
## 10 January 2018

# Synopsis

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

**India's** national **ID database** which contains approximately 1.2 billion citizens data, has been sold by **cybercriminals** to the **Indian Tribune** newspaper for a mere $8.

Amid **privacy** concerns over **Aadhaar**, the unique 12-digit identity number issued to all Indian residents, the **Unique Identification Authority of India** has created a virtual ID system in which a randomly generated 16-digit number will be used instead.

The **Singapore** University of Technology and Design have received a funding boost of $75 million from the Ministry of Education. New courses on **cybersecurity**, **data analytics** and **software design** will now be offered.

The technology giant **Intel** has disclosed details of two **security** vulnerabilities that could allow **hackers** to access information from virtually all devices containing chips produced in the last decade by Intel, **Advanced Micro Devices** (AMD) and **ARM Holdings**.

French President **Macron** has announced that he is introducing legislation to clamp down on **fake news** after a rise in **Russian propaganda**. The legislation should be completed by the end of 2018.

The **US** House of Representatives will vote to reauthorise section 702 of the **Foreign Intelligence Surveillance Act** on Thursday, which if passed will mandate **warrantless spying** on internet and phone networks. **Carnegie Endowment for International Peace**, a foreign-policy think tank have warned the United States to prepare for destructive **cyber-attacks** by **Iran** against US infrastructure and Government assets.

**Internet Association**, a US political lobbying body which represents **Google**, **Facebook** and several other tech giants, has joined the legal battle to block the **Federal Communications Commission's** appeal of **net neutrality**.

An **Iranian Government** backed **cyberespionage** group called **Infy** have cracked down on protesters by increasing their **cyber-attacks** not only on dissidents but anyone who is in contact with them abroad.

**Israel's** anti-trust regulator has announced that it will investigate large internet companies such as **Google** and **Facebook** to assess whether they are monopolising the **market** and stifling competition.

**The Kosciuszko Institute**, A **Polish** non-governmental research institute have predicted that the number of **cyber-attacks** on national infrastructure are likely to dramatically rise in 2018.

During a meeting with President **Borut Pahor** of **Slovenia**, **NATO** Secretary General **Jens Stoltenberg** urged for increased collaboration on issues such as **cybersecurity**.



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**

**10 January 2018**

## Table of Contents


**Synopsis** ..... 1

**Europe** ..... 4
- Internet governance ..... 4
- Cybersecurity ..... 5
- Privacy ..... 7
- Internet Inclusion ..... 8

**United States of America** ..... 9
- Internet governance ..... 9
- Cybersecurity ..... 11
- Privacy ..... 12
- Internet Inclusion ..... 15

**Pan-Asia** ..... 16
- Internet governance ..... 16
- Cybersecurity ..... 17
- Privacy ..... 19
- Internet Inclusion ..... 21

**Rest of the World** ..... 24
- Internet governance ..... 24
- Cybersecurity ..... 26
- Privacy ..... 27
- Internet Inclusion ..... 27

**Global Institutions** ..... 28

**Diary Dates** ..... 29

# Europe

## Internet governance

**04.01.18**

**Euractiv**

**Macron targets Russian fake news, moving ahead of Commission plans**

French President Macron announced last week that he is introducing legislation to clamp down on fake news after a rise in Russian propaganda. The legislation should be completed by the end of 2018.

*"French President Emmanuel Macron announced on Wednesday (3 January) that a law against fake news is in the making in France. The legislation is clearly aimed at Russian propaganda and should be completed by the end of 2018, government spokesman Benjamin Griveaux added on Thursday."*

*"The current hype behind fake news is linked to the fascination for illiberal powers, and it is most of the time financed by the same powers," Macron said."*

**09.01.18**

**Channel NewsAsia**

**Apple releases new update to fix 'Spectre' chip flaw**

Apple have released its latest security updates, Safari 11.0.2 and iOS 11.2.2 after security flaws were discovered in the microchips used by their devices.

*Apple Inc on Monday released an updated version of its operating system software to fix a major microchip security flaw that affected nearly all computer chips made in the last decade.*

*On its website, Apple explained that the latest security updates Safari 11.0.2 and iOS 11.2.2 both include security improvements to "mitigate the effects of Spectre".*

**10.01.18**

**Channel NewsAsia**

**Internet giants not doing enough to take down illegal content - EU**

Julian King, EU security commissioner has said that internet giants such as Google, YouTube and Twitter are not doing enough to remove illegal content off their websites.

