# IEEE GLOBAL INTERNET POLICY MONITOR

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

## 19 April 2017

## Synopsis

**Scroll to read full summaries with links to news articles.**

The **EU** will launch a public consultation into concerns about the future of the **internet**. A succession of surveys will seek “fresh ideas” on issues such as **privacy**, **security**, **AI**, **net neutrality** and **big data**.

A committee of **UK** Members of Parliament has published a report calling for the Government to set up a “monitoring unit” to protect against foreign interference in future **elections**. The recommendations follows allegations of Russian **hacking** in the US election, and reports that a foreign source may have hacked a voter registration website prior to the EU referendum vote last June.

The **British** Chamber of Commerce reported that one in five businesses fell victim to a **cyberattack** in the last year, whilst Government statistics revealed that seven in ten large companies have a identified a cyberattack.

In the **United States**, an adviser to former US President Obama has warned that increasingly **data** will be **weaponised** by foreign states and hostile groups in attempts to undermine democratic **elections**.

Comments made by US Senator Jim Sensenbrenner at a town hall meeting in Wisconsin have gained wide criticism, following his remark that “nobody’s got to use the internet” after voting against introducing information safeguards.

In **Asia**, the World Economic Forum Global Risks Report 2017 has listed **cyberattacks** as the sixth biggest risk to doing business in the APAC reason. It suggests that $81bn was lost by businesses in the region due to cyberthreats.

The Head of **US** Homeland Security **John Kelly** has said that he is more concerned about a **cyberattack** emanating from **North Korea** than a kinetic attack. Meanwhile the former British Foreign Secretary **Sir Malcolm Rifkind** suggested that North Korea’s thwarted nuclear test may have been sabotaged by a US cyberattack.

Copyright © 2017 IEEE. All rights reserved.

The Independent reported that **Snapchat** suffered a **cyber hack** making personal information of 1.7 million people vulnerable. Snapchat have denied that it has been hacked.

Members of the **African** Network Information Centre have discussed denying **internet access** to African Governments that shut down public internet access as a guard against authoritarian rulers.

Meanwhile a cyber analyst in **South Africa** has said that the number of **cyberattacks** in the country last year reached 8.8 million.

The trade association **Digital Europe** has published a position paper on the EU Commission's proposals for **ePrivacy** regulations, and has sent a letter to the EU Parliament, encouraging them to vote against a proposed resolution on the **EU - US Privacy Shield**.

Copyright © 2017 IEEE. All rights reserved.

# IEEE Global Internet Policy Monitor

**19 April 2017**

## Table of Contents

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

Copyright © 2017 IEEE. All rights reserved.

# Europe

## Internet governance

**12.14.17**

**Public Knowledge**

**EU to US: Undoing Broadband Privacy Signals U.S. Is Not Serious About Privacy Protections**

Members of the European Union Parliament are concerned that the United States are not taking privacy protection seriously enough, specifically in regards to President Trump's decision to change broadband privacy rules.

*"Last week, the European Parliament (EP) passed a resolution manifesting concern over the EU - US Privacy Shield, a legal scheme that allows American companies to transfer personal data from the European Union to the United States. In a nutshell, the EP is worried that the U.S. government doesn't take privacy protection seriously, and the Members of the European Parliament (MEPs) make explicit reference to, among other things, the Trump administration's undoing of the Federal Communication Commission's broadband privacy rules.*

*MEPs are worried that the takedown of Broadband Privacy provisions signals a lack of commitment of the Trump Administration with the protection of privacy and Privacy Shield."*

**18.04.17**

**The Guardian**

**EU launches public consultation into fears about future of internet**

The EU will launch a public consultation into concerns about the future of the internet. A succession of surveys will seek "fresh ideas" on issues such as privacy, security, AI, net neutrality and big data.

*"Privacy, security, artificial intelligence, net neutrality, big data and impact of internet on daily life among topics included in surveys. The European commission president, Jean-Claude Juncker, said the consultation would 'inspire fresh ideas' to solve society's problems.*

*The EU is launching an unprecedented public consultation to find out what Europeans fear most about the future of the internet.*

*A succession of surveys over the coming weeks will ask people for their views on everything from privacy and security to artificial intelligence, net neutrality, big* *data and the impact of the digital world on jobs, health, government and democracy."*

## Cybersecurity

**12.04.17**

**S.C Media**

**Parliamentary committee proposes unit to combat 'election hacking'**

A committee of UK members of Parliament called the Public Administration committee has published a report calling for the Government to set up a "monitoring unit" to protect against foreign interference in future elections. The recommendations follows allegations of Russian hacking in the US election, and reports that a foreign source may have hacked a voter registration website prior to the EU referendum vote last June.

*"A parliamentary committee has proposed a monitoring unit in order to ward off the threat of foreign powers trying to influence UK election.*

*The parliamentary committee was attempting to address the threat of election hacking. Parliament has recommended a "monitoring unit" to help ensure the integrity of UK Democracy. The Commons Public Administration committee, says as much in a new report, in an effort to safeguard the UK's voting systems against "election hacking" or interference by foreign powers."*

**18.04.17**

**Computer Weekly**

**UK businesses need to up cyber security with one in five hit by attacks**

The British Chamber of Commerce reported that one in five businesses fell victim to a cyberattack in the last year, with 21% of businesses believing the cyberthreats are preventing their companies from financial growth.

*"Big UK businesses are targeted by cyber attacks more heavily, but all need to improve cyber security with one in five UK firms falling victim in the past 12 months, a survey reveals*

*Out of the 20% of UK businesses hit by cyber attacks in the past year, 42% were companies with more than 100 staff, compared with 18% with fewer than 99 employees, according to the survey of more than 1,200 businesses by the British Chambers of Commerce (BCC)."*

**19.04.17**

**UK Government**

**Almost half of UK firms hit by cyber breach or attack in the past year**

Copyright © 2017 IEEE. All rights reserved.

Government statistics have revealed that seven in ten large companies have an identified a cyberattack in the past year, with companies holding individuals personal information the most susceptible to an attack.

*“Nearly seven in ten large companies identified a breach or attack, new Government statistics reveal. Businesses large and small are being urged to protect themselves against cyber crime after new Government statistics found nearly half of all UK businesses suffered a cyber breach or attack in the past 12 months.*

*The Cyber Security Breaches Survey 2017 reveals nearly seven in ten large businesses identified a breach or attack, with the average cost to large businesses of all breaches over the period being £20,000 and in some cases reaching millions. The survey also shows businesses holding electronic personal data on customers were much more likely to suffer cyber breaches than those that do not (51 per cent compared to 37 per cent).”*

## Privacy

**10.04.17**

**Euractiv**

**Romanian EU-funded project accused of data protection violations**

The Romanian Government has been accused of misappropriating EU funding to state Intelligence Services.

*“The Romanian government has been accused of bias in its awarding of EU funding to the country’s intelligence services. The e-Governance project is also facing serious allegations that it violates European and domestic laws on personal data protection.*

*A group of Romanian NGOs has submitted a claim to the European Anti-fraud Office (OLAF) alleging that over €26 million in EU funding has been misappropriated by the Romanian Intelligence Services (SRI) and that the process launched to award the money was unfair.”*

## Internet Inclusion

***No new items of relevance***

Copyright © 2017 IEEE. All rights reserved.

# United States of America

## Internet governance

**12.04.17**

**Public Knowledge**

**EU to US: Undoing Broadband Privacy Signals U.S. Is Not Serious About Privacy Protections**

Members of the European Union Parliament are concerned that the United States are not taking privacy protection seriously enough, specifically in regards to President Trump's decision to change broadband privacy rules.

*"Last week, the European Parliament (EP)* passed a resolution *manifesting concern over the EU-US* Privacy Shield*, a legal scheme that allows American companies to transfer personal data from the European Union to the United States. In a nutshell, the EP is worried that the U.S. government doesn't take privacy protection seriously, and the Members of the European Parliament (MEPs) make explicit reference to, among other things, the Trump administration's* undoing *of the Federal Communication Commission's* broadband privacy rules*.*

*MEPs are worried that the takedown of Broadband Privacy provisions signals a lack of commitment of the Trump Administration with the protection of privacy and Privacy Shield."*

## Cybersecurity

**13.04.17**

**SC Media**

**SC Media spies on NSA's annual Cyber Defense Exercise**

The NSA has carried out an annual defence exercise to test out young students in US and Canadian academies. The purpose of the test it to assess the cyber skills of the US coastguard academy, US Merchant Marine Academy, US Military academy.

