

CommsWire

Essential daily reading for the communications industry executive

An iWire publication

www.itwire.com

Editor: Stan Beer

Friday 14 December 2018

ACCC THROWS SPANNER INTO TPG-VHA MERGER



CommsWire (ISSN 2202-4549) is published by iWire 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

ACCC RAISES CONCERNS OVER PROPOSED VODAFONE-TPG MERGER

The Australian Competition and Consumer Commissions says that removing TPG, which it viewed as on the way to becoming a fourth mobile competitor in Australia, from the fray through its merger with Vodafone would substantially lessen competition in the sector.

In [a statement](#) issued on Thursday, the ACCC said that a mobile market with three major competitors was likely to have less competition than one with four.

The watchdog said it would also scrutinise the impact of removing Vodafone as a competitor in the fixed broadband market.

Vodafone Hutchison Australia and TPG Telecom [announced](#) a merger of equals on 30 August, with the scrip deal creating an enterprise values at about \$15 billion.

“Our preliminary view is that TPG is currently on track to become the fourth mobile network operator in Australia, and as such it’s likely to be an aggressive competitor,” ACCC chair Rod Sims said.

“We therefore have preliminary concerns that removing TPG as a new independent competitor with its own network, in what is a concentrated market for mobile services, would be likely to result in a substantial lessening of competition.

“If TPG remains separate from Vodafone, it appears likely to need to continue to adopt an aggressive pricing strategy, offering cheap mobile plans with large data allowances.”

“Our preliminary view is the merged TPG-Vodafone would not have the incentive to operate in the same way, and competition in the market would be reduced as a result.

“A mobile market with three major players rather than four is likely to lead to higher prices and less innovative plans for mobile customers.”

Sims said although Vodafone was a relatively minor player in fixed broadband at the moment, the ACCC considered it may become an increasingly effective competitor because of its high level of brand recognition and existing retail mobile customer base.

The ACCC said it would also look at the longer-term impact of the proposed merger, given that there was likely to be increased take-up of mobile broadband services rather than fixed home broadband services in future, especially after 5G was rolled out.

“The ACCC is continuing to consider whether operators will need to offer both mobile and fixed broadband services in the longer-term to remain competitive, meaning that TPG and Vodafone will necessarily be closer competitors in the future,” Sims said.

The watchdog has published [a statement of issues](#) and has invited submissions until 18 January 2019. A final decision on the proposed merger will be announced on 28 March 2019.

Sam Varghese

VODAFONE SAYS WORKING CLOSELY WITH ACCC ON MERGER ISSUES

Vodafone Hutchison Australia says it has engaged closely with the Australian Competition and Consumer Commission about its proposed merger with TPG Telecom, providing significant information about the consumer benefits and challenges faced by providers.

In a statement, the company said it was confident the merger would go ahead in the first half of 2019, subject to approvals.



A statement of issues, as [announced](#) by the competition watchdog on Thursday morning, was a common interim step in the merger review process, setting out issues for further consultation, VHA added.

It said it would look at the issues raised by the ACCC and provide comprehensive responses in due course.

Vodafone Hutchison Australia and TPG Telecom [announced](#) a merger of equals on 30 August, with the scrip deal creating a company with an

enterprise value of about \$15 billion.

VHA chief executive Iñaki Berroeta (above) said the company would continue to work with the ACCC on its review of the proposed merger.

"This proposed merger is a significant transaction, and we respect the need for the ACCC to make a carefully considered decision, so today's announcement wasn't unexpected," he said.

"Customers will be the big winners of a proposed merger between VHA and TPG Telecom, and we'll continue to engage with the ACCC as we have done over recent months."

"Increased investment requires increased scale, and the proposed merger will enable the merged entity to take competition in the market to the next level."

"The merged company will have significantly increased ability to invest in networks, new technologies, and competitive plans and products for Australian customers."

The merger is subject to approval by the Federal Court and TPG Telecom shareholders, as well as other regulatory approval processes.

Sam Varghese



John de Ridder

Telecommunications Economist

strategic management • wholesale and retail pricing • regulatory issues

[click here to go to www.deridder.com.au](http://www.deridder.com.au)

NSW TO BAN MOBILES IN GOVT PRIMARY SCHOOLS FROM 2019

The New South Wales Government will ban the use of mobile phones in government primary schools from next year, in an effort to reduce the incidence of online bullying and also to remove a major source of distraction.

The ABC [reported](#) that the decision was made in the wake of a review begun in June and headed by Dr Michael Carr-Gregg, a child psychologist.



France [introduced a ban](#) on mobiles from September across primary up to middle schools.

Under the French rule, the children are allowed to bring the devices to school but not allowed to take them out.

The NSW survey received about 14,000 responses and 80 submissions and the issues of lewd images being shared and unnecessary familiarity with strangers had also been raised.

Government high schools would be allowed to decide whether they want to join the ban or the extent to which they would allow mobiles to be used.

NSW Premier Gladys Berejiklian said: "We want to ensure mobile phones and other smart devices complement students' learning, and are handled at school in an age-appropriate way."

"Sometimes mobile phones can be useful in a secondary school context where they are used to augment learning activities," NSW Education Minister Rob Stokes said.

"But they can also be dangerous and be a distraction."

Sam Varghese

OPTUS TAKES KIDS ON A CYBER SECURITY JOURNEY AT LA TROBE

Students from grades five to eight participated in a number of workshops on cyber bullying, staying safe online and cyber security as part of a Digital Smarts Day organised by Singtel Optus on Wednesday.

The students, from across Melbourne, were taken to La Trobe University, for the free interactive program which is meant to help them learn how to be safe, responsible and thrive in the digital world.



Optus' Alison Polyik, students from Macleod College, Optus cyber security expert Stewart Hayes and Dr Alex Ng, lecturer in cyber security at La Trobe University.

Optus sustainability director Helen Maisano said: “Digital Smarts Day is developed from the Optus Digital Thumbprint program.

“We partner with Kids Helpline for primary school students and we also deliver Digital Thumbprint for secondary school students.

“Our aim through these free, interactive in-school programs is to support young Australians with the knowledge and practical advice for a positive online experience.”

The Digital Thumbprint program empowers young people to stay safe online and through it more than 100,000 students have learned to be safer and smarter online.



“With the demand for cyber skills and cyber jobs growing rapidly, we placed a strong focus on cyber security this year, expanding Digital Smarts Day by partnering with La Trobe University’s Cyber Faculty and including content from the Optus Cyber Security Experience powered by Life Journey.

“This cross-sector collaboration means that students can learn, at a young age, the skills and qualities that will help them thrive in the digital world,”

Maisano added.

“Students explored careers with Optus cyber security professionals and heard first-hand from students undertaking La Trobe University’s under and post graduate courses in cyber security.

“While the digital world presents significant issues such as cyber bullying, it also provides countless benefits and opportunities.

“Events such as Digital Smarts Day and our ongoing programs within primary and secondary schools provide young people with practical strategies to navigate risk and important insights to prepare for the cyber jobs of tomorrow.”

La Trobe University vice-chancellor Professor John Dewar said the Digital Smarts Day program was aligned with La Trobe’s expertise in cyber security research and teaching.

“We are delighted to partner with Optus on this important program which will not only help young people become responsible digital citizens but will also open their eyes to the wealth of exciting future job opportunities in the rapidly evolving field of cyber security,” he said.

“Students who choose to study one of La Trobe’s own wide-ranging cyber security degrees learn from research experts at the top of their game in disciplines spanning cyber intelligence, information technology, cyber-crime and cyber law – all areas in demand from employers in Australia and across the world.”

Sam Varghese

ASD MYTHBUSTER BURGESS SPREADS SOME MYTHS OF HIS OWN

COMMENT: It is somewhat ironic that the director-general of the Australian Signals Directorate, Mike Burgess, has chosen to vent about so-called myths around the new encryption law, when the man himself has been spreading a myth about 5G technology.

Burgess released [a statement](#) on Wednesday, listing seven myths which, [he said](#), had been spread about what is officially known as the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. (Burgess calls it the TOLA Act). But in trying to shoot them down, he appears to have advanced some myths of his own.



Burgess was [quoted](#) by *The Australian* in October as saying in what many dubbed a major speech: "The distinction between core and edge collapses in 5G networks. That means that a potential threat anywhere in the network will be a threat to the whole network."

This was advanced as justification for banning Chinese telecommunications companies Huawei and ZTE from a role in Australia's 5G rollout.

But this was [proven false](#), when a 5G trial in Auckland, conducted jointly by Huawei and New Zealand telco Spark used a Huawei 5G NR (New Radio on both the C-band and mmWave) and a 4G Radio Access Network, both of which were deployed by using dedicated hardware connected to the Cisco Evolved Packet Core, with each component isolated.

The ASD then [claimed](#) that Burgess' reference was to more "mature" 5G implementations.

That isn't correct either. You can read the claims and the refutation [here](#).

