CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Monday 14 January 2019

HOME AFFAIRS PUSH ENCRYPTION LAW MYTHS: CA

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

HOME AFFAIRS PERPETUATING MYTHS ABOUT ENCRYPTION LAW: CA

A document issued by the Government-funded Australian Cyber Security Growth Network over the new encryption law, has been dismissed by the Communications Alliance as a bid by Home Affairs to perpetuate myths about the legislation.

The **AustCyber document** was based on **a survey** it sponsored which was carried out by the Australian Strategic Policy Institute. ASPI is partly funded by the government but also receives funding from a number of big players in the defence industry.

The poll sought the views of 512 industry players, but only 63 responded.

The document was released on 20 December and therefore did not attract any coverage. ***CommsWire*** asked CA's chief John Stanton, who has been a strong advocate for the telecommunications industry on the issue, for comment.

The encryption law was **passed** on 6 December without any amendments to the version submitted to Parliament on 20 September. Some 50 pages of amendments were handed out to the various parties early on 6 December before debate on the bill began. But it was finally passed without amendments as the House of Representatives had already risen for the year by the time the amendments were taken up in the Senate.

Labor leader Bill Shorten agreed to this compromise on the proviso that the amendments would be passed during the first sitting of 2019. The government has said it would consider the amendments, but has made no commitment that it would accept all of them.

Stanton described the document put together by AustCyber as "an attempt to be helpful", adding that it illustrated the ways in which the Department of Home Affairs sought to perpetuate "a number of myths about the nature of the legislation and the ways in which it can be used".

He pointed to one such example. "For example, the Department states that the Act 'has very strict limitations on the type of assistance that can be compelled by a notice'. In fact, the 'Listed acts or things' at 317E of the Act is frighteningly broad."

There are three ways listed in the law by which the authorities can get industry to aid in gaining access to encrypted material. A technical assistance request (TAR) allows for voluntary help by a company; in this case, its staff would be given civil immunity from prosecution.

An interception agency can issue a technical assistance notice (TAN) to make a communications provider offer assistance.

Finally, a technical capability notice (TCN) can be issued by the attorney-general at the request of an interception agency; the communications minister of the day would also need to agree. This will force a company to help law enforcement, by building functionality.

Stanton said the issuing of the TANs and TCNs did not require a warrant to be obtained as claimed by AustCyber, though the government had continually implied warrants were required. "In fact, the Labor amendments that were withdrawn on the day the Bill passed the Senate would have introduced a warrant framework and judicial oversight," he added.

"But if there does happen to be a warrant in place, then the list of what actions communications providers can be ordered to do is completely open-ended - see the newly amended 317 E (da)."

He said the document also cited the Department as claiming that the legislation “won’t require an employee to be operating under a notice that their employer is ignorant of".

"Again — there is nothing in the legislation that provides that assurance — and there is ample scope (under 317 F) of the Act, for agencies to require that an employee not disclose to his or her employers that they have been served with a notice. The penalty for breaching the secrecy provisions is five years in prison," he said.

Stanton also noted that the assessment and reporting obligation introduced for TCNs did not include a requirement that the assessors – to be appointed by the Attorney-General – be independent.

This, he said, could allow for the appointment of an ASIO officer as the technical expert. "To top it off, the Attorney-General only needs ‘to have regard to’ the report, potentially in the same manner as regard was given to the feedback received during the drafting stages of the Bill," Stanton said, adding that there were many more such examples in the AustCyber document.

"What’s also becoming clear, on closer examination, is that there are all sorts of deficiencies and problems in the government amendments – which is hardly surprising, given that they were thrown together in an all-night drafting marathon and completed a couple of hours before they were rammed through the House of Representatives," he pointed out.

The Parliamentary Joint Committee on Intelligence and Security **announced** on 18 December that it would be conducting another review of the law after Parliament convenes for 2019 and will submit a report about it by 3 April.

Stanton said CA would attempt to highlight these and other problems in a submission to the reconstituted inquiry.

"There is an enormous amount of work still to do – including incorporating amendments along the lines of those proposed by Labor – to try to make this Act workable and reasonable," he said. "It really is a shame that so many stakeholders — who could have contributed much to a thorough and rational legislative development process on these issues — find themselves in the position of trying to mount a rescue mission, after the fact."

