

## **Foxtel, AMTA oppose anti-siphoning extensions**

Both Foxtel and the Australian Mobile Telecommunications Association have come out in force against any extension to anti-siphoning regulations. The two organisations have made submissions to an ongoing review on the anti-siphoning list, arguing that the laws are well past their use by date.

Anti-siphoning laws allow free-to-air broadcasters rights to sports events over broadband-based competitors such as Telstra or Pay TV operators like Foxtel. In its submission Foxtel argued that the regulations were a “historic relic” detrimental to viewers and sports codes alike.

Foxtel said the list was “unsustainable” in a digital economy, saying: “Protectionism reduces economic efficiency and innovation and has created a media industry that is generally stunted by regulatory impediments. Moreover Australian’s viewing habits have changed significantly over the last 15 years and people no longer accept that their viewing should be controlled by the old networks. Put at its simplest, Australians want to watch what they want, when they want to and where they want to and increasingly on the device of their own choosing.”

AMTA took up a similar argument, saying Australian viewing habits had undergone major shifts. “There have also been improvements to the capacity and speed of mobile and fixed broadband networks to accommodate the delivery of video services,” CEO Chris Althaus said. “It is... AMTA’s view that new media platforms are still in early development and must be provided the opportunity to grow and evolve without the burden of regulation that would, in effect, simply stifle innovation and protect the strongest players.”

Luke Coleman

## **Carriers “undermined” by mobile app stores: report**

Mobile carrier profits are being “undermined” by a growing number of mobile app stores, according to research firm Telsyte. Releasing a new report on the mobile market in Australia, Telsyte found that smartphones are now used by 16% business users and 12% of consumers – allowing users to bypass the traditional “walled gardens” of operators.

“About 40 smartphones will make their way to the Australian market this year alone, with almost half of those launched between now and Christmas,” said principal analyst Warren Chaisatien. The researcher said that vendor app stores like Apple’s iTunes and the Google Android Market were reducing mobile carriers to ‘dumb pipes’. “Mobile operators will be fighting back to put themselves in the picture again by introducing “open garden” portals in the next couple of years, where content and applications are personalised and made user-relevant through network-based intelligence and billing relationships,” he said.

But operators are not the only ones to lose out in the ongoing rise of the smartphone – traditional mobile juggernauts Nokia and Microsoft were said to be losing market share. The research found that the existing mobile landscape was poised to change “yet again” in the coming year, with “Apple, BlackBerry and Google’s Android... expected to gain more ground while Symbian and Microsoft will continue to lose momentum.” Apple’s iPhone is now the second most popular smartphone in Australia, Telsyte said.

Chaisatien added that mobile devices would become the next battleground for cloud computing applications. “As if three screens were not enough, Australians will be surrounded by “the fourth screen” – a highly portable, wireless Internet-enabled tablet computer – in the coming year. Amazon’s Kindle is just the beginning of a slew of new mobile devices to hit the local market next year.”

Luke Coleman

## **Symantec: ersatz security tsars on 4x Rudd’s salary!**

Top cybercriminals spruiking rogue security software are waltzing off with earnings almost four times higher than the Prime Minister of Australia, according to security firm Symantec. In an international study covering the twelve months to June 2009, the company found the number of rogue security scams perpetrated in the APAC region relatively small compared to the US and Europe – but still warned Australian consumers to beware the costs and knock-on security risks of ‘scareware’.

Rogue security applications presents themselves as legitimate security programs, but actually provide little or no functional value – and may come loaded with additional threats such as malicious code or security hacks. Users are typically conned into installing the bogus protection software via website ads posted by cybercriminals, telling internet surfers that their machines are infected and providing a link to download the rogue security software in order to ‘fix’ the non-existent problem.

Symantec had picked up 250 different fake security programs by June 2009; it listed the five most common as SpywareGuard 2008, AntiVirus 2008, Antivirus 2009, SpywareSecure, and XP Antivirus. 6% of the scams occurred in the APAC region, against 61% in North America and 31% in Europe, the Middle East, and Africa. The firm also noted that cybercriminals were monetising the scams via organised, pay-for-performance business models, with scammers rewarded for fooling users into installing the rogue programs: the top ten sales affiliates for one distribution site, said Symantec, were earning an average of \$25,000 per