Australian Journal of Telecommunications and the Digital Economy

Vol 2, No 1 (March 2014)

Table of Contents

Editorial: Interesting issues for an industry at a time of record growth

Peter Gerrand
Managing Editor

This editorial notes several key indicators of record growth in Australian telecommunications, as the backdrop to the second issue of this multidisciplinary policy Journal. The growth in social connectivity and 'big data', together with the rapid evolution of new infrastructure technologies, all pose interesting challenges for good policy making – and for keeping up with new developments. The satisfying backdrop of high growth in the telecommunications industry provides a canvas on which to introduce the other thirteen articles which make up this edition (V2 N1) of the *Australian Journal of Telecommunications and the Digital Economy*.

Introduction

Our industry is in a state of solid – and in some areas, spectacular – growth. The OECD has reported that in June 2013, Australia topped their league tables for mobile broadband, with a penetration rate of 114%[1]. However the ACMA notes that whereas the penetration of mobiles increased by 3% in the 2013 financial year, the major growth area lies in downloaded data, which increased by 59% (to 677 petabytes) – 93% of this by fixed-line access[2] (which rather justifies the need for the NBN, given we only had 25.6% penetration of fixed-line broadband access at the end of that year[3].)

Our mobile phone networks now cover 99% of the Australian population *where we live*, a very creditable statistic, although only 25% of the landmass[4]. And the coverage by the much faster 4G mobile networks is increasing: market leader Telstra reported in December 2013[5] that it had switched on its 3,500th base station, and Vodafone and Optus are clearly in a race to match its coverage. The national communications satellites provide 100% coverage in principle, but the demand has been such that their current capacity is effectively exhausted[6]. (NBN Co's two new Ka-band satellites will commence operation in 2015, providing 12 Mbps download speeds to 3% of the population living in remote locations.) As an additional encouraging sign from the demand side, the Telecommunications Industry Ombudsman reported in October[7] that the number of consumer complaints in the 2013 financial year represented a five-year low; and reported again in March that complaints received in the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.33

October-December quarter were the lowest in six years (although they still arrive at about 360 a day)[8].

It is clearly the growth in use of tablets and smart phones that is accelerating the take-up of broadband data, whether downloaded directly from cellular radio networks or (more commonly) via WiFi from fixed accesses to our homes, offices, hotels and cafes. By December 2013, 53% of Australian children between 6 and 13 years owned or used a tablet computer, according to a Roy Morgan survey[9]. And Telsyte reports[10] that the sales of tablets doubled in 2013 to reach an impressive 4.8 million units.

The next 'big things'

On the supply side, the next big development is 5G, the new mobile technology intended to support the 'Internet of Things'. We have commissioned Stuart Corner to write an overview article for this issue on what 5G means, and how its capabilities are likely to differ from those of the current 4G, 3G and earlier generations of mobile technologies. In our June issue, we plan to publish articles on the new mobile infrastructure technologies that will support 5G. In the meantime, as the adequacy of mobile coverage remains a contentious issue in some areas, we publish a paper by Shara Evans on lessons to be learned from US techniques in monitoring the coverage of current 3G and 4G networks.

Of course we are still waiting for the full realisation of 2009's 'next big thing', our National Broadband Network. Given that much of the NBN's business plan is still under review, we publish two policy articles aimed at encouraging positive outcomes for the new NBN. The first, by the current author, points out the implications of leaving uncorrected a fundamental error in the new Australian Government's deregulatory policy for NBN Co, which could be financially disastrous. The second, by Craig Watkins (from Informative Technology Innovations) and Kelvin Lillingstone-Hall (CEO, OAK Telecom), argues that providing Fibre to the Distribution Point is a more cost-effective technology solution for the NBN than Fibre to the Node, and provides a much cheaper transition to the ultimate broadband solution of Fibre to the Premises.

In our June issue we hope to provide expert critiques of the NBN reviews commissioned by the Minister of Communications.

Issues around 'big data'

Since Edward Snowden's revelations on the exhaustive extent of digital surveillance on our activities by national security agencies, issues of data security and privacy in using the Internet 'Cloud' remain legally contentious and uncertain. We continue the theme of Cloud data security, commenced in our November 2013 issue, with a structured, comprehensive

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.33

review by David Vaile, head of the Cyberlaw Centre at the University of NSW, of the research literature and legislation bearing on this topic. In particular his team addresses practical questions such as 'How can Cloud services be used safely, and when can they be dangerous?' and – more ominously – 'In a court case, could you prove and exercise your (the owner's) rights to control, access or delete data held in the Cloud?'.