*"Internet giants like Facebook, Google's YouTube and Twitter are not taking down illegal content from their websites fast enough, the European Union executive said on Tuesday after meeting with the companies."*

*"Several European governments have increased pressure on social media companies to do more to remove illegal content - from incitement to hatred and racism to extremist material to counterfeit products being sold online - and the companies have gone to greater efforts to detail the changes they are making."*

## Cybersecurity

**04.01.18**

**Nextgov**

**Iran's Cyberwar on Dissidents Could Infiltrate Your Mailbox**

An Iranian Government backed cyberespionage group called Infy have cracked down on protesters by increasing their cyber-attacks not only on dissidents but anyone who is in contact with them abroad.

*"Iran's crackdown on protesters could affect almost anyone in contact with them, thanks to a sophisticated internal police operation that routinely targets not only academics and dissidents but also those who have interacted with them — and even people only tangentially linked."*

*"Cybersecurity firms and prominent researchers of Iranian digital espionage efforts say one government-backed group in particular, Infy, will likely continue to increase its attacks even after the current unrest ends."*

**05.01.18**

**Computer Weekly**

**2018 could be year of critical infrastructure attacks, says report**

The Kosciuszko Institute, A Polish non-governmental research institute have predicted that the number of cyber-attacks on national infrastructure are likely to dramatically rise in 2018.

*"The coming year is likely to see an increase in the number of cyber-attacks on critical national infrastructure (CNI), according to a report based on experts' forecasts."*

*"While 2017 was a year of "electoral hacking" and an intense information war aimed at shaping the recipients' viewpoint, the latest cyber security report by The Kosciuszko Institute predicts that 2018 could be a year of cyber-attacks on critical infrastructure."*

**08.01.18**

**Computer Weekly**

**Sweden steps up cyber defence measures**

As part of Sweden's national security strategy, the country is shoring up their cyber resilience to ensure that potentially damaging attacks are dealt with effectively.

"Sweden is tightening up its cyber security defences as part of a wider national security strategy. The growing undercurrent of risk linked to the increase in cyber terrorism threats is changing both the character and direction of Sweden's national security policy and associated defence apparatus."

"In particular, Sweden's government and national security leaders are pursuing a more aggressive, capital-intensive programme to scale-up spending and strengthen the Nordic country's long-term capacity to defend itself against potentially damaging attacks from cyber terrorists and cybercrime organisations."

**09.01.18**

**NATO**

**NATO Secretary General discusses preparations for July Summit with President Pahor of Slovenia**

During a meeting with President Borut Pahor of Slovenia, NATO Secretary General Jens Stoltenberg urged for increased collaboration on issues such as cybersecurity.

*"NATO Secretary General Jens Stoltenberg welcomed President Borut Pahor of Slovenia to NATO Headquarters on Tuesday (9 January 2018) for discussions about the Alliance's adaptation and preparations for the NATO Summit in July. Mr. Stoltenberg thanked Slovenia for important contributions to NATO, including troops to the KFOR mission, contributions to the Alliance's mission in Afghanistan and to a NATO multinational battlegroup in Latvia."*

*"Mr. Stoltenberg also welcomed Slovenia's support for efforts to strengthen cooperation between NATO and the European Union."*

## Privacy

**04.01.18**

**The Independent**

**Intel chip flaw: Huge bug makes nearly any computer vulnerable to hacking**

The technology giant Intel has disclosed details of two security vulnerabilities that could allow hackers to access information from virtually all devices containing chips produced in the last decade by themselves, Advanced Micro Devices (AMD) and ARM Holdings.

*"Almost any computer could be vulnerable to a huge new computer bug."*

*"Researchers have found a flaw in the very core of computer chips that mean almost any recent device could be insecure and give up the sensitive information it is securing. The bug could affect everything from the phone in your pocket to the servers that help send it information."*

## Internet Inclusion

**03.01.18**

**Computer Weekly**

**Government yet to 'fully embrace' digital, says IoD report**

The Institute of Directors, a business organisation for entrepreneurs, business leaders and company directors have urged the UK Government to do more to open 'itself up to digital transformation.'

*"Institute of Directors report says the government's digital drive has lost momentum and calls on public sector to harness private sector technologies and innovation"*

*"The Institute of Directors (IoD) has called on the government focus on creating an environment for innovation rather than delivering specific technologies to take full advantage of digital transformation."*

**05.01.18**

**Computer Weekly**

**London attracted record tech investment in 2017**

According to research by the mayor of London agency, London & Partners, London technology firms received more venture capital than all of the major European cities combined in 2017.