Sam Varghese

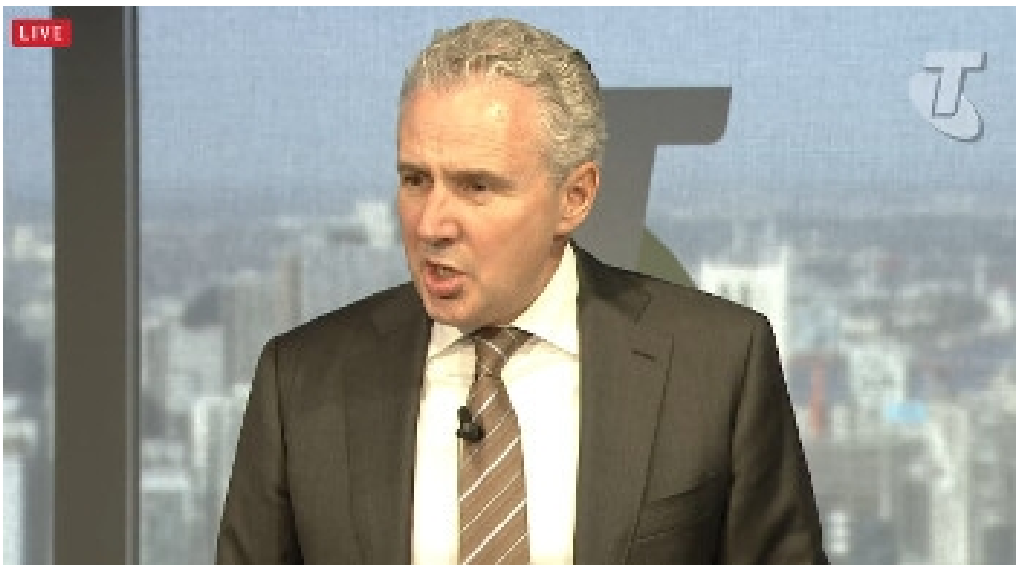
TELSTRA SAYS IT HAS CUT DEALS TO BE FIRST TO OFFER 5G PHONES

Telstra has announced that it has signed exclusive deals with unspecified companies to offer 5G smartphones to its customers in the first half of the year.

The company's chief executive, Andrew Penn, told a media conference at the CES technology show in Las Vegas last Thursday, that these would be some of the "world's biggest brands".

Whatever the brands are, they will be in the Android space only as Apple will not be releasing a 5G iPhone until at least 2020.

Last year, Telstra said that the Swedish telecommunications company Ericsson would be its main partner in the rollout of its 5G network.



“The 5G revolution is now very real.

“More than 200 Telstra 5G mobile base stations are now online across the nation and our customers will very soon be among the first in the world to experience the possibilities this revolutionary technology can deliver,” Penn (pictured above) said.

“Much faster downloads, high-resolution video streaming with less buffering and mobile gaming on the go are just the start of what 5G is capable of delivering.

“This is the year of 5G and, as a world leader in the testing and development of 5G, we have been working closely with numerous global manufacturing and industry partners to make this revolutionary technology real-world ready.

“These strategic relationships are now paying off directly for our customers, who will soon have exclusive access to 5G enabled devices on the nation’s largest and fastest mobile network, and other devices will also soon hit our stores.”

Sam Varghese

HUAWEI LAUNCHES ‘INDUSTRY'S FASTEST’ ARM-BASED CPU

Chinese telecommunications vendor Huawei Technologies has unveiled the Kunpeng 920, which it says is the industry's top-performing ARM-based CPU, in Shenzhen on Monday.

The company also released its TaiShan series servers powered by the new CPU. Three models - one with a focus on storage, another on high-density, and a third focused on balancing both requirements - were launched.

In a statement, the company said the new processor was meant for use in situations involving big data, distributed storage and ARM native application.

The launch marked its bid to join the rest of the industry and take computing performance to new heights.

The Kunpeng 920 uses the cutting-edge 7nm process and was independently designed by Huawei based on the ARMv8 architecture licence.

It is claimed to significantly improve processor performance by optimising branch prediction algorithms, increasing the number of OP units, and improving the memory subsystem architecture.

"At typical frequency, the SPECint Benchmark of the Kunpeng 920 CPU scores over 930, which is 25% higher than the industry benchmark," the company said.

"At the same time, power efficiency is 30% better than that offered by industry counterparts.

“Kunpeng 920 provides much higher computing performance for data centres while slashing power consumption."

The processor integrates 64 cores at a frequency of 2.6 GHz. The chipset integrates 8-channel DDR4, and memory bandwidth exceeds incumbent offerings by 46%.

"System integration is also increased significantly through the two 100G RoCE ports," the company said.

Kunpeng 920 supports PCIe Gen4 and CCIX interfaces, and provides 640 Gbps total bandwidth.

“In addition, the single-slot speed is twice that of the incumbent offering, effectively improving the performance of storage and various accelerators."

"Huawei has continuously innovated in the computing domain in order to create customer value," said William Xu, director of the board and chief strategy marketing officer of Huawei.

"We believe that, with the advent of the intelligent society, the computing market will see continuous growth in the future.

“Currently, the diversity of applications and data is driving heterogeneous computing requirements.

"Huawei has long partnered with Intel to make great achievements. Together we have contributed to the development of the ICT industry.

“Huawei and Intel will continue our long-term strategic partnerships and continue to innovate together.