A topical issue in Internet governance

New issues in Internet governance have recently arisen in the treatment of geographical names in the domain name system (DNS). Who has ultimate rights to domain names such as .berlin, sydney.com or melbourne.com.au? Heather Forrest from the Law School of the Australian Catholic University provides a report on the current treatment of geographic names by ICANN, on the one hand, and WIPO's Universal Domain Name Resolution Process (UDRP) on the other. Chris Chaplow, the founder of the andalucia.com tourism website, writes a memoir on the first application of the UDRP to a disputed geographic name (his own!); and David Lindsay from Monash University, himself the author of a authoritative textbook on Internet Domain Name Law, provides a book review of Dr Forrest's new book on the protection of geographical names in international law and in ICANN's DNS policy.

Policy research to serve the digitally enabled society

But all this new infrastructure, whether in the DNS or in broadband networks, has presumably a broader purpose: to serve the digital economy and, more fundamentally, the digitally enabled society. The essay by Professor Catherine Middleton of Ryerson University on 'Building a digital society: questions for communications researchers' outlines three areas in which media and communications researchers can offer insights into the ongoing development of a digital society: infrastructure development, the role of mobile connectivity, and the need for better data through which to understand engagement in the digital society. Man Chui Jung (from the South Korean Foundation of Agriculture, Technology, Commercialization and Transfer) and co-authors Sora Park and Jee Young Lee from the University of Canberra describe the results of their study of South Korea's Information Network Village project, an investment in human capital that demonstrated how the 'digital divide' can be reduced in rural Korea. And RMIT University research economist Professor Jason Potts writes on the economic arguments for investing in free public WiFi – very topical given the initiatives being taken by several cities around the world to provide free WiFi in order encourage inward tourism.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.33

Memoirs by telecommunications activists

To celebrate major initiatives within Australian telecommunications, this Journal has initiated what we hope will be a regular History section, in which we encourage the publication of memoirs by those who took a key role in creating those initiatives. We inaugurate this series with a memoir by Robin Eckermann on the creation of TransACT, Australia's first VDSL broadband carrier, for which he was the founding Chief Architect.

An interview with our Chief Scientist

Lastly, we are pleased to publish an interview by free lance journalist Beverley Head with Professor Ian Chubb AO, Australia's Chief Scientist, which draws out his career trajectory and provides him with an additional forum in which to present his views on the policies needed to provide Australia with greater capacity for innovation in the post-mining boom era.

Notes

[1] See http://www.oecd.org/sti/broadband/communications-outlook.htm

[2] See http://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/communications-report-fast-facts

[3] See http://www.oecd.org/sti/broadband/communications-outlook.htm

[4] See http://www.communications.gov.au/mobile_services/mobile_phones

[5] See: http://www.computerworld.com.au/article/433391/updated_4g_australia_state_nation/

[6] See http://www.smh.com.au/it-pro/government-it/nbn-satellites-near-full-capacity-20131115-hv2m5.html

[7] See http://www.arnnet.com.au/article/529665/telco_complaints_drop_five-year_low/

[8] See http://news.theage.com.au/breaking-news-national/telco-complaints-hit-sixyear-low-20140320-3542v.html

[9] See http://www.roymorgan.com/findings/5486-tablet-computer-use-now-mainstream-among-young-australians-december-2013-201403132227

[10] See https://www.telsyte.com.au/?page_id=691

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.33

‘STEM education and innovation are essential for national success’

A profile of Australia’s Chief Scientist, Ian Chubb

Beverley Head

Beverley Head interviews Australia's Chief Scientist, Professor Ian Chubb AC. This article plots his scientific and academic journey, and reveals his concerns regarding the need to boost Australia's performance in science, technology, engineering and mathematics (STEM) in order to transform the national economy.

In the late 1940s a grey-suited teacher called Mr Honey sent a small boy outside, into the schoolyard, sparking a lifelong passion for science and learning.

The Menzies Creek Primary School had one room and one teacher for its 20 children; Mr Honey needed to concentrate on the older students so would buy himself some time by sending the younger children outside to study the natural world.

Concentrating on the movement of a worm, the appearance of a butterfly, or the emergence of a cicada, the young Ian Chubb started to develop a fierce curiosity about the natural world. Mr Honey, who Professor Chubb still characterises as the most influential teacher he ever met, sparked an interest in, and passion for, science that would sustain Chubb to the very top of his profession.