*"SC Media was granted inside access to the NSA's annual Cyber Defense Exercise, where computer network specialists tested the network security know-how of the finest young tech minds the U.S. and Canadian military academies have to offer.*

*They're called the "Red Cell" – a team of computer network specialists, working under the auspices of the* National Security Agency*, whose mission is to*

Copyright © 2017 IEEE. All rights reserved.

*relentlessly launch cyberattacks against the finest young tech minds the U.S. and Canadian military academies have to offer."*

**13.04.17**

**Politico**

**[CIA director labels WikiLeaks a 'hostile intelligence service']**

The CIA has classified WikiLeaks as a non-state hostile intelligence service, which has served as a middle man for aggressive Russian hackers.

*"CIA Director Mike Pompeo launched a broadside Thursday against the anti-secrecy group WikiLeaks, calling it a "non-state hostile intelligence service often abetted" by hostile countries like Russia.*

*"WikiLeaks walks like a hostile intelligence service, and talks like a hostile intelligence service," Pompeo said at the Center for Strategic and International Studies in his first public remarks since becoming CIA chief."*

**14.04.17**

**The Hill**

**[DHS head: North Korea more of a cyber threat]**

The Head of US Homeland Security John Kelly has said that he is more concerned about a cyberattack emanating from North Korea than a kinetic attack.

*"Homeland Security Secretary John Kelly said he's more concerned about North Korea launching a cyber attack on the U.S. than any direct military action.*

*"In the case of North Korea, you know, a kinetic threat against the United States right now I don't think is likely, but certainly a cyber threat," he said in an interview set to air Sunday with NBC's "Meet the Press."*

*"So we would raise various threat levels in the event that something happened and we felt as though there were a possible threat. You always want to come down on the side of caution."*

**16.04.17**

**The Telegraph**

**[North Korea's unsuccessful missile launch 'may have been thwarted by US cyber attack']**

Former British Foreign Secretary Sir Malcolm Rifkind suggested that North Korea's thwarted nuclear test may have been sabotaged by a US cyberattack.

*"Missiles are driven past the stand during a military parade marking the 105th birth anniversary of country's founding father in Pyongyang*

Copyright © 2017 IEEE. All rights reserved.

*A North Korean missile launch that failed shortly after it was fired may have been thwarted by cyber attacks from the US.*

*The medium-range missile exploded seconds after it was launched on Sunday from a site near the port city of Sinpo, as Mike Pence, the US vice president, arrived in Seoul for talks with the South Korean government over how to deal with Pyongyang's belligerence."*

**18.04.17**

**The Hill**

**Former Obama adviser: Election-style hacks 'bound' to happen again**

In the United States, an adviser to former US President Obama has warned that increasingly data will be weaponised by foreign states and hostile groups in attempts to undermine democratic elections.

*"A former adviser to President Obama predicts that nation-states and others will try to use cyber intrusions to disrupt future election processes and "weaponize" data as Russia did during the 2016 U.S. presidential election.*

*The hacks targeting high-level Democratic Party officials marked a "new threshold" in cyber activity, Lisa Monaco, who advised Obama on homeland security and counterterrorism, told CNN commentator David Axelrod on his podcast "The Axe Files."*

**19.04.17**

**Computer Weekly**

**Skype most popular communication channel for cyber criminals**

The Cyber Criminal Network has published a report suggesting that Skype is the most commonly attacked software by cybercriminals, ahead of AOL, WeChat, QQ and WhatsApp.

*"The cyber criminal network is truly global and collaborative, making use of popular messaging services, a study has revealed.*

*Skype is the most popular communication platform for cyber criminals, and appears in the top five for the seven language groups analysed by business risk intelligence firm Flashpoint.*

*Skype use was highest across the English language criminal underground from 2012 to 2016, but more recently it has ceded ground to Jabber, ICQ and Kik Messenger."*

Copyright © 2017 IEEE. All rights reserved.