*"London-based tech firms received record levels of venture capital funding last year. Tech firms in London received more venture capital funding in 2017 than all other major European cities combined, with the amount invested doubling since 2016."*

*"According to research by the mayor of London agency, London & Partners, £2.45bn in funds were invested in London-based firms in 2017, compared with £1.23bn in 2016. London accounted for 80% of investment in the UK."*

# United States of America

## Internet governance

**06.01.18**

**Gadgets Now**

**US net neutrality: Internet Association to join legal battle**

Internet Association, a US political lobbying body which represents Google, Facebook and several other tech giants, has joined the legal battle to block the Federal Communications Commission's appeal of net neutrality.

*"In a bid to block the repeal of net neutrality, the Internet Association, a US political lobbying body representing Google, Facebook and other tech giants, will join the legal battle to sue the Federal Communications Commission (FCC)."*

*"According to a report in The Hill late Friday, the Internet Association also reiterated its call for Congress to come up with a legislative replacement for the new FCC rules released by its Indian-origin Chairman Ajit Pai this week."*

**09.01.18**

**Reuters**

**Democrats vow to force vote on net neutrality**

U.S. Senate Democrats have said they will force a vote on net neutrality later this year which could overturn the Federal Communications Commission's decision to roll back net neutrality rules.

*"U.S. Senate Democrats said on Tuesday they will force a vote later this year on the U.S. Federal Communications Commission's reversal of landmark Obama administration net neutrality rules and will try to make it a key issue in the 2018 congressional elections."*

*"Senate Democratic Leader Chuck Schumer said the issue will be a major motivating factor for young voters the party is courting."*

**09.01.18**

**Channel NewsAsia**

**Apple releases new update to fix 'Spectre' chip flaw**

Apple have released its latest security updates, Safari 11.0.2 and iOS 11.2.2 after security flaws were discovered in the microchips used by their devices.

*Apple Inc on Monday released an updated version of its operating system software to fix a major microchip security flaw that affected nearly all computer chips made in the last decade.*

*On its website, Apple explained that the latest security updates Safari 11.0.2 and iOS 11.2.2 both include security improvements to "mitigate the effects of Spectre".*

**10.01.18**

**Channel NewsAsia**

**Internet giants not doing enough to take down illegal content - EU**

Julian King, EU security commissioner said internet giants such as Google, YouTube and Twitter are not doing enough to remove illegal content posted on their websites.

*"Internet giants like Facebook, Google's YouTube and Twitter are not taking down illegal content from their websites fast enough, the European Union executive said on Tuesday after meeting with the companies."*

*"Several European governments have increased pressure on social media companies to do more to remove illegal content - from incitement to hatred and racism to extremist material to counterfeit products being sold online - and the companies have gone to greater efforts to detail the changes they are making."*

## Cybersecurity

**04.01.18**

**Nextgov**

**Iran's Cyberwar on Dissidents Could Infiltrate Your Mailbox**

An Iranian Government backed cyberespionage group called Infy have cracked down on protesters by increasing their cyber-attacks not only on dissidents but anyone who is in contact with them abroad.

*"Iran's crackdown on protesters could affect almost anyone in contact with them, thanks to a sophisticated internal police operation that routinely targets not only academics and dissidents but also those who have interacted with them — and even people only tangentially linked."*

*"Cybersecurity firms and prominent researchers of Iranian digital espionage efforts say one government-backed group, Infy, will likely continue to increase its attacks even after the current unrest ends."*

**05.01.18**

**Computer Weekly**

**2018 could be year of critical infrastructure attacks, says report**

The Kosciuszko Institute, A Polish non-governmental research institute have predicted that the number of cyber-attacks on national infrastructure are likely to dramatically rise in 2018.

*"The coming year is likely to see an increase in the number of cyber-attacks on critical national infrastructure (CNI), according to a report based on experts' forecasts."*

*"While 2017 was a year of "electoral hacking" and an intense information war aimed at shaping the recipients' viewpoint, the latest cyber security report by The Kosciuszko Institute predicts that 2018 could be a year of cyber-attacks on critical infrastructure."*

**05.01.18**

**The Hill**

**Experts say US should expect more Iranian cyberattacks**

Carnegie Endowment for International Peace, a foreign-policy think tank have warned the United States to prepare for destructive cyber-attacks by Iran against US infrastructure and Government assets.

*"Experts say in new research that the United States should be prepared for Iran to target U.S. infrastructure, including economic and government assets, with destructive cyberattacks."*

*"In order to guard against such attacks, the U.S. government should increase the security of infrastructure and deepen cooperation with allies and nongovernmental organizations that have been targeted by Tehran's cyber operations, they argue in a new* report *from the Carnegie International Endowment for Peace."*

**09.01.18**

**Reuters**

**Intel to form new cybersecurity group amid chip flaw**

The technology giant Intel has created a new internal cybersecurity group after flaws in its microchips were discovered.

