**16 August 2017**

## Synopsis

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

The former head of the **UK's** MI5 **espionage** agency has stated that the Government's plans to increase law enforcement access to **encrypted messaging** services would do greater damage to the UK's economy and wider interests.

**Google** have published a new website detailing how the internet giant will seek to comply with the **EU's** General **Data Protection** Regulations when they are introduced next year.

Results from the **US** Air Force's **bug bounty** program has found a total of 207 vulnerabilities, with the top researcher, aged 17, finding 30 valid issues.

The **Federal Trade Commission** has ordered **Uber** to undergo **data privacy audits** for the next two decades as part of a settlement deal for a major data breach in 2014.

The **FCC** has extended its consultation on its plans to repeal **net neutrality** rules implemented during the Obama administration.

**China** has launched probes into its three biggest domestic internet companies over concerns that they have not done enough to adhere to the government's strict **internet rules**. Internet retailer **Alibaba** has been separately warned to desist from selling equipment that allows users to bypass China's Great Firewall.

**Indonesia** and **Singapore** have announced that following successful talks the countries have agreed to exchange **cybersecurity** knowledge and intelligence.

**India's** telecommunications regulator **TRAI** has announced that the body's final recommendations for **net neutrality** policy will likely be announced in September, following a detailed discussions workshop in Delhi later this month.

Following the conclusion of last week's election in **Kenya**, National Super Alliance candidate **Raila Odinga** has suggested that the country's electoral commission may have suffered a **cyberattack**, impacting the final result.

The **Colombian** Government has suggested that it could shortly classify the **US** as a safe destination for **data transfer**, potentially providing a significant boost to e-commerce between the two countries.

**ICANN** have issued a new RFP for information system **auditors** to support existing commitments outlined in contracts between ICANN and its affiliate bodies like the **PTI**.

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

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

2

**IEEE Global Internet Policy Monitor**

**16 August 2017**

## Table of Contents

# Europe

## Internet governance

*No new items of relevance*

## Cybersecurity

**11.08.17**

**SC Media**

### SMEs ahead of larger orgs in IoT security, study

A new study by Pwnie Express has found that small and medium sized enterprises are better prepared to deal with the cybersecurity threats posed by IoT devices.

*"When it comes to Internet of Things (IoT) security, size really does matter, though bigger isn't necessarily better – as it turns out small and medium sized enterprises (SMEs) are better prepared to handle the threats posed by IoT.*

*SMEs may not have the resources of their larger peers but they're training them on identifying threats and determining the potential dangers connected devices pose, according to a study of 950 professionals conducted by Pwnie Express."*

**11.08.17**

**Computing**

### Weakening encryption would damage the UK's wider interests says former MI5 chief

The former head of the UK's MI5 espionage agency has stated that the Government's plans to increase law enforcement access to encrypted messaging services would do greater damage to the UK's economy and wider interests.

*"Encryption is "very positive" in the context of the UK's commercial and national security interests and it would be a mistake to weaken it, according to Jonathan Evans, who was head of MI5 until 2013.*

*In an interview with [BBC Radio 4](#), Evans acknowledged that the increasing use of encryption had made the job of the police and authorities more difficult, but he suggested that calls for it to be weakened, such as those made repeatedly by [home secretary Amber Rudd](#), are misguided."*

**16.08.17**

**Computer Weekly**

[**Hackers hit Holyrood with Westminster-style brute-force attack**](#)

The Scottish Parliament has been subjected to a major cyberattack, similar in nature to the cyberattack to the Westminster Parliament earlier this year.

*"Cyber attackers have reportedly tried to steal the email credentials of Scottish MPs in a [brute-force](#) attack just over seven weeks after a [similar 12-hour assault aimed at Westminster MPs](#)."*

## Privacy

**15.08.17**

**Bloomberg BNA**

[**Google details its preparations for upcoming EU privacy regime change**](#)

Google have published a new website detailing how the internet giant will seek to comply with the EU's General Data Protection Regulations when they are introduced next year.