Professor Ian Chubb AC is now Australia’s Chief Scientist. His role is to provide high-level independent advice to the prime minister and other government ministers on science, technology and innovation. He is also the nation’s prime advocate for Australian science internationally.

“The real issue is that we have some very good research in Australia,” he says. But he tempers that, noting; “The average research is not spectacularly good but it’s OK. We could do better and be more strategic about it.”

He offers the metaphor of science policy being akin to a gardener who wants to grow flowers of a specific colour. “We tend to throw the seeds up and hope we get the right colour,” where

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.30

he says in other countries, particularly the US, UK, Sweden, Germany and many countries in Europe, gardening policy would have already ensured that the right mix of seeds was present to get the desired flower colour.

Part of the problem he believes is a lack of interaction between business and education. Only 4 per cent of businesses in Australia collaborate with universities he says, compared to 50 per cent in the UK. “That is simply not good enough, and it’s particularly important in Australia because our researchers tend to be found in higher education institutions.

“The British have taken a very strategic approach to build bridges. We’ve talked about it for 20 years, it’s about time we did it.”

Chubb also believes that there is a need to foster closer links with international research efforts noting that although about 3 per cent of the world’s research outcomes emerge from Australia – that still means that 97 per cent are found overseas. “How do we link our research to that?”

In terms of the “flower colours” Australia needs, Chubb says; “The reality for us is that there are things that are particularly important to Australia. We need to understand the environment better: water, our aquifers, how we can be a food bowl for anywhere when the weather patterns have changed so much.

“I believe we can’t innovate something if we don’t know about it – so we need to be linking to other countries and other organisations,” and analysing global information sources in order to better prepare Australian industry for the challenges ahead.

It’s for that reason that he believes digital platforms and high speed communications networks are essential underpinnings for effective e-collaboration adding; “That’s why Australia can seriously lament the fact that the number of ICT graduates has fallen from 4,600 a year to 2,500 and the number of female graduates in ICT has dropped from 1,500 a year to 500.”

In early 2014 Chubb wrote an article published in the *Australian Financial Review* which lamented the 36 per cent decline in students starting an IT degree since 2001, and the even starker 41 per cent decline in students graduating with IT degrees in the same timeframe.

Chubb, who boasts a storied biography, has an intimate understanding of science, tertiary education and the need to encourage graduates across the STEM (science, technology, engineering, maths) disciplines.

Studying chemistry and biochemistry as an undergraduate instilled an interest in the human brain, which he describes as “the ultimate puzzle – why it works and why it doesn’t”.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.30

After a couple of years at Belgium's University of Ghent he took up a research position at Oxford University for several years before returning to Australian in 1978 to the new school of medicine at Flinders University.

Asked to nominate his greatest achievement as a scientist Chubb modestly claims it came through "accumulating a good team of excellent people. When I came back to the new medical school in Adelaide the lab was a room with a sink and nothing else." After relocating the sink Chubb set about building a team of 15 people who together advanced neuroscience. Among his colleagues, both at Oxford and Adelaide, was Chubb's lifelong friend, Professor Peter Somogyi, today acknowledged as one of the world's greatest neuroscientists and now director of Oxford University's anatomical neuropharmacology unit.

One hot October night, swinging in a backyard hammock with a glass of wine to hand, Chubb's wife suggested that his life could perhaps be a bit harder. It led him to look for other opportunities and he accepted the role of deputy vice chancellor at Wollongong and honorary professor of biology.

Chubb's final science experiment was conducted in 1986, since when he has worked in senior roles in tertiary education (senior deputy vice chancellor of Monash University, vice chancellor of Flinders University and vice chancellor of the ANU along with a series of senior advisory roles in the sector) before taking on the role as Chief Scientist in 2011.

His tenure officially ends in May next year. Chubb, now 70, quips that "this is no country for old men" although he does not rule out a further term noting the appointment of Chief Scientist is a question for the government of the day.

Age does not seem to have wearied him; Chubb remains passionate about the need for effective science policy and most particularly the supporting education infrastructure needed to develop the nation's skills base.

Throughout his tenure Chubb has stressed the need for a more strategic approach to STEM education from primary level up. In an address to the 17th National Engineering Heritage Conference in November last year Chubb noted that Australia spends less than 3 per cent of primary teaching time on science and 18 per cent on some form of mathematics. This by 2011 had translated to just 9.6 per cent of students studying advanced maths compared to 14.1 per cent 16 years earlier.