*"Intel Corp (INTC.O) will create a new internal cybersecurity group in the wake of recently disclosed flaws in its microchips, the Oregonian newspaper reported on Monday, citing a memo sent to company employees."*

*"The new group would be run by Intel human resources chief Leslie Culberstone who has worked in the chipmaker since 1979 and would be called, "Intel Product Assurance and Security."*

## Privacy

**04.01.18**

**The Independent**

**Intel chip flaw: Huge bug makes nearly any computer vulnerable to hacking**

The technology giant Intel has disclosed details of two security vulnerabilities that could allow hackers to access information from virtually all devices

containing chips produced in the last decade by themselves, Advanced Micro Devices (AMD) and ARM Holdings.

*"Almost any computer could be vulnerable to a huge new computer bug."*

*"Researchers have found a flaw in the very core of computer chips that mean almost any recent device could be insecure and give up the sensitive information it is securing. The bug could affect everything from the phone in your pocket to the servers that help send it information."*

**05.01.18**

**The Straits Times**

**Intel CEO Promises Fix for Serious Chip Security Flaw**

Brian Krzanich, CEO of technology giant Intel, has promised to fix the decade old security vulnerabilities found in their processors. The vulnerabilities, known as Meltdown and Spectre, have, between them, effected almost every device made in the last ten years.

*"Intel has big plans to steer toward new business in self-driving cars, virtual reality and other cutting-edge technologies.*

*"But first it has to pull out of a skid caused by a serious security flaw in its processor chips, which undergird many of the world's smartphones and personal computers."*

**05.01.18**

**Computer Weekly**

**Apple confirms all devices affected by Meltdown and Spectre**

Apple have released its latest security updates, Safari 11.0.2 and iOS 11.2.2 after security flaws were discovered in the microchips used by their devices.

*"Apple has confirmed that all iPhones, iPads and Mac computers are affected by the recently discovered microprocessor exploits as the financial services industry assesses the risk."*

*"Apple has released software updates for its* operating systems *after confirming that all its devices are affected by the microchip flaws dubbed Spectre and Meltdown."*

**08.01.18**

**SC Media**

**[ACLU says House surveillance bill increases likelihood of abuse]**

The American Civil Liberties Union have condemned the House Surveillance Bill, which attempts to reauthorise the spying on Americans without a warrant, on grounds that it increases the opportunity for abuse.

*"The text of a House bill that would reauthorize Section 702 released Friday immediately drew opposition from the American Civil Liberties Union (ACLU)."*

*"The bill would let federal agencies, including the FBI, the broad authority to sift without a warrant through data gather under Section 702 for information about Americans, prior to opening an active investigation."*

**08.01.18**

**The Hill**

**[Cryptocurrency being routed to North Korean university: report]**

AlienVault, a US based cybersecurity firm, has discovered malware being used to mine Monero cryptocurrency. The malware, according to the firm, transfers the mined Monero to a university in North Korea.

*"A U.S.-based cybersecurity firm has uncovered malware apparently being used to mine the Monero cryptocurrency and send it to a university in North Korea."*

*"Cyber firm AlienVault released an* analysis *of the malware on Monday, saying that it installs software on victim computers that instructs them to perform complex computational tasks to "mine" Monero. The mined currency is then sent to a server located at Kim Il Sung University in Pyongyang. "*

**10.01.18**

**The New York Times**

**[Surveillance and Privacy Debate Reaches Pivotal Moment in Congress]**

The US House of Representatives will vote to reauthorise section 702 of the Foreign Intelligence Surveillance Act on Thursday, which if passed will mandate warrantless spying on internet and phone networks.

*"A yearslong debate over National Security Agency surveillance and protections for Americans' privacy rights will reach a climactic moment on Thursday as the House of Representatives takes up legislation to extend a program of*

*warrantless spying on internet and phone networks that traces back to the Sept. 11 attacks."*

*"There is little doubt that Congress will extend an expiring statute, known as Section 702 of the FISA Amendments Act, that permits the government to collect without a warrant from American firms, like Google and AT&T, the emails and other communications of foreigners abroad — even when they are talking to Americans."*

## Internet Inclusion

***No new items of relevance***

# Pan-Asia

## Internet governance

**09.01.18**

**Channel NewsAsia**

**Apple releases new update to fix 'Spectre' chip flaw**

Apple have released its latest security updates, Safari 11.0.2 and iOS 11.2.2 after security flaws were discovered in the microchips used by their devices.