*"With a little more than nine months left until the effective date of a new European Union privacy regime, Alphabet Inc.'s Google has launched a website setting out how the search engine and internet giant intends to comply. The site is intended to help businesses understand their options for ensuring they are ready for new stricter customer consent rules, mandatory data breach notice, and the potential for massive fines of up to the greater of 20 million euros ($25.5 million) or 4 percent of a company's worldwide income."*

## Internet Inclusion

***No new items of relevance***

# United States of America

## Internet governance

*No new items of relevance*

## Cybersecurity

**10.08.17**

**Reuters**

**[Defense Secretary Mattis sees growth for Silicon Valley defense unit](#)**

Jim Mattis, the US Defence Secretary has stated his interest in further developing the DoD's Defence Innovation Experimental Unit based in Silicon Valley, to further improve the US reaction to complex technological challenges.

*"U.S. Defense Secretary Jim Mattis said on Thursday an Obama-era experimental defense outpost in Silicon Valley would grow in importance under the Trump administration and that the nation's technology entrepreneurs were vital to national defense.*

*Mattis paid his first official visit to the Pentagon's Defense Innovation Experimental Unit, or DIUx, in Mountain View, California, as part of a two-day outreach tour to the U.S. technology industry intended to highlight the Pentagon's commitment to technology innovation."*

**10.08.17**

**SC Media**

**[USAF bug bounty program finds 207 vulnerabilities](#)**

Results from the US Air Force's bug bounty program has found a total of 207 vulnerabilities, with the top researcher, aged 17, finding 30 valid issues.

*"The U.S. Air Force's first bug bounty program ended in June with bug hunters finding 207 vulnerabilities and receiving $133,400.*

*The Hack the Air Force program, operated by HackerOne, began on May 30 and ran through June 23 with 272 hackers taking part, HackerOne reported. The hackers only looked at several of the Air Force's public facing websites."*

**11.08.17**

**Computing**

## [WikiLeaks unveils CIA tool for capturing video from IoT cameras](#)

WikiLeaks have revealed further cyberespionage tools alleged to have originated with the CIA. The latest tool named CouchPotato allows users to capture the video cameras of IoT devices.

*"WikiLeaks continues to add to its growing trove of alleged CIA documents, known as [Vault 7](#), with a user guide for a programme called [CouchPotato](#), which is designed to capture video from IoT cameras.*

*Critics of WikiLeaks have said that the documents posted to Vault 7 are several years out of date, but this document is relatively recent: it dates back to February 2014."*

**11.08.17**

**SC Media**

## [SMEs ahead of larger orgs in IoT security, study](#)

A new study by Pwnie Express has found that small and medium sized enterprises are better prepared to deal with the cybersecurity threats posed by IoT devices.

*"When it comes to Internet of Things (IoT) security, size really does matter, though bigger isn't necessarily better – as it turns out small and medium sized enterprises (SMEs) are better prepared to handle the threats posed by IoT.*

*SMEs may not have the resources of their larger peers but they're training them on identifying threats and determining the potential dangers connected devices pose, according to a [study](#) of 950 professionals conducted by Pwnie Express."*

**14.08.17**

**The Hill**

[State Department quietly establishes new cybersecurity office](#)

A new unit has been established in the State Department's Diplomatic Security Service to provide cybersecurity protections for the US diplomatic corp.

*"The State Department quietly established a new office earlier this year within its Diplomatic Security Service to safeguard against and respond to cybersecurity threats.*

*The State Department officially launched the new office, called the Cyber and Technology Security (CTS) directorate, on May 28, a department official confirmed. The establishment of the directorate was first* reported by *Federal News Radio last week."*


**16.08.17**

**NextGov**

[Election Commission wants to work with DHS on election cybersecurity](#)

The Election AssistanceCommission has begun work with States and Local election officials to help focus the support provided by the Department of Homeland Security.

*"The Homeland Security Department made a unilateral move to raise its involvement in the cybersecurity of U.S. election infrastructure last year, but a commission that helps state and local election commissioners wants to turn DHS' decision to its advantage.*

*The Election Assistance Commission's plan is to query state and local election officials about what help from DHS would be most useful and to urge DHS to focus in those areas, Executive Director Brian Newby told commissioners Wednesday."*

## Privacy

**11.08.17**

**Bloomberg BNA**

[Colombia May Designate U.S. as Data-Transfer-Safe Destination](#)

The Colombian Government has suggested that it could shortly classify the US as a safe destination for data transfer, potentially providing a significant boost to e-commerce between the two countries.