As Chubb noted, more attention must be paid to the time spent teaching science to primary students, societal attitudes to science as a career, and the pre-requisite subjects for university admission.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.30

During that November address he stated: “We should commit to developing a long term and cohesive national strategy for STEM in Australia.” Asked whose responsibility this should be, Chubb says: “This isn’t for government, universities or business to fix on its own. We are all inside the tent to work out the solution. “

Without access to skills, Chubb worries that national innovation will stagnate.

“Four per cent of Australian companies have taken new products and services to the international market, 4 per cent to the domestic market – given there is some crossover that means that some number equal or less than 8 per cent of innovation is for the market. I would think that is a fairly small level of innovation.

“Some keep innovation inside the company – but when that is over 60 per cent, compared to 8 per cent focused on new products, the proportions seem odd.” Chubb questions whether innovation’s contribution to competitive advantage is properly understood by industry and whether incentives to support innovation are properly aligned.

In August 2013 in a joint article with the CEO of the Business Council of Australia, Jennifer Westacott, Chubb discussed the need for “a 50-year agenda founded on Australia’s capacity to innovate, adapt and value add in traditional sectors”.

Again he expounded the need for collaborative platforms, noting that “It will be collaboration that allows us to create the systems and the environment that foster and drive innovation…innovation can only flourish when people and organisations have the requisite skills and abilities and when they operate in an environment that provides them with the scope and incentive to collaborate and innovate”.

In terms of the industrial sectors which hold most promise for Australia’s long term prosperity, Chubb notes: “We have grown medical devices and biotechnology from a really small businesses ten years ago to a fairly substantial base.

“In quantitative terms you get greater innovation out of your smaller businesses – although that is a little unfair to larger companies which do innovate.

“We need to encourage people employing often 10-100 people and that’s where the university links should come in - where they can learn that some people might be using a different alloy or a different IT system. The university researchers can walk along the path with them.

“We have got to think of what sort of economy we want in 10, 15, 20 years because it all starts with education. We are in a global market and it is no use thinking that we can attract people here because Australia is a nice place to live.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.30

"We need enough computer science people and big data skills so that we can be looking at sharing data and conducting e-research."

In terms of the technological underpinnings to support national and international e-research and collaboration Chubb notes that "It seems fairly simple that the better we can communicate at high speed and on a big scale the better it will be".

Slow Internet speeds would inevitably prove a hindrance. "Communications at speed and with volume and dependability – the benefit to us all would be huge."

While Chubb has been a vocal and publicly active Chief Scientist, he needs also to ensure his messages resonate at the highest level of Government, and he has recommended that Australia borrow a leaf from the US and establish a body equivalent to the US Presidential Council of Advisors of Science.

"From what I have seen of the US system it works well. They have strategic research priorities that we have never had – and out of that one result was the programme to create technology teachers for schools."

He acknowledges the US funding model differs from that in Australia, but he does not view the funding regime as an insurmountable barrier.

Precisely how Australia lifts its game in science and technology is still unclear. That it must is unquestionable.

"When I sit down and think of the challenges facing us as a people and the whole planet…science will be there at the core.

"We have got to understand how to work with the community and expectations. It's really important we understand the natural world, the constructed world, how biology works – and there is a lot of physics and maths in the smartphone we carry in our pocket."

Asked about the legacy he hopes to leave as Chief Scientist, Chubb says that he hopes to drive an embedded and strategic approach to science and innovation; an acceptance of science as a core issue rather than an optional extra; and an increase in the number of science students who are "fascinated by the intrinsic awesomeness of science".

Whether they go on to become scientists after graduating is less important. "They can go and work in a bank and be awesome there – but they will be infiltrating all segments of the economy," says Chubb.

A solid STEM foundation and industry-research collaboration will be essential if Australia and Australian industry is to become seriously, strategically and internationally engaged he argues.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.30

It's a long way from Menzies Creek and Mr Honey. "As you grow up some interests increase more than others. I was interested in how biology worked and when I think back on it, which I haven't before this moment, it was when the teacher sent us out to look at butterflies, worms and cicadas.

"The teacher had to teach six classes in one room. While he was teaching other grades he would set us a task. If you did it well you were given a pencil. If you did it really well there was a pencil with an eraser. People like me wanted the one with the eraser."