*Apple Inc on Monday released an updated version of its operating system software to fix a major microchip security flaw that affected nearly all computer chips made in the last decade.*

*On its website, Apple explained that the latest security updates Safari 11.0.2 and iOS 11.2.2 both include security improvements to "mitigate the effects of Spectre".*

**10.01.18**

**The Economic Times**

**UIDAI introduces new two-layer security system to improve Aadhaar privacy**

Amid privacy concerns over Aadhaar, the unique 12-digit identity number issued to all Indian residents, the Unique Identification Authority of India has created a virtual ID system in which a randomly generated 16-digit number will be used instead.

*"Days after newspaper report claimed breach in the Aadhaar database, the Unique Identification Authority of India (UIDAI) today released a 2-layer safety net -- creating a Virtual ID and limiting Know Your Customer (KYC) - for the 12-digit biometric code."*

*"The two moves will cover Aadhaar users from any breach. The two moves will cover Aadhaar users from any breach. Virtual ID will end any need to share your Aadhaar number at the time of authentication. This will be a 16-digit, randomly-generated number, which will be used for authentication instead of your Aadhaar number."*

**10.01.18**

**The Straits Times**

**Parliament: Proposal to appoint select committee to examine 'online falsehoods'**

Minister K. Shanmugam, Home Affairs and Law Minister has warned that Singapore is “highly susceptible” to fake news and has urged that a Select Committee be established to examine ‘online falsehoods.’

*“Singapore is "highly susceptible" to the threat of fake news, warned Home Affairs and Law Minister K. Shanmugam on Wednesday (Jan 10), in moving a motion to appoint a select committee to study the issue.”*

*“The 10-MP committee will examine the causes and consequences of deliberate online falsehoods, said Mr. Shanmugam. It may also call for public feedback, and is to consult "as widely as possible", he added.”*

## Cybersecurity

**04.01.18**

**Nextgov**

**Iran’s Cyberwar on Dissidents Could Infiltrate Your Mailbox**

An Iranian Government backed cyberespionage group called Infy have cracked down on protesters by increasing their cyber-attacks not only on dissidents but anyone who is in contact with them abroad.

*“Iran’s crackdown on protesters could affect almost anyone in contact with them, thanks to a sophisticated internal police operation that routinely targets not only academics and dissidents but also those who have interacted with them — and even people only tangentially linked.”*

*“Cybersecurity firms and prominent researchers of Iranian digital espionage efforts say one government-backed group in particular, Infy, will likely continue to increase its attacks even after the current unrest ends.”*

**05.01.18**

**Gadgets Now**

**Cyber crimes rose between 2014 and 2017: Government**

The Indian Government announced that cyber-crimes rose significantly between 2014 and 2017. The number rose from 9,622 and 11,592 to 12,317 during 2014, 2015 and 2016 respectively.

*"Cyber crimes cases registered in the country have grown in the last three years, with the number rising from 9,622 and 11,592 to 12,317 during 2014, 2015 and 2016 respectively, the government said today."*

*"During the Question Hour in Rajya Sabha, members expressed concern over the safety of digital transactions, to which the Minister of Electronics and Information Technology Ravi Shankar Prasad said that the government was alert to the challenges."*

**05.01.18**

**SC Media**

**India's 1.2 billion citizen national database reportedly breached**

India's national ID database which contains approximately 1.2 billion citizens data, was sold by cybercriminals to the Indian Tribune newspaper for a mere $8.

*"India's national ID database containing the information of nearly 1.2 billion people was breached with cybercriminals selling access to the information for $8, though officials deny the extent of the incident."*

*"On Jan. 3, 2018, The Indian Tribune claimed to have purchased access to the stolen information containing the names, addresses, dates of birth, mobile numbers, all ten fingerprints, and iris scans of the country's citizens. India started collecting the information into a centralized government database called Aadhaar to create a voluntary identity system in 2010."*

**05.01.18**

**Computer Weekly**

**2018 could be year of critical infrastructure attacks, says report**

The Kosciuszko Institute, A Polish non-governmental research institute have predicted that the number of cyber-attacks on national infrastructure are likely to dramatically rise in 2018.