*"Colombian business interests are reacting favorably to a government [proposal](#) to make data transfers to the U.S. easier by finding its privacy laws adequate to protect personal data, privacy attorneys tell Bloomberg BNA.*

*The draft amendments to Colombia's privacy rules aim for a more market-friendly approach that could ease the flow of low-level personal data to other nations and help attract investment, particularly by U.S. companies. Allowing U.S.-based multinationals to more easily move information in the global digital economy would make Colombia a stronger prospect for business investment, attorneys said."*

**15.08.17**

**Ars Technica**

[Feds demand 1.3 million IP addresses of those who visited Trump protest site](#)

The Justice Department has requested that IP addresses relating to a website that orchestrated protests on the day of Donald Trump's inauguration be turned over. The warrant for 1.3million IP addresses has however been challenged by DreamHost, the web host of the [disruptj20.org](#) website in question.

*"The Justice Department is seeking the 1.3 million IP addresses that visited a Trump resistance site. The search warrant is part of an investigation into Inauguration Day rioting, which has already resulted in the [indictment of 200 people](#) in the District of Columbia. DreamHost, the Web host of the [disruptj20.org](#) site that helped organize the January 20 protests, is challenging the warrant it was served as being an "unfocused search" and declared that it was a "clear abuse of government authority."*

**15.08.17**

**SC Media**

## [Uber FTC settlement requires 20 years of privacy audits following 2014 breach](#)

The Federal Trade Commission has ordered Uber to undergo data privacy audits for the next two decades as part of a settlement deal for a major data breach in 2014.

*"[Uber](#) has agreed to the Federal Trade Commission ([FTC](#)) that it will undergo 20 years of privacy audits after the consumer protection agency said the ride-sharing service "failed consumers."*

*The settlement stems from the May 2014 data breach which allowed an intruder to compromised more than 100,000 names and driver's license numbers that Uber stored in a datastore operated by Amazon Web Services, according to an Aug. 8, FTC press [release](#)."*

## Internet Inclusion

**11.08.17**

**Ars Technica**

## [FCC faces backlash for saying Americans might not need fast home Internet](#)

As part of the Federal Communications Commission (FCC) annual analysis of broadband deployment, US internet users have filed a high number of objections to the FCC's implication that mobile data could be used as a substitute for cable and fibre broadband.

*"American Internet users are telling the Federal Communications Commission that mobile broadband is not a full replacement for fast home Internet service. This week, the FCC kicked off its annual analysis of broadband deployment and signaled that it might [determine that smartphone access is a proper substitute for cable or fiber Internet](#). In doing so, the FCC could conclude that broadband is already being deployed to all Americans in a reasonable and timely fashion, and thus the commission could take fewer steps to promote deployment and competition."*

**11.08.17**

**The Hill**

**[FCC extends deadline for net neutrality comments](#)**

The FCC has extended its consultation on its plans to repeal net neutrality rules implemented during the Obama administration.

*"The Federal Communications Commission (FCC) on Friday agreed to extend a deadline for submitting comments on its proposal to repeal Obama-era net neutrality rules.*

*The deadline for responding to the first round of public comments, which closed last month, has been [extended](#) from Aug. 16 to Aug. 30."*

# Pan-Asia

## Internet governance

**10.08.17**

**CNBC**

[China's three internet giants being investigated for content that 'endangers national security'](#)

China has launched probes into its three biggest domestic internet companies over concerns that they have not done enough to adhere to the government's strict internet rules.

*"[Chinese](#) internet giants [Tencent](#), [Baidu](#) and [Sina Weibo](#) are under investigation for cyber-security violations, the mainland's office for cyberspace administration said on Friday.*

*An English translation of a notice on the office's website said the social media platforms of the three companies — WeChat, Tieba and Weibo respectively — have users spreading "violence and terror, false rumors, obscene pornography and other content that endangers national security, public safety and social order."*

## Cybersecurity

**11.08.17**

**SC Media**

[SMEs ahead of larger orgs in IoT security, study](#)

A new study by Pwnie Express has found that small and medium sized enterprises are better prepared to deal with the cybersecurity threats posed by IoT devices.

