CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Friday 30 November 2018

OPPONENTS APPLY BRAKES TO ENCRYPTION BILL

CommsWire (ISSN 2202-4549) is published by iTWire Pty Ltd. 18 Lansdown St, Hampton, Vic, 3188
CommsWire/Telecommunications Editor: Stan Beer
Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder
Advertising: CEO and Editor in Chief, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

ENCRYPTION BILL 'MAY CLASH WITH PARLIAMENTARY PRIVILEGE'

The push by the Australian Government to bring the encryption bill to a vote before Parliament rises for the year is facing an obstacle, after Senate president Scott Ryan raised the possibility that powers in the bill could conflict with parliamentary privilege.

In **a submission** to the Parliamentary Joint Committee on Intelligence and Security, which is currently inquiring into the bill — formally known as the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 — Senator Ryan said parts of the bill clashed with ongoing work to secure privilege rules against executive investigative powers.

Both Morrison and Dutton **have put pressure** on the PJCIS to complete their inquiry into the bill — the last hearing is scheduled for 4 December — so that Parliament can pass the bill before it rises for the year on 6 December.

"Although the bill does not deal with privilege directly, it sits in tension with work being undertaken across the Parliament to properly secure privilege against the exercise of executive investigative powers," Senator Ryan said in his submission.

Under the bill, it may become impossible for a member of Parliament to claim parliamentary privilege or public interest immunity on material that is seized, because the bill allows for material to be seized without any notification.

"In the Commonwealth jurisdiction, the protection of parliamentary material from seizure under search warrant is governed by an MOU [memorandum of understanding] between the Parliament and the Executive signed in 2005," Senator Ryan wrote.

The scope of that protection was designed to ensure that AFP officers executed search

warrants in a way that did not amount to a contempt of Parliament.

After the AFP raid to find out the origin of an alleged leak from NBN Co during the 2016 election campaign, the Senate Privileges Committee had found that documents seized were protected by privilege and should be withheld from the investigation, Senator Ryan said.

The Committee had said that when information, which might attract privilege, was seized or accessed, procedures should be developed to allow claims of privilege to be raised before the seized material was examined.

Senator Ryan (left) said that the Senate had accepted the panel's recommendation that processes should be developed which achieved the objectives cited above.

He said the process was now ongoing and the panel had told him and the Speaker that the use of powers to covertly seize metadata — for which a warrant is not needed — could erode the protections of parliamentary privilege.

"A particular concern to the Senate committee in relation to the covert use of such powers was the question how claims of parliamentary privilege can be raised and resolved when no-one with standing to make a claim is aware that such information is being accessed," Senator Ryan wrote.

"These concerns may be exacerbated by the provisions of the Assistance and Access Bill 2018."

He said suitable changes to the bill could be added through amendments if there was no time to examine them and stick to the timetable that the government had laid down for passage of the bill.

Senator Ryan said he had written to Attorney-General Christian Porter and Dutton about the matter.

"I note that there is a precedent for the committee to work with the ministers responsible to secure the proper protection of privileged material, as was done in relation to the Foreign Influence Transparency Scheme Bill," he said.

Sam Varghese

SENETAS SAYS ENCRYPTION BILL MAY FORCE IT TO MOVE OFFSHORE

Australian end-to-end encryption technology firm Senetas has raised the possibility that it may be forced to manufacture its products outside the country if the Federal Government's encryption bill is passed and becomes law.

In a forceful presentation to the Parliamentary Joint Committee on Intelligence and Security, Senetas chairman Francis Galbally (below) said the bill was demonstrably and fundamentally flawed, adding that the laws of mathematics were not a plaything for politicians.

He pointed out that it was surprising that such a big Australian player in the encryption technology export space like his company had not been consulted at all in the drafting of the bill. It was surprising that the bill had been introduced at all, given the level of objection to it, he added.

Asked by Senator Jim Molan directly whether Senetas was consulted, Galbally responded, "No, and I am gobsmacked that we were not invited."

Appearing along with the Senetas team, the Consilium International Group's Michael Zarew pointed out that four weeks ago, Senetas has sent the submission it had made to the PJCIS to the Home Affairs department.

But, he said, there been no response from the department at all, adding that it looked very much like the government agencies were avoiding Senetas.

Asked many times about how he would define a system weakness — which the bill claims it is not asking anyone to create — Galbally pointed out what many others have failed to do at other PJCIS hearing.

Galbally said it was not possible to say what would create such a weakness until a change was made and then observed for many years.

In the last couple of days, news has emerged of the mass hijacking of routers, with the exploit used having been based on one that was stolen from the NSA and leaked on the Web in 2017.

Galbally pointed to this and said that if an organisation like the NSA, which was the most technologically advanced spy agency in the world, could not secure its exploits, then Australian organisations stood no chance.

Sam Varghese

ENCRYPTION BILL: EFA QUESTIONS NEED TO RUSH LEGISLATION

Digital rights organisation Electronic Frontiers Australia says it is extremely concerned that the Federal Government is rushing the review of the proposed encryption bill, adding that both civil society and the technology industry have serious concerns.

The EFA pointed out, in a statement, that despite comments made by Home Affairs Minister Peter Dutton that the bill needed to be passed before Christmas, the Australian Security Intelligence Organisation was unaware of his (Dutton's) intention to speak to the media.

Nor could ASIO offer any justification for the alleged need for urgency in passing the bill **during a hearing** of the Parliamentary Joint Committee on Intelligence and Security on Monday.

The EFA quoted the chair of its policy team, Angus Murray, as having told the PJCIS on 19 October: “It is incumbent on me, and you; in your capacity as members of this Committee, members of your electorates and individuals who call this great country home, to ensure that we are considering the future and the way that actions today may affect that future.