"At the same time, the ARM industry is seeing a new development opportunity. The Kunpeng 920 CPU and TaiShan servers newly released by Huawei are primarily used in big data, distributed storage, and ARM native applications.

"We will work with global partners in the spirit of openness, collaboration, and shared success to drive the development of the ARM ecosystem and expand the computing space, and embrace a diversified computing era."

Representatives from Huawei's partners — the Green Computing Consortium, Linaro, the Open Edge and HPC Initiative, Hortonworks and China Standard Software — were present for the launch.

Sam Varghese

AIREON SATELLITE A 'NEW ERA' OF AIRCRAFT SURVEILLANCE

US global aircraft tracking system operator Aireon has announced a successful eighth and final launch and deployment of the Iridium NEXT satellite constellation hosting the Aireon space-based Automatic Dependent Surveillance-Broadcast (ADS-B) payloads.

The launch took place with the lift off of a SpaceX Falcon 9 rocket from Vandenberg Air Force Base in California and placed the final 10 Iridium NEXT satellites into low earth orbit (LEO).

The launch brought the total number of Aireon payloads in orbit to 75 (66 operational payloads and 9 spares), completing the historic launch program and passing one of the last remaining milestones before Aireon ushers in what it says will be a new era of global air traffic surveillance and aircraft tracking.

Aireon is the world's first 100% global air traffic surveillance system and the company claims it is revolutionising the way the world travels with space-based technology.

Unlike existing aircraft surveillance and tracking infrastructure, the Aireon system uses space-based ADS-B technology, which enables the automatic and real-time collection of aircraft position data. The Aireon technology gives air traffic controllers and airlines a complete and comprehensive view of the entire sky, like never before.

With this upgraded insight into the world's flight paths, including those in remote and oceanic airspace, Aireon says the entire industry will experience significant direct and indirect benefits.

Claimed benefits include increased safety, more efficient flight routes, more accurate

arrival and departure predictions, faster emergency response times, reduced aircraft separation, a decrease in CO_2 emissions and more.

“Today we passed a major milestone on our journey to revolutionise air traffic surveillance and are just weeks away from a fully operational system,” said Don Thoma, chief executive of Aireon.

“Now that the launches are complete, final integration and testing of the recently launched payloads can commence, after which the world’s first, real-time, truly global view of air traffic will be a reality.

“It’s difficult to contain the excitement until we are formally operational, especially since from a performance standpoint, our technology has far exceeded expectations. Many think this is the end of a journey, being the last Iridium NEXT launch, but for us, this is the beginning of a new way air traffic will be managed.”

Aireon says the system has out-performed all predictions and is processing more than 13 billion ADS-B messages per month, with that number expected to grow upon full deployment.

Air traffic controllers rely on the best and most accurate surveillance data possible to separate aircraft, which is often achieved through multiple redundant layers.

Aireon’s data will provide air traffic controllers with a fully redundant data feed that covers the entire airspace, increasing the availability and reliability of a critical component in air traffic management, with a positive impact on safety and efficiency. This will in turn, help improve flight optimisation by eliminating gaps in fleet data reports, and ultimately enhance the overall safety, accuracy and efficiency of worldwide air travel.

“Aireon’s space-based ADS-B network is just what the aviation industry needs,” said Marion Blakey, former administrator at the US Federal Aviation Administration.

“During my time at the FAA, extensive work was done to promote ADS-B technology for global air traffic management efforts. Today’s successful launch is not only a victory for Aireon but for the aviation industry, as we are now one step closer to having a clear, accurate and complete picture of the world’s airspace, including over the oceans and remote areas.”

A total of 81 Iridium NEXT satellites have been built, all of which have the Aireon payload onboard. There are now 75 satellites deployed, with nine serving as on-orbit spares and the remaining six as ground spares.

Peter Dinham

EARLY WARNING NETWORK HACKED, BOGUS THREATS SENT OUT

Hackers gained access to the database of a New South Wales-based company that sends free weather warnings on the weekend, through the use of stolen credentials and sent bogus alerts to some users of the system.

Early Warning Network said in a statement on its website on Monday that the unauthorised alerts were sent on Saturday night.

It said the alerting system was accessed at about 9.30pm on 5 January, and a "nuisance message' sent out to some subscribers whose addresses were in its database. Email, text and landline messages were sent.

"EWN staff at the time were able to quickly identify the attack and shut off the system limiting the number of messages sent out," the company said.

"Unfortunately, a small proportion of our database received this alert.

“Our systems are back up and running providing ongoing alerts for severe weather and natural hazard events.

“Investigations are continuing with police involvement."

The bogus messages said: "EWN has been hacked. Your personal data is not safe. Trying to fix the security issues."

The statement said the police and the Australian Cyber Security Centre had been notified.

EWN said no personal information had been exfiltrated as a result of the hack.

Sam Varghese