Talking to Professor Chubb today it's clear that he wants the pencil with the eraser not just for himself – but for the nation.

Cite this article as: Head, Beverley. 2014. "STEM education and innovation are essential for national success': A profile of Australia's Chief Scientist, Ian Chubb'. ***Australian Journal of Telecommunications and the Digital Economy*** **2 (1): 30.1-30.6. DOI: http://doi.org/10.7790/ajtde.v2n1.30. Available from: http://telsoc.org/journal**

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.30

How 5G will be different

Stuart Corner
Freelance writer

Mobile telecommunication services incorrectly branded '4G' are now widely available. By contrast future mobile technology, dubbed 5G, has already received coverage in the mainstream press, but does not yet exist. This article will summarise the 'state of play' in 5G by reviewing the requirements that are driving its development, the performance targets it is aiming for and the technologies being explored to achieve these. It will also examine the major collaboration initiatives that have been created to progress development towards universally accepted standards. Finally, it will look at what 5G services are expected to offer from the users' perspective.

Introduction

Most users of mobile phones in Australia probably know that the latest and greatest mobile technology is '4G'. They might even have heard of the next evolution of mobile technology '5G' which has already made headlines in the mainstream press, even though it is some years from becoming a reality.

So where does the marketing hype around 5G end and the technical reality begin? This article will attempt to answer several questions about 5G: Why do we need it? What technologies will it embody? How will it be developed? What user benefits will it bring?

Why we need 5G

There is almost universal agreement amongst vendors and carriers that mobile technologies beyond 4G/LTE-A will be needed, and needed soon. The mobile industry has been a victim of its own success. The multimegabit mobile data bandwidths that have been available since the introduction of high speed packet access (HSPA), coupled with increasing functionality in smartphones and tablets, have fuelled growth in demand for speed and capacity in mobile networks that shows no signs of abating.

Nokia Siemens Networks (now Nokia Solutions & Networks, NSN) in 2011 produced a white paper '2020: Beyond 4G Radio Evolution for the Gigabit Experience' (NSN 2011). There was no mention in it of 5G, but it said: 'Extrapolations of current growth trends predict that networks need to be prepared to support up to a thousand-fold increase in total mobile

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

broadband traffic by 2020…[assuming] a ten-fold increase in broadband mobile subscribers and up to 100 times higher traffic per user (beyond 1Gbyte/sub/day)'.

It suggested that this would be achieved by increasing the number of base stations ten-fold, increasing spectral efficiency ten-fold and increasing the available spectrum ten-fold. All this, it said, would need to happen without mobile operators gaining significant revenue increases. Clearly no one is going to pay 1000 times more for their mobile service than they pay today. Therefore the cost per bit will have to come down about 1000-fold over the same period!

By 2020 also the mix of connected devices will also have shifted significantly. The population of personal communications tools like smartphones and tablets will have been overtaken by 'the Internet of Things' (IoT): a huge variety of devices from wearables to connected cars. According to research firm Gartner (2013), IoT - which excludes PCs, tablets and smartphones - will grow to 26 billion installed units in 2020, representing an almost 30-fold increase from 0.9 billion in 2009.

While many of these devices may not be heavy users of bandwidth, the sheer volume of them will impose a significant signalling load on the networks to which they are connected. It is envisaged that 5G networks will have to handle millions of 'always on' devices in a single cell and devices for which the signalling traffic will consume almost 100 percent of the citation provided bandwidth they use.

What technologies will 5G embody?

Today's 3G and 4G networks were conceived primarily to serve one sort of device: the mobile phone, or a modem that was functionally identical to the data communications capability of the phone. 5G networks will need to serve many different types of devices with widely different requirements and therefore will not adopt a 'one technology fits all' solution.

According to an Ericsson White Paper (2013), today's wide area technologies will continue to evolve to deliver enhanced system performance and more capabilities, but they will be complemented with other technologies for particular use cases that they are ill-suited to addressing. Ericsson says that 5G will be 'a set of seamlessly integrated radio technologies' and that the evolution of LTE will be fundamental to this future, as will the evolution of HSPA and Wi-Fi.

To support the expected orders of magnitude increase in device numbers, base station densities will have to increase massively. Ericsson and other vendors foresee indoor deployments with access nodes in every room and outdoor deployments with access nodes at

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

lamppost distance apart. These devices will have transmission bandwidths possibly of several gigahertz and will operate at frequencies as high as 100GHz.

They are likely to use radio access technologies quite different from those in the macro networks, but will nevertheless be tightly integrated with those macro networks.

Today's cellular networks 'trombone' all traffic to a central switch, even between devices in close proximity. This mode of communication will be neither appropriate nor practicable for communications functions that are primarily only invoked when devices are co-located. However unlike today's short-range communications technologies – bluetooth and Wi-Fi – in 5G this device-to-device communication will use licensed spectrum and will take place under network control to ensure that performance and reliability requirements can be met. LTE standards are already evolving to cater for device-to-device communications.

Additional spectrum alone is not expected to satisfy the ever-increasing demand for bandwidth. Communications capacity will be further increased by increasing the number of antennas on transmitters and receivers to create more signal paths, by exotic advanced modulation techniques and by full duplex communications technologies in which the same spectrum is used simultaneously for transmit and receive functions. (Today's cellular technologies either use different frequencies for transmit and receive or transmit and receive on the same frequencies at different times).

According to a recent ZTE White Paper (2014) research is focussed on new coding and modulation schemas and multiple access techniques. In the area of multiple access, major research efforts include NOMA (non-orthogonal multiple access) and FTN (Faster-Than-Nyquist). Research on receivers has focused on the development of new waveforms that support MIMO (multiple-input and multiple-output), and full duplex techniques with shortened TTl (transmission time interval) radio links. Other new techniques such as software-defined air interface are expected to enable future networks to use multiple radio access technologies and multiple frequencies simultaneously.

These disparate radio technologies, the need to support many different types of devices - including devices that communicate directly with each other but under network control - and the need for a network that is 'user aware' will place massive demands on the core switching and processing resources of future networks. The new technologies of software defined networking and network functions virtualisation will be called on to meet these demands and networks will transition to an intelligent cloud architecture.

This network cloud will coordinate the disparate types of network resources, manage inter-radio access technology, inter-frequency and inter-site radio access and interference cancellation to deliver improved network performance, especially at the cell edge.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

Intelligent cloud technologies will also be needed to provide spectral agility for 5G networks. Work is already underway on global harmonisation of future mobile spectrum, but the regional diversity of LTE spectrum – there are more than a dozen different bands – shows just how hard this will be (Wikipedia 2014).

According to Huawei (2013), to maximise spectrum efficiency, spectrum access and programmable air interface technologies will be needed that are capable of mapping service requirements to the best suitable combinations of frequency and radio resources. The continuing deep integration of SDN and cloud architecture technologies will help realise this, Huawei suggests that these technologies will: facilitate the on-demand customisation of mobile networks to ensure QoS, reduce energy consumption and enable operators to maximise the value of their network investments

Much of the focus of 5G research is on reducing latency and while latency will clearly always be limited by the speed of light, this only becomes significant when accessing distant resources (light travels about 300km in one millisecond); many of the applications envisaged for 5G will operate over much shorter distances, so the limiting factors will be network switching and processing times.

Huawei talks of 'faster than thought' speeds (ie minimal latency), so fast that 'the apparent distance between connected people and connected machines will shrink to a virtual "zero distance" gap.' It suggests that 'instant immediacy' in mobile services will support the proliferation of whole new set of mobile apps that push the capabilities of communications beyond what is currently possible.

How is 5G being developed?

Despite the countless adverts for '4G' mobile phones and services there are very few 4G mobile networks in commercial operation. Long Term Evolution (LTE), the technology now almost universally referred to as '4G', is no such thing according to the official rankings of mobile technologies. That term is reserved for LTE Advanced (LTE-A).

The marketeers managed to blur the boundaries between 3G and 4G and sow confusion. They are likely to do so to a greater extent with 5G because, unlike the definition of LTE-A as 4G, there is yet no clear and unambiguous definition of a standard for 5G, only a general consensus on its required performance, some of the technological advances that will be needed to achieve that performance and the functionality it will be required to deliver. The general view seems to be that commercial 5G networks will start to appear around 2020.

Nevertheless the marketeers are already on the 5G bandwagon, seeking the kudos of 5G leadership. One of the first was Samsung. On 13 May 2013 the company issued a press

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

release claiming that it had successfully developed technology that 'sits at the core of 5G mobile communications system and will provide data transmission up to several hundred times faster than current 4G networks.'

As a PR exercise it was hugely successful. A Google search on '5G' and 'mobile' made shortly after the announcement produced a near monopoly of references to Samsung in the top 100 hits.

