of programmes to enhance the participation of citizens in the fully digitalised economy, the study said cyber security centres set up by the Reserve Bank of India would be insufficient. "While RBI centres often come to IITs such as IIT-K for expert opinion, IITs do not engage in relevant research on cyber security," the study said.”

02.08.17

MIS Asia

Cybersecurity is the No.1 concern for Asia’s internet users

A new report by the Internet Society has found that Cybersecurity has become the number one concern for internet users in the Asia-Pacific region.

“Cybersecurity is the No. 1 concern for internet users in the region, according to the annual Survey on Internet Policy Issues in Asia-Pacific by the Internet Society.

Sixty percent of the 2,000 people polled said they are aware of internet-related policies, regulation or laws enacted by their national government in the past year. These efforts mainly sought to address cybersecurity, cybercrime, access, privacy and data protection.”

Privacy

02.08.17

Computing

Most GDPR-compliant organisations are actually not

Veritas Technologies has reported that companies in Europe and Asia are over emphasising their compliance with GDPR ahead of its introduction, finding that only 2% of the 900 respondents it surveyed were fully compliant.

“Many of the companies that claim to be ready for the GDPR do not actually comply with its regulations, a study by Veritas Technologies has found.

31 per cent of the 900 respondents across Europe and Asia told Veritas that their organisation already matches the "key requirements" of the GDPR; however, when questioned further they were found to lack understanding and are unlikely to actually comply. Only two per cent appear fully ready for the incoming legislation.”

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

27.07.17

Info Security

Australia Calls to Fight Back Against Attempts to Control Internet

Dr Tobias Feakin the Australian Ambassador for Cyber Affairs has told the RSA Conference in Singapore that more should be done to fight against both domestic and international controls of the internet, calling instead for the international community to develop a free, open and secure internet.

“The Australian Ambassador for Cyber Affairs insists that in order to reap the enormous economic growth opportunity that cyberspace offers, the internet must remain free, open and uncensored

In his keynote at RSA Conference 2017 Asia Pacific and Japan in Singapore on July 27 2017, Dr Tobias Feakin, the Australian Ambassador for Cyber Affairs, shared his concern about some nations’ desire to control and restrict the flow of data.”

31.07.17

SC Media

Putin signs law prohibiting VPNs, anonymizers

Russia has banned the use of Virtual Private Networks as the Government seeks to block access to unlawful content on the internet.

“A Russian official said the law is meant to block access to content deemed unlawful." Following the lead of China, Russian President Vladimir Putin signed a law banning the use of virtual private networks in an attempt to thwart access to websites prohibited by the government.

The law, which already has been approved by the country's lower house of parliament, the Duma, also puts the kibosh on the use of anonymizers, according to a report by Reuters.”

Cybersecurity

28.07.17

China News Service

BRICS communications ministers talk IT cooperation, cybersecurity

Communications Ministers from each of the BRICS countries have met in Hangzhou, China to discuss further cooperation in digital transformation and cybersecurity. The roundtable event was also attended by leading communications and technology companies from each of the five countries.

“A year after major economies jointly published the G20 Blueprint for Innovative Growth, officials from the BRICS group have gathered to further discuss digital transformation during the third BRICS Communications Ministers' Meeting in Hangzhou.

Leading IT and communications companies from the BRICS countries also participated in a round-table, with the group publishing a ministerial manifesto on information technology.”

Privacy

26.07.17

Euractiv

EU court’s blow to Canada deal marks new hurdle for data laws

The European Court of Justice has ruled that the data sharing agreement between the EU and Canada violates the EU’s data privacy protections, in a ruling similar to that which derailed the US-EU Safe Harbour in 2015.

“An EU data sharing agreement with Canada is illegal because it violates privacy rights, the European Court of Justice said Wednesday (26 July), marking a new legal blow to the bloc’s data deals.

The top EU court’s opinion on a draft passenger name record deal with Canada is the latest setback for the European Commission’s data rules—after it knocked down data retention laws and in 2015, the safe harbour agreement allowing companies to transfer personal data to the United States.”

Internet Inclusion

02.08.17

IT Web Africa

'Zero rating not an on-ramp to the internet'

Mozilla has expressed concerns that zero rating could lead the worlds poorest to miss out on access to the internet due to dangerous anti-competitive consequences.

“Experts at Mozilla have expressed concern that zero rating poses dangerous anti-competitive consequences and leaves the poorest users behind in terms of access to the internet.

This is one of the key takeaways from Mozilla-backed research, carried out by Research ICT Africa, focused on how citizens use the internet when data is subsidised and when it is not.”

Global Institutions

31.07.17

ITU

ITU releases 2017 global information and communication technology facts and figures

ITU has published its 2017 report detailing its analysis of the facts and figures of global information and communication technology use. The report identifies the increase in internet access, with notable increases in the number of young people accessing the internet.

“New data released by ITU, the United Nations specialized agency for information and communication technologies (ICTs), show that 830 million young people are online, representing 80 per cent of the youth population in 104 countries. ITU's ICT Facts and Figures 2017 also shows a significant increase in broadband access and subscriptions with China leading the way.

This much-anticipated annual release of global ICT data shows that youths (15-24 year olds) are at the forefront of Internet adoption. In Least Developed Countries (LDCs), up to 35 per cent of individuals using the Internet are aged 15-24, compared with 13 per cent in developed countries and 23 per cent globally. In China and India alone, up to 320 million young people use the Internet.”

01.08.17

ENISA

Cybersecurity workshop organised by ENISA and the Dutch National Cyber Security Center in October

ENISA has announced a new cybersecurity workshop to be held with the Dutch National Cyber Security Center in October which will bring public and private sector stakeholders together to discuss emerging cybersecurity issues.

“ENISA in cooperation with the Dutch National Cyber Security Center (NCSC) is organising a workshop in the Hague, on the 4th of October 2017.

During this event, ENISA will mainly focus on the topics of National Cyber Security Strategies(NCSS), Public Private Partnerships (PPPs) and Information Sharing and Analysis Centers (ISACs) in the EU.”

01.08.17

ICANN

Extended Deadline: Request for Proposal for the SSAC Organizational Review

ICANN have extended the deadline for proposal submissions for its Independent Review of the Security and Stability Advisory Committee.

"The deadline has been extended for the Request for Proposal for the Independent Review of the Security and Stability Advisory Committee (SSAC). The ***new deadline is 21 Aug 2017 at 11:59 PM PDT****.*

The Internet Corporation for Assigned Names and Numbers (ICANN) is seeking a provider to conduct an independent assessment of the Security and Stability Advisory Committee (SSAC)."

Diary Dates

Modernising the regulations establishing the .eu top-level domain name – 05.05.17-04.08.17

European Commission

ITU WTDC-17 – 09.10.17–20.10.17

Buenos Aires, Argentina

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland