20 September 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **European Union**, following Jean-Claude Juncker's earlier speech, is ramping up its **cybersecurity** with a number of new proposals. A new certification scheme will aim to verify different services and products as safe to operate.

Matt Hancock, the **British** Minister for Digital, gave a speech at the **Singapore** international **Cyber Week**. He highlighted the chance for both nations to deepen their relationship on **cybersecurity** and to adapt to the changing global internet.

The **privacy agreement** between the **USA** and the **EU** will not be impacted by Trump's 'America first' (at least for now). The assurance comes after Vera Jourova's, the EU Justice Commissioner, commented on the issue in a media interview.

European Commission Vice-President and Digital Commissioner **Andrus Ansip** wrote about the risk of data protectionism to the **Digital Single Market** in a blog post, highlighting the importance of data sharing across member states.

The Senate passed the **National Defense Authorisation Act** that puts in place a distinct cyber doctrine for responses to **cybercrime** and security issues, as opposed to the previous ad hoc responses to attacks.

Following the large **Equifax breach**, Massachusetts and Hawaii Senator's Elizabeth Warren and Brian Schatz introduced **The Freedom from Equifax Exploitation Act** in an attempt to protect consumers in the future. The proposed legislation would give consumers more control over the data held by credit rating agencies.

Homeland Security has enforced an order requiring government agencies to stop using **Kaspersky software**. The order comes in light of the controversies over the 2016 US Presidential election and fears of further Russian **cyberattacks**.

A **Memorandum of Cooperation** has been agreed between **Singapore** and **Japan** in an attempt to further cooperation on **cybersecurity**. Practices, policy and information reciprocity are included within the agreement.

Estonia has stated its intention to aid **India** in its **cybersecurity**, helping with skills, resources and responses. **NATO** and the **EU** both have their training of cybersecurity in Estonia and the knowledge shared with India would undoubtedly boost its capabilities against cyberattacks.

The **European Union** has passed its **WIFI4EU** law which aims to enable free wi-fi in all public spaces across all European Union nations. The law endeavours to bring about **net neutrality** for the EU.

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

20 September 2017

Table of Contents

Europe

Internet governance

14.09.17

Computer Weekly

Government aligns data laws with GDPR

The UK Data Protection Bill will attempt to align with the current EU GDPR. The new law will aim to allow people in the UK to have better control over their personal data, particularly with reference to social media.

"The UK government announces details of its data protection law that will align with the EU's GDPR. The UK government has announced details of its Data Protection Bill, which it said will update existing law to make it fit for the digital age. The UK Data Protection Bill is the result of a commitment to align data protection laws in the UK with the European Union's (EU's) General Data Protection Regulation (GDPR)."

18.09.17

Government computing

EU wants to tackle "data nationalism"

European Commission Vice-President and Digital Commissioner Andrus Ansip wrote about the risk of data protectionism to the Digital Single Market in a blog post, highlighting the importance of data sharing across member states.

"EU wants to build cross-border data-focused economy within Digital Single Market, reinforce ENISA's role and beef up security standards to raise user confidence in areas like IoT

Ansip highlighted the lack of legal certainty about applicable rules and practices when it comes to data movement, outside the situations covered by forthcoming general Data Protection Regulation (GDPR) regulation. Ansip wants to avoid so called "data localisation" and to increase cross-border storage and processing of data. He proposes the establishment of free movement of data as a basic principle in EU law"

Cybersecurity

14.09.17

Euractiv

Ansip: Member states will need help from EU cyber emergency fund

The European Commission released a cyber security strategy for the EU which aims, amongst other things, to aid nations in their response to cyberattacks. Andrus Ansip followed this up by suggesting that more money will still be asked for after major attacks, despite the strengthening in cybersecurity.

"EU technology chief Andrus Ansip predicted that member states will ask for money from a planned European emergency fund if they suffer major hacking attacks, despite wariness over the EU stepping up its cyber security plans.

"No deep analysis is needed to understand that in some situations, there can really be a need [for emergency funding] in case of a hurricane or an earthquake. It's the same story with large-scale cyber attacks," Commission Vice-President Ansip said in an interview."

19.09.17

European Commission

State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks

The European Union, following Jean-Claude Juncker's earlier speech, is ramping up its cybersecurity with a number of new proposals. A new certification scheme will aim to verify different services and products as safe to operate.

"On 13 September, in his annual State of the Union Address, President Jean-Claude Juncker stated: 'In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks.'

Europeans place great trust in digital technologies. They open up new opportunities for citizens to connect, facilitate the dissemination of information and form the backbone of Europe's economy. However, they have also brought about new risks as non-state and state actors increasingly try to steal data, commit fraud or even destabilise governments."

18.09.17

Economic Times – India Times

Estonia open to assist India on cyber security

Estonia has stated its intention to aid India in its cybersecurity, helping with skills, resources and responses. NATO and the EU both have their training of cybersecurity in Estonia and the knowledge shared with India would undoubtedly boost its capabilities against cyberattacks.

"Estonia is keen to help India combat cyber-attacks by engaging with the South Asian country in joint drills and offering its cutting edge technical resources in the field at a time when cyber strikes across the globe are seen as dangerous to the stability of democracies and growth economies."

15.09.17

Swissinfo

Cabinet seeks more data safety as hackers strike

A cyberattack that hit the Ministry of Defence in Switzerland was thwarted, only seeking to further the statement of the Justice Ministry that further improvements of data protection were needed.

"The Swiss defence ministry foiled a cyberattack by malware similar to that used in other global hacking campaigns, the government revealed on Friday, the same day the justice ministry presented plans for improved data protection.

Experts discovered the attacks – which were carried out with the Turla malware, a sophisticated virus used for cyber-espionage – on several servers of the defence ministry and a contractor of the foreign ministry in July, according to the cabinet spokesman.The government declined to give information about the origin of the attack or say whether any damage including data theft had occurred. It cited security considerations."

Privacy

19.09.17

Euractiv

Jourova reassured 'America first' does not weigh on EU-US privacy shield

The privacy agreement between the USA and the EU will not be impacted by Trump's 'America first'(at least for now). The assurance comes after Vera Jourova's, the EU Justice Commissioner, commented on the issue in a media interview.

"EU Justice Commissioner Věra Jourová said she was relieved that US President Trump's "America first" policy will not shatter the EU-US privacy shield agreement on data transfers, after meeting with Commerce Secretary Wilbur Ross on Monday (18 September) to scrutinise the one-year-old deal.

Jourová and a group of data protection watchdogs from EU countries started a process to review the EU-US data transfer agreement in Washington with Ross and other US officials. The review has been highly anticipated because Jourová could pull the plug on the controversial deal if she decides that American authorities have not set up enough safeguards to protect EU citizens' privacy."

18.09.17

Computer Weekly

Heads roll as Equifax reveals 400,000 Britons affected by breach

The huge Equifax breach that heavily impacted the USA, also managed to affect over 400,000 British consumers. Although the UK systems were not involved in the breach, a number of British consumers' data was being stored in the USA, which has consequently led to the dismissal of two senior staff.

"Equifax replaces two senior staff members as it reveals how many Britons were hit by a massive data breach that affected millions of consumers. Financial services firm Equifax has revealed that around 400,000 UK consumers were affected by the data breach earlier this year alongside more than 140 million US and Canadian consumers.

The company said Equifax UK systems were not affected by the breach, but a file containing UK consumer information may have potentially been accessed. This was due to a "process failure", corrected in 2016, which the company said led to a limited amount of UK data being stored in the US between 2011 and 2016."

15.09.17

Silicon Republic

PwC cybersecurity lead on GDPR: 'Everybody is starting too late'

Cybersecurity investment is not large enough, according to PWC, which is not a good sign for the impending GDPR which will heavily impact many EU organisations.

"As the countdown begins to GDPR, Irish and European organisations are seriously underprepared, says PwC's Pat Moran. For the second year running, Irish CIOs and CEOs are being invited to take part in PwC's Economic Crime Survey (deadline Friday 22 September). It is already apparent to the consulting firm's Irish cybersecurity lead, Pat Moran, that very few tech leaders in Ireland are investing sufficiently in their cyber defences.

This is despite an unprecedented rise in cyberattacks globally, manifesting in major malware such as WannaCry, botnets targeting the internet of things, embarrassing data leakages at local banks and the recent data breach at Equifax."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

15.09.17

Engadget

The missing trade war against China's digital protectionism

China has been continuing its own standards for the internet through blocking and censorship. Nigel Cory, an analyst of trade policy at the Information Technology and Innovation Foundation has stated *"China's extensive use of digital trade barriers ... have reshaped the production and sales of many global tech sectors as they've been forced to either adapt to China's restrictive and costly requirements or avoid the market entirely,"*

Cybersecurity

19.09.17

Politico

Political campaigns prep for battle with hackers

Eversince the hacks during the US presidential election last year, new cybersecurity plans have been enforced for the upcoming campaigns in the USA. The Democratic Party in particular have started using encrypted messaging apps rather than internal email in order to avoid further attacks.

"Candidates are quizzing prospective campaign managers on anti-hacking plans. Democratic committees like the Democratic Congressional Campaign Committee, which was breached last year, have switched internally from email to encrypted messaging apps. And both parties are feverishly trying to spread advice and best practices to new campaigns before they become targets.

The political world is officially obsessed with cybersecurity in 2017 — especially the Democrats burned by the hacking of their committees and operatives during the 2016 election. Much of the Democratic Party's permanent apparatus has already changed its day-to-day operations as a result, while beginning the slow process of persuading its decentralized, startup-like campaign ecosystem to follow suit."

18.09.17

The Hill

Senate's defense authorization would set cyber doctrine

The Senate passed the National Defense Authorisation Act that puts in place a distinct cyber doctrine for responses to cybercrime and security issues, as opposed to the previous ad hoc responses to attacks.

"The National Defense Authorization Act (NDAA) passed Monday by the Senate mandates a thorough, distinct doctrine for cyber warfare, filling a void long bemoaned by lawmakers. Legislators, particularly Senate Armed Services Committee Chairman John McCain (R-Ariz.), have complained about the ad hoc approach to responding to, conducting and deterring cyberattacks since the Obama administration.

'The threat is growing, yet we remain stuck in a defensive crouch, forced to handle every event on a case-by-case basis, and woefully unprepared to address these threats,' McCain said in May."

Privacy

19.09.17

Euractiv

Jourova reassured 'America first' does not weigh on EU-US privacy shield

The privacy agreement between the USA and the EU will not be impacted by Trump's 'America first'(at least for now). The assurance comes after Vera Jourova's, the EU Justice Commissioner, commented on the issue in a media interview.

"EU Justice Commissioner Věra Jourová said she was relieved that US President Trump's "America first" policy will not shatter the EU-US privacy shield agreement on data transfers, after meeting with Commerce Secretary Wilbur Ross on Monday (18 September) to scrutinise the one-year-old deal.

Jourová and a group of data protection watchdogs from EU countries started a process to review the EU-US data transfer agreement in Washington with Ross and other US officials. The review has been highly anticipated because Jourová could pull the plug on the controversial deal if she decides that American authorities have not set up enough safeguards to protect EU citizens' privacy."

15.09.17

SCmagazine

600,000 Alaskan voters' data left exposed

A database which held nearly 600,000 Alaskan voters' data became public on the internet due to a breach that the protection software company did not manage to secure.

"Kromtech Security Center researchers discovered an unsecured U.S. voter database was exposed to the public internet due to a misconfiguration of CouchDB instance. The database contained information on 593,328 Alaskan voters and appeared to be part of VoterBase, a national voter file compiled and provided by TargetSmart, a provider of political data and technology, according to a Sept. blog post.

The breach was attributed to Minnesota AI software firm Equals3's failure to secure some of their data and some data they license from TargetSmart. The AI company claims that misconfigured information has since been secured and said although the data was left exposed, it wasn't accessed by unauthorized personnel."

18.09.17

SCmagazine

Warren, Schatz introduce bill to protect consumers after Equifax breach

Following the large Equifax breach, Massachusetts and Hawaii Senator's Elizabeth Warren and Brian Schatz introduced The Freedom from Equifax Exploitation Act in an attempt to protect consumers in the future. The proposed legislation would give consumers more control over the data held by credit rating agencies.

"In the wake of a massive Equifax breach that left sensitive information on 143 million consumers at risk, a bill introduced Friday by Sen. Elizabeth Warren, D-Mass., and Sen. Brian Schatz, D-Hawaii, would give consumers more control over their credit and personal data and help prevent future incidents. The Freedom from Equifax Exploitation (FREE) Act would also put strictures in place to keep credit monitoring companies from profiting off of the breach in part by preventing them from selling information during a credit freeze."

15.09.17

Newburgh Gazette

U.S. bans govt use of Russian Kaspersky Newburgh Gazette

Homeland Security has enforced an order requiring government agencies to stop using Kaspersky software. The order comes in light of the controversies over the 2016 US Presidential election and fears of further Russian cyberattacks.

"The US government's Department of Homeland Security has issued an order to governmental agencies that they should stop using Kaspersky software over fears of Russian-led cyberespionage. The US Department of Homeland Security (DHS) on Wednesday directed federal departments and agencies to remove Kaspersky Lab products from their information systems. 'If there is even a breadcrumb of evidence that Kaspersky may be meddling with the Russian government, then obviously that is a problem for the fed', said Robert Siciliano, a cybersecurity expert with Hotspot Shield.

It said Wednesday that its products have been sold at Best Buy for a decade. What did the USA government actually do? Nicholas Weaver, a computer security researcher at the University of California, Berkeley, called the USA government decision "prudent"; he had argued for such a step in July."

Internet Inclusion

19.09.17

Nextgov

Broadband is largely inaccessible to those who need it most

Net neutrality is an unfamiliar concept for the US, according to the Brookings Institution who have stated in a report that the poorest areas and most rural areas are far less likely to have strong or indeed any broadband.

"The internet is a way for people in poorer or far-flung communities to connect with social programs and educational opportunities, such as employment and health services, to which they might not otherwise have access. But according to a new report from the Brookings Institution, residents in low-income or rural neighborhoods are the least likely to have broadband subscriptions.

The current standard for broadband in the U.S. is internet with a 25 Mbps (Megabits per second) download speed. The richer and more educated a neighborhood is, the Brookings report says, the more likely its residents are to have internet that reaches that threshold. While 73 percent of Americans have broadband service in their homes, college graduates are three times more likely to have the subscription than high-school graduates."

19.09.17

Truthdig

[FCC Pressured to Release Complaints in Net Neutrality Case]

The strides made by Obama on net neutrality are set to be retracted by the Federal Communications Commission. An abundance of complaints and comments, however, were made to the Commission, and a record of the complaints given have asked to be released by a number of organisations.

"Last month, the Federal Communications Commission was flooded with 22 million comments on its plan to roll back Obama-era net neutrality protections. Now, interest groups are asking for information on complaints and a new public comment period to review those complaints.

According to an email released by the National Hispanic Media Coalition, the organization has 'filed a joint Motion, with 20 additional organizations, in the FCC's Restoring Internet Freedom Notice of Proposed Rulemaking (NPRM) proceeding asking the FCC to enter into the record all open internet complaints, ombudsperson correspondence and carrier responses since the 2015 Open Internet Order, and set a comment period to allow for public input on the new evidence.'"

Pan-Asia

Internet governance

19.09.17

Network Asia

Singapore, Japan sign Memorandum of Cooperation on Cybersecurity

A Memorandum of Cooperation has been agreed between Singapore and Japan in an attempt to further cooperation on cybersecurity. Practices, policy and information reciprocity are included within the agreement.

"Singapore and Japan have signed a Memorandum of Cooperation (MOC) to strengthen cybersecurity cooperation between the two countries. The MOC was signed by Mr David Koh, Chief Executive, Cyber Security Agency of Singapore (CSA), and Dr Ikuo Misumi, Deputy Director-General of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Japan.

The MOC covers cybersecurity cooperation in key areas including regular policy dialogues, information exchanges, collaborations to enhance cybersecurity awareness, joint regional capacity building efforts, as well as sharing of best practices between both countries."

19.09.17

Network Asia

ASEAN members agree on importance of closer coordination of regional efforts

An attempt to build further trust between ASEAN members in order to create some sort of internet standard between member states was secured during the Singapore International Cyber Week. Building upon current norms, a shared standard is becoming more likely.

"At the second ASEAN Ministerial Conference on Cybersecurity (AMCC), ASEAN Member States expressed their support for the development of basic, operational and voluntary norms of behavior to guide the use of ICTs in ASEAN in a responsible manner. These would take reference from the norms set out in the 2015 Report of the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

The Conference, part of the Singapore International Cyber Week 2017, agreed that such norms will help to enhance trust among ASEAN Member States and build confidence in the use of cyberspace so as to harness its full potential to bring about greater economic prosperity."

Cybersecurity

20.09.17

Out-Law

Singapore cybersecurity bill delayed until 2018

Despite progress being made in Singapore on fighting cybercrime, the cybersecurity bill has been further delayed to allow for the increased consideration of a number of key issues. The delay will be for the better but will leave the nation vulnerable for a little while longer.

"Yaacob Ibrahim, minister for communications and information told a cybersecurity conference this week that the government has consulted with stakeholders including sector leads, potential critical information infrastructure (CII) owners, and the wider industry, and extended the public consultation period in response to interest in the legislation.

Technology law expert Bryan Tan of Pinsent Masons MPillay, the Singapore joint venture partner of Pinsent Masons, the law firm behind Out-Law.com, said: 'While the delay allows the various stakeholders more time to consider the issues, the cybersecurity threat is an ever-present danger and organisations should remain on their guard and harden their digital defences even as the legislation makes its passage.'"

18.09.17

Economic Times – India Times

Estonia open to assist India on cyber security

Estonia has stated its intention to aid India in its cybersecurity, helping with skills, resources and responses. NATO and the EU both have their training of cybersecurity in Estonia and the knowledge shared with India would undoubtedly boost its capabilities against cyberattacks.

"Estonia is keen to help India combat cyber-attacks by engaging with the South Asian country in joint drills and offering its cutting edge technical resources in the field at a time when cyber strikes across the globe are seen as dangerous to the stability of democracies and growth economies."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

19.09.17

Computer Weekly

UAE banks share information to combat cyber threats

A new programme launched by the UAE's banking federation will allow for banks to share cybersecurity and attack information between themselves in order to prevent future attacks.

"Banks in the United Arab Emirates will share information on cyber attacks through a platform instigated by the country's banking federation. United Arab Emirates banks are sharing information about cyber attacks through a platform from the UAE Banks Federation (UBF).

Initially, 13 of the UBF's 48 member banks will share information via the Information Sharing and Analysis Center (ISAC), which is provided by security software supplier Anomali."

Privacy

15.09.17

Newburgh Gazette

U.S. bans govt use of Russian Kaspersky Newburgh Gazette

Homeland Security has enforced an order requiring government agencies to stop using Kaspersky software. The order comes in light of the controversies over the 2016 US Presidential election and fears of further Russian cyberattacks.

"The US government's Department of Homeland Security has issued an order to governmental agencies that they should stop using Kaspersky software over

fears of Russian-led cyberespionage. The US Department of Homeland Security (DHS) on Wednesday directed federal departments and agencies to remove Kaspersky Lab products from their information systems. 'If there is even a breadcrumb of evidence that Kaspersky may be meddling with the Russian government, then obviously that is a problem for the fed', said Robert Siciliano, a cybersecurity expert with Hotspot Shield.

It said Wednesday that its products have been sold at Best Buy for a decade. What did the USA government actually do? Nicholas Weaver, a computer security researcher at the University of California, Berkeley, called the USA government decision "prudent"; he had argued for such a step in July."

Internet Inclusion

No new items of relevance

Global Institutions

17.09.17

ITU

New Broadband Commission report highlights emerging global skills gap

A skills gap in technology has been announced by the Broadband Commission. With the growing technological importance today it is vital that the gap is closed in order to engage and engage in society.

"A new report from the Broadband Commission for Sustainable Development entitled "Digital skills for life and work" shows that education systems worldwide are only just beginning to help learners cultivate the digital skills they need to excel in in our increasingly digitized societies.

The report, released today, highlights the emergence of a new global skills gap where gender, class, geography and age can have a huge impact on whether a person is able to harness new technologies or not. It also presents strategies for ensuring all groups of people can develop these skills."

14.09.17

European Parliament

EU funds for fast and free internet connection all over Europe

The European Union has passed its WIFI4EU law which aims to enable free wi-fi in all public spaces across all European Union nations. The law endeavours to bring about net neutrality for the EU.

"MEPs have approved WIFI4EU, a scheme to promote free wi-fi connectivity in public spaces across the EU. The objective of the WIFI4EU European initiative is to provide more than 6,000 communities across the EU with free high-speed wi-fi connection by 2020. Access to this initiative is reserved to public entities with spaces open to the public such as libraries, hospitals, parks, train stations and bus terminals. They would receive a grant from the EU to set up free wi-fi connection points.

MEPs approved the agreement negotiated with the Council during the plenary session on 12 September. Applications could already be submitted at the beginning of next year. "This is the opportunity to give a more broad and equal access, more inclusive access to the future for all Europeans — free access to high-quality internet independent of geographical location, independent of how much money they earn," said Portuguese S&D member Carlos Zorrinho, who is responsible for steering the proposal through Parliament."

20.09.17

Europol

[Joint action day targets counterfeiters on the darknet]

The EU has engaged in a joint action day that managed to lead to the arrest of over fifty cybercriminals. The success has highlighted the growing importance of cooperation in order to defeat cyberattacks and succeed in security.

"A joint action day carried out by seven EU Member States and coordinated by Europol has resulted in the arrest of 53 criminals active on the Darknet. The arrestees were involved in buying and/or selling counterfeit euro banknotes on illegal Darknet marketplaces, such as AlphaBay and Hansa Market.

In February 2017, Austrian authorities dismantled an illegal euro banknote print shop in Vienna and arrested one person. The data retrieved from this operation mainly related to illegal euro banknote counterfeiting on the Darknet. Among the documents seized, investigators found details of 33 different European and non-European countries to which the arrested person had sent counterfeit money."

Diary Dates

No new items of relevance