*"The coming year is likely to see an increase in the number of cyber-attacks on critical national infrastructure (CNI), according to a report based on experts' forecasts."*

*"While 2017 was a year of "electoral hacking" and an intense information war aimed at shaping the recipients' viewpoint, the latest cyber security report by The Kosciuszko Institute predicts that 2018 could be a year of cyber-attacks on critical infrastructure."*

**09.01.18**

**Gadgets Now**

**Give cyber security top priority: PM at cops meet**

The Prime Minister of India, Narendra Modi has told police forces across the country that cybersecurity must be a top priority, in particular dealing with online radicalisation.

*"PM Narendra Modi told police heads from across the country on Monday to deal with issues relating to cyber security on an immediate and priority basis. Particularly mentioning online radicalisation by terrorist outfits, he urged for appropriate use of technology to pinpoint problem areas for timely redressal."*

*"Delivering the valedictory address on concluding day of the three-day DGPs/IGPs conference, Modi suggested counter campaigns on social media should rely on local languages for greater effectiveness."*

## Privacy

**04.01.18**

**The Independent**

**Intel chip flaw: Huge bug makes nearly any computer vulnerable to hacking**

The technology giant Intel has disclosed details of two security vulnerabilities that could allow hackers to access information from virtually all devices containing chips produced in the last decade by themselves, Advanced Micro Devices (AMD) and ARM Holdings.

*"Almost any computer could be vulnerable to a huge new computer bug."*

*"Researchers have found a flaw in the very core of computer chips that mean almost any recent device could be insecure and give up the sensitive information it is securing. The bug could affect everything from the phone in your pocket to the servers that help send it information."*

**05.01.18**

**The Straits Times**

**Critical flaws put nearly all devices at risk**

Singapore's Computer Emergency Response Team have urged users to download security fixes immediately to mitigate the risks posed by devices containing Intel chips, Advanced Micro Devices (AMD) and ARM processors.

*"Critical hardware flaws revealed this week are putting billions of computers and smartphones at security risk, and Singapore's cyber security authority has urged all users to apply available security software fixes immediately."*

*"Issuing the alert yesterday, the Singapore Computer Emergency Response Team (Singer) said: "The vulnerabilities enable attackers to steal any data processed by the computer."*

**08.01.18**

**The Hill**

**Cryptocurrency being routed to North Korean university: report**

AlienVault, a US based cybersecurity firm, has discovered malware being used to mine Monero cryptocurrency. The malware, according to the firm, transfers the mined Monero to a university in North Korea.

*"A U.S.-based cybersecurity firm has uncovered malware apparently being used to mine the Monero cryptocurrency and send it to a university in North Korea."*

*"Cyber firm AlienVault released an* analysis *of the malware on Monday, saying that it installs software on victim computers that instructs them to perform complex computational tasks to "mine" Monero. The mined currency is then sent to a server located at Kim Il Sung University in Pyongyang. "*

**08.01.18**

**The Straits Times**

**Parliament: New laws on data sharing between public sector agencies**

The Singapore Parliament have passed new data sharing laws which mandate that public-sector officers who share personal data of Singaporeans without consent will face fines of up to fines of up to $5,000 or jail time.

*"Public sector officers who share the personal data of Singaporeans without authorization can now be fined up to $5,000, jailed for up to two years, or both."*

*"The same applies to those who make use of data to benefit themselves or re-identify anonymised data without authorisation."*

## Internet Inclusion

**05.01.18**

**Computer Weekly**

**Plugging Singapore's cyber security skills gap**

Twenty teams of cybersecurity professionals competed against one another in a competition that aimed to reduce the skills gap in Singapore.

*"Some 20 teams of cyber security industry professionals and tertiary students in Singapore pitted their skills against one another in a competition aimed at plugging the cyber security skills gap in the city-state."*

*Conducted in December 2017, the Ixia Cyber Combat competition saw "participants from industries including financial services, technology, government and education take down enemy servers, expose vulnerabilities and win flags, while defending their home ground against enemy attacks."*

**05.01.18**

**The Straits Times**

**Indonesia's new cybersecurity agency looks to recruit staff of hundreds**

Djoko Setiadi, the head of the National Cyber and Encryption Agency has announced that the they are recruiting hundreds of people with cyber skills, including graduates.

*"Indonesia's recently established cyber security agency will recruit hundreds of personnel in the coming months, its chief said on Friday (Jan 5)."*

*"The agency has been set up amid rising concern over online misinformation and hoaxes ahead of simultaneous local elections set to take place across the country later this year."*

**06.01.18**

**Gadgets Now**

**Public Wi-Fi hotspots set up at 204 rural BSNL Exchanges in J&K**

In a push to get rural areas digitalised, Public Wi-Fi hotspots have been set up at 204 rural BSNL broadband service exchanges in 21 districts in Jammu and Kashmir.