But to the matter at hand: myths. The first one that Burgess claimed was being spread was that the information of individuals is no longer safe. In support of this, he stated the bleeding obvious: "If you are using a messaging app for a lawful purpose the legislation does not affect you."

I have done [my fair share of writing and commenting](#) on the encryption law, but have never seen any claim like this. Not sure where Burgess got that one.

The second myth Burgess says is being spread is that agencies get unfettered power under the law. As warrants can give one access to phone calls, there is no difference if they allow access to encrypted communications, runs his argument.

There are three new powers in the law which force individuals or companies/organisations to build in backdoors into devices or software. Fines or prison beckon for those who resist. And this is not extreme power?

What can law enforcement gain from encrypted content that it cannot deduce from metadata – which, few will inform the public, *cannot be encrypted?* (Emphasis mine).

As to unfettered power, let me digress a bit. When Australia passed the metadata retention law in 2015, we were assured that only the 20 or so agencies authorised to access it would be allowed to do so. But last month, Communications Alliance chairman John Stanton [provided a list](#) of some 80 agencies which had sought access. Open slather would be a gross understatement.

Who's to guarantee a repeat won't occur with this law too?

Flying in the face of statements from variously highly qualified technical experts, Burgess claims that the security of the Internet is not under threat because of the law. But when vulnerabilities are introduced, they are accessible both to the law-abiding citizen and the crook. Claiming that such vulnerabilities are "highly targeted" is a red herring, because nobody can predict the impact of a software change and all its possible ramifications.

A hint to Burgess: just call your counterparts at the NSA and ask them about [the Shadow Brokers](#).

While tech companies themselves have been saying that the law will force them offshore, Burgess dismisses this, saying that Australia is not the first to pass such a law, the UK went first. True, but the UK has a bill of rights, which Australia lacks. Also, some part of the UK bill has now been struck down. And though the UK bill was passed in 2016, it has yet to be used. Why, one wonders. [*iTWire* has [a story](#) this morning from an unnamed firm which is planning to move operations from January.]

The next myth being spread, avers Burgess, is, "There is no way to be sure that the

communications of Australians won't be jeopardised." Here he cites oversight from the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman as mitigating factors, as also the review by former judicial officials and a techie who is certified by ASIO. Why not have a sitting judge? And why have a techie certified by ASIO – who is almost certain to be an ex-ASIO man/woman? Since when did the Commonwealth Ombudsman have oversight of intelligence agencies?

The next myth is, again, one I have never heard: that ASD will be able to spy on Australians. ASIO is doing an excellent job of that, along with all the other law enforcement agencies we have. This, again, seems to be a red herring.

The final myth that Burgess set out to bust is that the reputation of Australian tech companies will suffer. Here he tries to draw a difference between what Australia has meted out to Huawei and the impact that the law will have on Australia. Others, like Andrew Hastie, the head of the Parliamentary Joint Committee on Intelligence and Security, have run a similar argument based on the reasoning that Australia is a democracy and China is a dictatorship.

But this reasoning is fallacious [as pointed out](#) by Francis Galbally, the chairman of encryption technology firm Senetas, a company which exports a sizeable portion of the \$3.2-billion-odd Australian tech exports each year. During [a hearing](#) of the PJCIS, he responded to Hastie, saying: "With respect, Chair, you say there's no equivalent, and I agree, it's not equivalent, but I can tell you other countries take a different view. At the moment, as we stand in the world, Australia is regarded as the most trustworthy country in the world for cyber security products, bar none.

"There are countries in the world that don't trust the US. There are countries in the world that don't trust Israel. There are countries that don't trust Singapore. There are countries in the world that don't trust other countries for all sorts of reasons. Australia stands up as the most trustworthy.

"That's why we've been able to sell our products into more than 40 countries around the world. That's why even eastern European countries use our products for their secret service protection; we're trusted. This bill gives a perception of mistrust, and whatever you say, whether it's really going to apply to us or not or whether there's a democracy or not, it gives a perception of mistrust."

Trust. Perhaps Burgess should spend some time trying to understand that concept.

Sam Varghese

Not your copy of CommsWire? If so please join up!

All material on CommsWire is copyright and must not be reproduced or forwarded to others.

**If you have a trial subscription that you are finding valuable please subscribe formally via subscriptions@itwire.com
Subscriptions are very affordable for individuals, corporate and small teams/SMB. Special deals and discounts for PR firms**

For editorial, contact, Stan Beer, CommsWire Editor: 0418 516 720 | stan.beer@itwire.com

To subscribe or advertise contact, Andrew Matler, CEO: 0412 390 000 | andrew.matler@itwire.com