*"When it comes to Internet of Things (IoT) security, size really does matter, though bigger isn't necessarily better – as it turns out small and medium sized enterprises (SMEs) are better prepared to handle the threats posed by IoT.*

*SMEs may not have the resources of their larger peers but they're training them on identifying threats and determining the potential dangers connected devices pose, according to a [study](#) of 950 professionals conducted by Pwnie Express."*

**12.08.17**

**Tempo Magazine (Indonesia)**

[Indonesia, Singapore to Exchange Knowledge on Cyber Security](#)

Indonesia and Singapore have announced that following successful talks the countries have agreed to exchange cybersecurity knowledge and intelligence.

*"The Indonesian and Singaporean government will share knowledge on the development of cyber world activities. It is aimed at strengthening cyber security of both countries.*

*"Both countries have maintained a good relationship. One of the ways to maintain the relationship is by providing thorough and extensive information on measures to fight against terrorism and cyber-related problems," Coordinating Political, Legal, and Security Affairs Minister Wiranto said after meeting Singapore Deputy Prime Minister Teo Chee Hean in Jakarta on Friday, August 11."*

## Privacy

**11.08.17**

**The Economic Times**

[TRAI defends data privacy paper; says consumer interest vital](#)

R. S. Sharma, head of India's telecommunications regulator TRAI has defended the organisation's decision to issue a discussion paper on data privacy, highlighting the importance of protecting consumers.

*"Defending the move of issuing a discussion paper on data privacy and ownership, TRAI chief R S Sharma has said the regulator raised the "right questions" to protect the legitimate interest of telecom consumers, and is mandated to do so.*

*Brushing off the criticism, the TRAI chief sought to allay industry's fears on overregulation and jurisdiction, saying people should not presume the outcome or "cry foul" at this stage when the consultation has just about started."*

# Internet Inclusion

**14.08.17**

**Indian Television**

[TRAI's final recommendations on net neutrality likely by September](#)

India's telecommunications regulator TRAI has announced that the body's final recommendations for net neutrality policy will likely be announced in September, following a detailed discussions workshop in Delhi later this month.

*"India's telecoms and broadcast regulator Telecom Regulatory Authority of India (TRAI) is expected to come out with its final recommendations on net neutrality next month.*

*TRAI chairman R S Sharma told indiantelevision.com that after detailed discussions were held in Bengluru last month on the consultation paper on Net Neutrality (NN) issued mid-2016, a similar round has been fixed for 30 August 2017 in Delhi after which TRAI will begin work on its final recommendations to ensure national security and customer privacy."*

**16.08.17**

**Bloomberg**

[Chinese Watchdog Warns Alibaba on Sale of Web Access Tools](#)

Internet retailer Alibaba has been warned to desist from selling equipment that allows users to bypass China's Great Firewall.

*"China's top cyberspace regulators have warned [Alibaba Group Holding Ltd.](#) and other online services against carrying illicit content, substances and tools to help users circumvent the nation's internet content barriers.*

*The Cyberspace Administration of China on Thursday singled out five services, including Alibaba's Taobao internet bazaar, for criticism and ordered them to rectify their problems immediately. Responding to reports from users, it discovered "controlled substances" as well as illegal virtual private network tools -- used to access foreign websites -- for sale on Taobao, the regulator's Zhejiang branch said in a [post](#) on its WeChat account."*

# Rest of the World

## Internet governance

*No new items of relevance*

## Cybersecurity

**10.08.17**

**IT Web Africa**

### [Hacking claims cloud Kenya's elections](#)

Following the conclusion of last week's election in Kenya, National Super Alliance candidate Raila Odinga has suggested that the country's electoral commission may have suffered a cyberattack, impacting the final result.

*"From Kenya, hours after the election results started streaming in, National Super Alliance (NASA) presidential candidate Raila Odinga suggested the IEBC (Independent Electoral and Boundaries Commission) result transmission database had been hacked.*

*According to the IEBC procedure, every result relayed from the polling station had to be accompanied with a scanned copy of form (34A) that showed the manual tallying and the signatures from the party agents. By Wednesday morning, there was only one form on the IEBC portal, while the provisional results showed nearly all polling stations had relayed their results."*

**11.08.17**

**SC Media**

### [SMEs ahead of larger orgs in IoT security, study](#)

A new study by Pwnie Express has found that small and medium sized enterprises are better prepared to deal with the cybersecurity threats posed by IoT devices.