## Privacy

**15.04.17**

**The Hill**

**Microsoft: All security issues from NSA leaks patched in current software**

Microsoft has said that software flaws exposed in a cyber hack have been fixed.

*"Microsoft says all of the security flaws exposed in Friday's leak of National Security Agency (NSA) hacking tools were already fixed in supported versions of its software.*

*In a late Friday blog post, a top Microsoft security figure lists the NSA hacking tools published Friday by the leakers known as "The Shadowbrokers," and notes the specific software update that patched each flaw that every individual tool exploited."*

**17.04.17**

**The Register**

**'Nobody's got to use the internet,' argues idiot congressman in row over ISP privacy rules**

Comments made by a US Senator named Jim Sensenbrenner at a town hall meeting in Wisconsin have gained wide criticism, after saying that "nobody's got to use the internet" after voting against introducing information safeguards.

*"Faced with an angry citizen asking why he had voted away their online privacy rights, US House Rep Jim Sensenbrenner (R-WI) had a remarkable answer: you don't have to use the internet if you don't like it.*

*Speaking at a town hall meeting in Wisconsin on Friday, the Republican legislator was asked about his vote to kill off proposed information safeguards – a move that effectively gave American ISPs the green light, as well as the right, to sell subscribers' sensitive personal details without requiring their consent or even having to inform them."*

**18.04.17**

**Morning Consult**

**McSweeny: FTC Cannot Maintain Internet Privacy Alone**

A Democratic Federal Trade Commissioner has criticised the changes to privacy regulations, warning of the dangers of the "no cops on the beat approach to privacy and data security".

*"The lone Democratic commissioner at the Federal Trade Commission, Terrell McSweeny, is criticizing the recent reversal of privacy regulations passed by the*

Copyright © 2017 IEEE. All rights reserved.

*Federal Communications Commission, saying her agency cannot be solely responsible for policing internet service providers' privacy practices and maintaining the principles of an open internet.*

*During a Monday event at New America's Open Technology Institute, McSweeny took aim at a measure passed by Congress — and signed into law by President Donald Trump April 3 — repealing the FCC's broadband privacy rules."*

## Internet Inclusion

***No new items of relevance***

Copyright © 2017 IEEE. All rights reserved.

# Pan-Asia

## Internet governance

***No new items of relevance***

## Cybersecurity

**14.04.17**

**The Hill**

**DHS head: North Korea more of a cyber threat**

The Head of US Homeland Security John Kelly has said that he is more concerned about a cyberattack emanating from North Korea than a kinetic attack.

*“Homeland Security Secretary John Kelly said he's more concerned about North Korea launching a cyber attack on the U.S. than any direct military action.*

*“In the case of North Korea, you know, a kinetic threat against the United States right now I don’t think is likely, but certainly a cyber threat,” he said in an interview set to air Sunday with NBC's "Meet the Press."*

*“So we would raise various threat levels in the event that something happened and we felt as though there were a possible threat. You always want to come down on the side of caution.”*

**18.04.17**

**Security Asia**

**Cyberattacks ranked 6th biggest risk to doing business in APAC**

The World Economic Forum Global Risks Report 2017 has listed cyberattacks as the 6th biggest risk to doing business in the APAC reason. It suggests that $81bn was lost by businesses in the region due to cyberthreats.

*“Cyberattacks moved up in the ranks to become the sixth biggest risk to doing business in APAC, according to the APAC results of the World Economic Forum (WEF) Global Risks Report 2017, produced in partnership with Zurich Insurance.*

*In a complex environment – which cost the global economy an estimated US$315 billion through cybercrime in 2015, $81bn of which was lost in APAC – executives in Australia, Japan, Malaysia, New Zealand and Singapore single out cyberattacks as a top three risk of highest concern.”*

Copyright © 2017 IEEE. All rights reserved.