*“In a major push to digitisation in the rural areas of Jammu and Kashmir, public Wi-Fi hotspots were set up at 204 rural BSNLexchanges in 21 districts.”*

*"To give impetus to telecom services in rural and remote areas with development of Wi-Fi infrastructure, the Department of Telecommunications through USOF has set up public Wi-Fi hotspots in 204 rural BSNL telephone exchanges of various districts," an official spokesman said.”*

**08.01.18**

**Gadgets Now**

**Indian Railways to equip all 8,500 stations with Wi-Fi**

As part of the Indian Government’s Digital India Initiative, 8,500 railway stations have been equipped with Wi-Fi facilities.

*“All railway stations -- nearly 8,500 across the country, including those in rural and remote areas -- will be equipped with Wi-Fi facilities at an estimated cost of Rs 700 crore ($110 million).”*

*“As part of the government's ambitious Digital India initiative, the national transporter has currently commissioned Wi-Fi services at 216 major stations enabling about seven million rail passengers to log on to the free Internet facility.”*

**08.01.18**

**Gadgets Now**

**Skilling enterprises, start-up developers key to India's digital dream: IBM**

Technology company IBM have collaborated with Telecom Sector Skill Council to give students in India the opportunity to get skilled in Big Data, Cloud Computing, IoT and mobile applications.

*“With digital transformation comes the daunting task of preparing a workforce for technologies like Big Data, Cloud, Artificial Intelligence (AI) and Internet of*

*Things (IoT) that can address the massive demand coming from governments and businesses in India."*

*"According to a top IBM executive, the time is ripe to start the journey right from schools and universities, leading to up-skilling and re-skilling the enterprise and start-up developers' community in the country."*

**10.01.18**

**The Straits Times**

**SUTD to receive up to $75 million from MOE, and opens an adult education academy**

The Singapore University of Technology and Design have received a funding boost of $75 million from the Ministry of Education. New courses on cybersecurity, data analytics and software design will now be offered.

*"Singapore's fourth autonomous university will get a funding boost of up to $75 million from the Ministry of Education (MOE)."*

*"The Singapore University of Technology and Design (SUTD) also launched adult learning initiative SUTD Academy on Wednesday (Jan 10). In the pipeline is a micro-master's programme, a certification which is the first of its kind here, according to SUTD's acting president and provost Professor Chong Tow Chong."*

# Rest of the World

## Internet governance

**04.01.18**

**Euractiv**

**Macron targets Russian fake news, moving ahead of Commission plans**

French President Macron announced last week that he is introducing legislation to clamp down on fake news after a rise in Russian propaganda. The legislation should be completed by the end of 2018.

*"French President Emmanuel Macron announced on Wednesday (3 January) that a law against fake news is in the making in France. The legislation is clearly aimed at Russian propaganda and should be completed by the end of 2018, government spokesman Benjamin Griveaux added on Thursday."*

*"The current hype behind fake news is linked to the fascination for illiberal powers, and it is most of the time financed by the same powers," Macron said."*

**06.01.18**

**Gadgets Now**

**Iran ministers criticised for not blocking internet: Judiciary**

The head of Iran's Cybercrime Committee has threatened ministers with punishment for failing to censor all channels on the messaging app, Telegram.

*"Iranian ministers should be punished if they deliberately failed to censor online content by "trouble-makers and enemies", said the head of the country's cybercrime committee on Friday."*

*"The order to block all channels on encrypted messaging service Telegram, that in recent days incited the population to violence and trouble, was transmitted by judicial officials to the telecoms ministry a long time ago, but unfortunately nothing was done," said Abdolsamad Khoramabadi, according to local media."*

**08.01.18**

**Gadgets Now**

**[Israel's anti-trust regulator to look at internet giants]**

Israel's anti-trust regulator has announced that it will investigate large internet companies such as Google and Facebook to assess whether they are monopolising the market and stifling competition.

*"Israel's anti-trust regulator said it will look at the business practices of internet giants such as Facebook and Google to make sure they are not stifling competition."*

*"We will look closely at the activity of the internet giants to see whether they are abusing their power and breaching the Anti-Trust Authority's rules," the head of the authority, Michal Halperin, told parliament's Economic Affairs Committee."*

**09.01.18**

**Channel NewsAsia**

**[Apple releases new update to fix 'Spectre' chip flaw]**

Apple have released its latest security updates, Safari 11.0.2 and iOS 11.2.2 after security flaws were discovered in the microchips used by their devices.