"In this context, our security is important; however, we must be constantly vigilant to ensure that security does not become a catch cry for the dissolution of basic human rights… the extremely short consultation period for submissions into this Bill and its rapid progression is comprehensively wrong.”

The EFA also pointed to **the evidence** given to the PJCIS by UN Special Rapporteur on the right to privacy, Professor Joseph Cannataci, who pointed out that power was meant to be measured against freedom and justice in a democratic society. Rushing the bill through parliament would make it impossible to achieve this balance.

The organisation also said that the bill lacked proper judicial oversight, reporting, and transparency mechanisms and "seriously increases the government’s ability to secretly monitor Australians and it threatens our software industry’s ability to create secure products and sell them overseas".

It said that building secure software was "incredibly difficult" and that bill had the potential to create vulnerabilities in both software and hardware which could be found and exploited by others.

"The proceedings of the committee so far have not given any indication that this inquiry is complete, or should be cut short - on the contrary, the proceedings have revealed significant issues with the use of existing surveillance powers, that should be of deep concern to all Australians," the EFA said.

"Australians ought to expect better from their government and EFA calls on Australians to demand proper democratic process."

Sam Varghese

ERICSSON INKS FIVE-YEAR CONNECTED VEHICLE DEAL WITH VOLVO

Ericsson has been selected by the Volvo Car Group to provide its industrialised Connected Vehicle Cloud platform, to further enable its digital vehicle services in more than 120 markets worldwide for the next five years.

The deal with Ericsson comes as Volvo Cars, like other major players in the automotive industry, is increasing focus on securing high-quality connected-vehicle services as digitisation increases the importance of software services.

Ericsson says the services will also benefit from the increased speed, low-latency and capacity for mission critical applications, such as autonomous driving, that commercial 5G networks will enable.

Delivered via several geographically distributed centres, the platform takes full account of legal, security, and privacy obligations on a global scale – such as compliance with the European Union's General Data Protection Regulation.

According to Ericsson, with digital services increasingly becoming a differentiation factor for automotive consumers, the need for a secure and dependable service provision infrastructure is critical to provide quality of service at scale.

"This is what the Ericsson Connected Vehicle Cloud delivers – meeting Volvo Cars' high services and applications availability and stability expectations, and allowing Volvo Cars to focus on the value creation of connected vehicle digital customer experiences as a differentiator," Ericsson said.

Åsa Tamsons, head of Business Area Technologies & New Businesses, Ericsson, said: "Ericsson is providing a highly scalable and global platform for connected services to Volvo Cars. By removing complexity in areas such as data legislation and storage management, and improving services latency, our platform enhances the overall user experience of Volvo Cars' connected services.

"Our Ericsson Connected Vehicle Cloud platform will result in rapid innovation and the faster launch of new services to the benefit of Volvo Cars' partners and customers. The new platform enables the latest development in telematics, infotainment, navigation, automation, and fleet management."

Peter Dinham

OPPO RAMPS UP INVESTMENT, WITH $2B R&D IN 5G TECHNOLOGY

Chinese smartphone vendor OPPO is set to invest A$1.97 billion in research and development next year - a 150% increase year-on-year – as the company ramps up investment and research and development in 5G technology.

OPPO says the RMB 10 billion investment comes as it makes “significant strides forward in the development of 5G handsets”.

The Chinese company says that since 2015, it has been investing in R&D into the 5G standard, and when 5G standards were frozen in December 2017, it quickly invested in the development of 5G products.

This the company said allowed it to take the lead in enabling the interoperability of 5G signalling and data links in August 2018 – and by October, OPPO had realised the first 5G smartphone connection.

OPPO announced its latest investment at its technology-focused *‘2018 OPPO Technology Exhibition’* in Shenzhen, China – along with a slew of announcements around its R&D investment, 5G, artificial intelligence (AI) and smart devices.

“5G is a significant network upgrade, which will bring unprecedented speeds and applications to our mobile networks here in Australia.

In addition to striving to become the first manufacturer to launch 5G smartphones, OPPO's exploration of application opportunities in the 5G+ era will ultimately determine the value of 5G," said Michael Tran, managing director at OPPO Australia.

"OPPO will fully integrate 5G with applications and user insights, and continuously innovate to provide users with revolutionary, necessary, convenient and seamless mobile experiences."

To date, OPPO says it has applied AI technologies across a wide range of applications, including photography, facial recognition and fingerprint identification .

In addition, AI has enabled it to launch innovative features including an AI-powered beauty camera, 3D portrait lighting and intelligent recognition scenarios.

But, according to Tran, this is only the beginning of what is possible with AI.

"The benefits brought about by AI technologies will truly be realised when 5G launches in Australia. For OPPO, AI is both a capability and a mindset, meaning our development prospects for AI are very broad."

Tran says that by employing AI to continuously learn users' habits, OPPO smartphones are able to proactively provide a better service and more personalised experiences, "while will lead to smartphones becoming our personal assistants moving forwards".

"In the future, smartphones will be our intelligent personal assistants - and this is something OPPO will definitely enable," said Tran.

"The smartphone is one of the best devices for AI, but there is still considerable room for improvement.

"OPPO will actively embrace artificial intelligence while dedicating focus and resources to cutting-edge AI technologies and applications."

Tran says that with OPPO's commitment to becoming a leader in an era where 5G, AI and Internet of Things are broadly applied, the company is set to expand its product range to include smartwatches and smart home technologies, with its smartphones at the centre of a connected ecosystem.

"We must continue to explore and innovate within this new connected era. In the future, OPPO will fully integrate technological innovation to develop smart devices and homes, with the smartphone at their core.

"Our priority is to develop and provide smart technologies to meet the increasing demands for connected devices in the age of the Internet of Things," Tran said.

Peter Dinham