**18.04.17**

**Security Asia**

**40% of industrial computers faced a cyberattack in 2nd half of 2016**

A report from Kaspersky Lab's has revealed that half of industrial computers faced a cyberattack in the back six months of 2016.

*"On average two-in-five computers, related to the technological infrastructure of industrial enterprises, faced cyberattacks in the second half of 2016. This is a finding from Kaspersky Lab's report, the "Threat Landscape for Industrial Automation Systems in the second half of 2016."*

*The percentage of industrial computers under attack grew from over 17% in July 2016 to more than 24% in December 2016, with the top three sources of infection being the Internet, removable storage devices, and malicious e-mail attachments and scripts embedded in the body of e-mails."*

## Privacy

**18.04.17**

**SC Media**

**Details on 1.7M Snapchat users allegedly posted in India**

The Independent reported that Snapchat suffered a cyber hack making personal information of 1.7 million people vulnerable. Snapchat have denied that it has been hacked.

*"Snapchat CEO Evan Spiegel might want to tone down his comments while discussing the target demographic for his app.*

*A former employee at Snapchat, instigating a lawsuit, told a Los Angeles court that Spiegel interrupted him as he was making a presentation about the app's growth prospects overseas. "This app is only for rich people. I don't want to expand into poor countries like India and Spain," Spiegel said, according to Anthony Pompliano, who worked at the company for three weeks after moving over from Facebook."*

## Internet Inclusion

**17.04.17**

**Business Insider**

**For Filipinos, poor Internet connection a more bothersome issue than poverty, corruption**

Copyright © 2017 IEEE. All rights reserved.

A survey was recently conducted in the Philippines about the biggest problems the country faced, and poor internet connection came out as top, ahead of poverty, corruption, food security and energy security.

*"Bad Internet connection is a more pressing problem in the country compared to poverty and corruption, according to a study released by the Philippine Institute for Development Studies (PIDS).*

*In a discussion paper, PIDS Research Information Department Director Sheila Siar, Senior Research Fellow Jose Ramon Albert, and President Gilberto Llanto said this concern may have stemmed from the dependence of the country on the services sector, particularly the business-process outsourcing (BPO) industry."*

**19.04.17**

**China Daily**

**'Sense of benefit' highlighted as China strives to build cyber power**

China is making a concerted effort to improve rollout of internet coverage in its rural areas; Chairman of Alibaba Jack Ma has described this as "an historic opportunity for China".

*"Internet was once virtually unheard of in China's rural areas, but after over two decades, even the most remote villages have access.*

*"I used to spend about 10 days claiming back hospital expenses, but now, one day is enough," said Tian Chenglin, a villager in Northwest China's Ningxia Hui autonomous region, citing the high efficiency of the internet."*

Copyright © 2017 IEEE. All rights reserved.

# Rest of the World

## Internet governance

**18.04.17**

**All Africa**

**African Governments That Shut Down the Internet Could Lose It**

Members of the African Network Information Centre have discussed denying internet access to African Governments that shut down internet access, as an anti-shutdown policy against authoritarian rulers.

*"In an unprecedented policy suggestion, some members of the AFRINIC community have proposed denying internet to African governments that shut it down in their respective countries.*

*AFRINIC stands for African Network Information Centre, and it is one of the world's five regional internet registries, with responsibility for Africa."*

**19.04.17**

**XINHUA Net**

**Rwanda seeks to digitize education system**

The Rwandan Government has announced plans to digitise its educational system in an aim to lower the cost of delivering the teaching whilst improving overall standards in education.

*"Rwanda has announced plans to digitize education system to further innovation, social inclusion, job creation, education quality and national competitiveness, the education minister said Wednesday.*

*Musafiri Papias Malimba told reporters that the country entered an agreement with Microsoft Corporation to digitize Rwanda education through a "smart-classroom" project."*

## Cybersecurity

**18.04.17**

**Security Asia**

**Cyberattacks ranked 6th biggest risk to doing business in APAC**

The World Economic Forum Global Risks Report 2017 has listed cyberattacks as the 6th biggest risk to doing business in the APAC reason. It suggests that $81bn was lost by businesses in the region due to cyberthreats.

Copyright © 2017 IEEE. All rights reserved.