*"When it comes to Internet of Things (IoT) security, size really does matter, though bigger isn't necessarily better – as it turns out small and medium sized enterprises (SMEs) are better prepared to handle the threats posed by IoT.*

15

*SMEs may not have the resources of their larger peers but they're training them on identifying threats and determining the potential dangers connected devices pose, according to a [study](#) of 950 professionals conducted by Pwnie Express."*

## Privacy

**11.08.17**

**Bloomberg BNA**

### [Colombia May Designate U.S. as Data-Transfer-Safe Destination](#)

The Colombian Government has suggested that it could shortly classify the US as a safe destination for data transfer, potentially providing a significant boost to e-commerce between the two countries.

*"Colombian business interests are reacting favorably to a government [proposal](#) to make data transfers to the U.S. easier by finding its privacy laws adequate to protect personal data, privacy attorneys tell Bloomberg BNA.*

*The draft amendments to Colombia's privacy rules aim for a more market-friendly approach that could ease the flow of low-level personal data to other nations and help attract investment, particularly by U.S. companies. Allowing U.S.-based multinationals to more easily move information in the global digital economy would make Colombia a stronger prospect for business investment, attorneys said."*

## Internet Inclusion

**10.08.17**

**PR Newswire**

### [Angola Cables announced watershed moment for African Internet](#)

The first subsea cable between Africa and South America has moved closer to completion, providing optimism for internet users in both continents.

*"[Angola Cables](#) today took a step closer to completion of the South Atlantic Cable System (SACS) at an official launch in Sangano, Angola. SACS is the first direct link between Africa and South America. The installation of the South Atlantic Cable System (SACS) – a subsea cable with 40 Tbps of capacity that will extend more than 6,500 km to Fortaleza, Brazil – began on the Angolan coast in the municipality of Quissama. The SACS system is being constructed by [NEC Corporation](#)."*

# Global Institutions

**11.08.17**

**ENISA**

## ENISA organises workshop on Cyber Insurance

ENISA is to conduct a study as part of its work to promote the uptake of cybersecurity insurance by companies across the EU.

*"As part of its Work Programme 2017, ENISA is conducting a study to propose recommendations to support the uptake of cyber insurance and the growth of the cyber insurance market in the EU. The focus of ENISA's 2017 study is on the commonality of the risk assessment language in cyber insurance. To validate the findings and recommendations of the study, ENISA is organising a work meeting with industry representatives."*

**11.08.17**

**ICANN**

## Request for Proposal: PTI Service Organization Control Audits

ICANN have issued a new RFP for information system auditors to support existing commitments outlined in contracts between ICANN and its affiliate bodies like the PTI.

*"The Internet Corporation for Assigned Names and Numbers ("ICANN") is seeking a provider to conduct information systems audits mandated by the various contracts between the ICANN organization and the Internet Engineering Task Force (IETF) and the Regional Internet Registries (RIR). The audits are also part of the contract between the ICANN organization and its affiliate, Public Technical Identifiers (PTI)."*

**15.08.17**

**ICANN**

[**Request for Proposal: Human Rights Impact Assessment RFP**](#)

ICANN has published an RfP for an organisation to conduct a Human Rights Impact Assessment of ICANN.

*"The Internet Corporation for Assigned Names and Numbers ("ICANN") is seeking a provider to conduct an independent internal Human Rights Impact Assessment (HRIA) of ICANN's organizational operations.*

*The HRIA is intended to review ICANN organization's internal operational commitment to respect human rights, including mitigate risks and capitalize on opportunities to improve global business operations. The findings will enhance the transparency of internal operations and optimize planning and budgeting necessary to meet the ICANN organization's continued commitment to respect human rights."*

# Diary Dates

**ITU WTDC-17** – **09.10.17–20.10.17**

Buenos Aires, Argentina

**ICANN 60** – **28.10.17-03.11.17**

Abu Dhabi, United Arab Emirates

**IGF 2017** – **18.12.17–21.12.17**

Geneva, Switzerland