*Apple Inc on Monday released an updated version of its operating system software to fix a major microchip security flaw that affected nearly all computer chips made in the last decade.*

*On its website, Apple explained that the latest security updates Safari 11.0.2 and iOS 11.2.2 both include security improvements to "mitigate the effects of Spectre".*

**10.01.18**

**BBC News**

**[Why ordinary Iranians are turning to internet backdoors to beat censorship]**

The rise in internet censorship in Iran, has led to several young people downloading proxies and virtual private networks (VPNs) to bypass the internet blocks.

*“Social media in Iran is carefully controlled, but its usefulness - including in organising protests - leads many ordinary Iranians to see out ways around the censors.”*

*“Most young people in Iran already knew how to bypass internet blocks by using proxies and virtual private networks (VPNs). As a result of recent protests in the country, restrictions became tighter - some social networks were temporarily banned.”*

## Cybersecurity

**04.01.18**

**Nextgov**

**Iran’s Cyberwar on Dissidents Could Infiltrate Your Mailbox**

An Iranian Government backed cyberespionage group called Infy have cracked down on protesters by increasing their cyber-attacks not only on dissidents but anyone who is in contact with them abroad.

*“Iran’s crackdown on protesters could affect almost anyone in contact with them, thanks to a sophisticated internal police operation that routinely targets not only academics and dissidents but also those who have interacted with them — and even people only tangentially linked.”*

*“Cybersecurity firms and prominent researchers of Iranian digital espionage efforts say one government-backed group in particular, Infy, will likely continue to increase its attacks even after the current unrest ends.”*

**05.01.18**

**The Hill**

**Experts say US should expect more Iranian cyberattacks**

Carnegie Endowment for International Peace, a foreign-policy think tank have warned the United States to prepare for destructive cyber-attacks by Iran against US infrastructure and Government assets.

*“Experts say in new research that the United States should be prepared for Iran to target U.S. infrastructure, including economic and government assets, with destructive cyberattacks.”*

*“In order to guard against such attacks, the U.S. government should increase the security of infrastructure and deepen cooperation with allies and nongovernmental organizations that have been targeted by Tehran’s cyber*

*operations, they argue in a new* report *from the Carnegie International Endowment for Peace."*

**05.01.18**

**Computer Weekly**

**2018 could be year of critical infrastructure attacks, says report**

The Kosciuszko Institute, A Polish non-governmental research institute have predicted that the number of cyber-attacks on national infrastructure are likely to dramatically rise in 2018.

*"The coming year is likely to see an increase in the number of cyber-attacks on critical national infrastructure (CNI), according to a report based on experts' forecasts."*

*"While 2017 was a year of "electoral hacking" and an intense information war aimed at shaping the recipients' viewpoint, the latest cyber security report by The Kosciuszko Institute predicts that 2018 could be a year of cyber-attacks on critical infrastructure."*

## Privacy

**04.01.18**

**The Independent**

**Intel chip flaw: Huge bug makes nearly any computer vulnerable to hacking**

The technology giant Intel has disclosed details of two security vulnerabilities that could allow hackers to access information from virtually all devices containing chips produced in the last decade by themselves, Advanced Micro Devices (AMD) and ARM Holdings.

*"Almost any computer could be vulnerable to a huge new computer bug."*

*"Researchers have found a flaw in the very core of computer chips that mean almost any recent device could be insecure and give up the sensitive information."*

## Internet Inclusion

***No new items of relevance***

# Global Institutions

**09.01.18**

**NATO**

**NATO Secretary General discusses preparations for July Summit with President Pahor of Slovenia**

During a meeting with President Borut Pahor of Slovenia, NATO Secretary General Jens Stoltenberg urged for increased collaboration on issues such as cybersecurity.

*"NATO Secretary General Jens Stoltenberg welcomed President Borut Pahor of Slovenia to NATO Headquarters on Tuesday (9 January 2018) for discussions about the Alliance's adaptation and preparations for the NATO Summit in July. Mr. Stoltenberg thanked Slovenia for important contributions to NATO, including troops to the KFOR mission, contributions to the Alliance's mission in Afghanistan and to a NATO multinational battlegroup in Latvia."*

*"Mr. Stoltenberg also welcomed Slovenia's support for efforts to strengthen cooperation between NATO and the European Union."*

# Diary Dates

**GDPR Summit – 30.01.18**

London, England

**Manusec Europe – 07.02.18-08.02.18**

Munich, Germany

**Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18**

Ottawa, Canada

**RSA – 16.04.18–20.04.18**

San Francisco, USA

**Africa Internet Summit – 29.04.18-11.05.18**

Dakar, Senegal