*"Cyberattacks moved up in the ranks to become the sixth biggest risk to doing business in APAC, according to the APAC results of the World Economic Forum (WEF) Global Risks Report 2017, produced in partnership with Zurich Insurance.*

*In a complex environment – which cost the global economy an estimated US$315 billion through cybercrime in 2015, $81bn of which was lost in APAC – executives in Australia, Japan, Malaysia, New Zealand and Singapore single out cyberattacks as a top three risk of highest concern."*

**19.04.17**

**SABC**

**Cyber-attacks reaching a critical point in SA**

Meanwhile a cyber analyst in South Africa has said that the number cyberattacks in the country last year reached 8.8 million.

*"Chief Technology Officer at Gold N' Links Cyber Jim Green says last year alone 8.8 million South Africans admitted to being cyber attacked in one form or another.*

*Chief Technology Officer at Gold N' Links Cyber, Jim Green, says last year alone 8.8 million South Africans admitted to being cyber attacked in one form or another.(SABC)*

*According to reports cyber-attacks are increasing at an alarming rate. In 2015, more than 500 million personal records were stolen or lost due to cyber-crime, since then Phishing, a form of cyber-fraud increased to 55%."*

## Privacy

***No new items of relevance***

## Internet Inclusion

***No new items of relevance***

Copyright © 2017 IEEE. All rights reserved.

# Global Institutions

**18.04.17**

**EU Parliament News**

**E-privacy: MEPs look at new rules to safeguard your personal details online**

Members of the European Union Parliament are concerned that the United States are not taking privacy protection seriously enough, specifically in regards to President Trump's decision to change broadband privacy rules.

*"The EU could soon have new privacy rules to take account of new practices such as internet-based messaging and allow users better control of their privacy settings, especially when it comes to cookies. Parliament's civil liberties committee discussed the plans by the European Commission on 11 April. Marju Lauristin, the MEP responsible for steering the rules through Parliament, said that if companies providing communication services wanted to be trusted they needed to ensure confidentiality."*

**18.04.17**

**Digital Europe**

**DIGITALEUROPE publishes initial views on the draft ePrivacy Regulation**

The group Digital Europe has published a position paper on the EU Commissions proposals for ePrivacy regulations.

*"On 3 April, DIGITALEUROPE published its initial views on the European Commission's proposal for an ePrivacy Regulation ("ePR"). The position paper follows the January 2017 publication by the European Commission, which aims to update the current ePrivacy Directive and replace it with a more stringent and directly applicable Regulation."*

**18.04.17**

**Digital Europe**

**DIGITALEUROPE sends letter to Parliament on Privacy Shield Resolution**

Digital Europe has also sent a letter to the EU Parliament, encouraging them to vote against a proposed resolution on the EU-US Privacy Shield.

*"On 5 April, DIGITALEUROPE sent a letter to Members of the European Parliament ("MEPs") urging them to vote against the proposed resolution on the EU-US Privacy Shield, which was voted on the following day.*

Copyright © 2017 IEEE. All rights reserved.

*The draft resolution contained a number of damaging statements that could seriously disrupt cross-border commerce and harm European businesses if approved by a wide majority."*

Copyright © 2017 IEEE. All rights reserved.

# Diary Dates

**Building the European data economy – 10.01.17-26.04.17**

**ITU Council 2017 – 15.05.17 – 25.05.17**

Geneva, Switzerland

**Africa Internet Summit (AIS) 2017 – 29.05.17 – 02.06.17**

Nairobi, Kenya

**European Dialogue on Internet Governance – 06.06.17-07.06.17**

Tallinn, Estonia

**World Summit on the Information Society Forum (WSIS) 2017 – 12.06.17 – 16.06.17**

Geneva, Switzerland

**16th European Conference on Cyber Warfare and Security ECCWS – 29.06.17-30.06.17**

Dublin, Ireland

**ITU WTDC-17 – 09.10.17 – 20.10.17**

Buenos Aires, Argentina

**IGF 2017 – 18.12.17 – 21.10.17**

Geneva, Switzerland

Copyright © 2017 IEEE. All rights reserved.