ITU: from 3G to 5G

The ultimate arbiter of 3G and 4G mobile technology standards to date has been the International Telecommunication Union (ITU). It has developed sets of requirements for mobile telecommunications systems since the 1970s, and then approved technologies and standards developed by other organisations that met these requirements, along with the frequencies in which these operate.

Thus in 1998 the organisation announced that it was 'working on one of its most ambitious projects ever: a federation of systems for third generation mobile telecommunications that will provide wireless access to the global telecommunication infrastructure . . . coined IMT 2000 [that] will make it possible to communicate anywhere-anytime offering a seamless operation of mobile terminals worldwide'.

Over the next decade technologies were developed, submitted to and accepted by the ITU as meeting the requirements of IMT-2000 (International Mobile Telecommunications 2000) and those technologies are what we know as 3G today.

In 2003 the ITU initiated the next phase in the evolution of mobile technology, in Recommendation ITU-R M1.1645, 'Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.'

That set of requirements became known as IMT-Advanced and the ITU announced in October 2010 that 'LTE-Advanced and WirelessMAN-Advanced [have been] accorded the official designation of IMT-Advanced, qualifying them as true 4G technologies' (ITU 2010). In can be argued that WirelessMAN-Advanced was an evolution of the earlier IEEE802.16 WiMax technology and has gained very little market traction compared to LTE-A.

The ITU is adopting a similar approach for 5G but, given the number of other initiatives already underway and the ITU's relatively late start, it seems unlikely that it will play such a central role.

ITU Working Party 5D is developing a new Recommendation ITU-R M [IMT.VISION] 'Framework and overall objectives of the future development of IMT for 2020 and beyond'

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

that the ITU says 'will help encourage and guide industry and administrations in further development of IMT for 2020 and beyond.'

In a liaison statement to external organisations, issued in February 2013, the ITU said: 'The scope of this Recommendation will focus on what the roles of IMT will be and how IMT can better serve society in the future, and the framework and overall objectives of further development of IMT for 2020 and beyond. It will be based on global market, technology and spectrum trends, including user demand for mobile broadband communication services, new service applications and the needs of developing countries'

The ITU plans to stabilise the document in early 2015 and to capture the current perspectives of the industry on the future vision it called on external organisations to submit material no later than the 18th meeting of WP 5D, but preferably earlier. That meeting was held in Vietnam in mid February 2014.

Asian players on the rise

The ITU's role aside, the evolution of 5G will be significantly different from that of 3G and 4G thanks to the rising power of Asia, particularly China, both as a market and as a source of technology.

Research firm IHS (2014) has forecast that 4G (LTE) smartphone sales in China in 2014 will be around 72 million units, 16 times greater than in 2013, and will reach 300 million by 2018. And IDC (2014a) on 29 January forecast there would be a total installed base of 1.4 billion 'smart connected devices' in China by the end of 2017.

Chinese telco equipment maker Huawei – which announced on 6 November 2013 (Huawei 2013a) that it would invest a minimum of $US600 million in research and innovation for 5G technologies by 2018 - in mid-2012 overtook Ericsson, the world's then-largest telecom vendor in terms of revenue (Le Maistre 2012).

Huawei, Ericsson and all the other major vendors will be devoting considerable R&D resources to 5G wireless but standardisation will only be achieved by their participation in organisations like the ITU that foster the co-operation needed to bring their different ideas together. There are several significant initiatives underway.

China, Japan and Korea

Confusingly what looks like it should be the name of the ITU's 5G project, IMT-2020, is actually a Chinese initiative. According to China's Future Mobile Communications Forum, (FMCF 2013) in February 2013, China's Ministry of Industry, Development and Reform Commission and its Ministry of Science jointly set up the IMT-2020 (5G) advance group to

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

build a 5G technology research and standard promotion platform. An IMT-2020 5G Vision Summit was held in May.

At the same time a similar initiative was underway in South Korea. According to the Korea IT Times, its members are the Electronics and Telecommunications Research Institute (ETRI), major telcos, SK Telecom, KT, LG Uplus and major electronics companies, including Samsung Electronics, LG electronics, KMW and Dio Interactive (Korea IT Times 2014).

MSIP expects the 5G Forum will perform as the initiator of global cooperation, and will propose the formation of Asian Council to lead the international standardisation of 5G technology,' the report said. China and South Korea lost no time in trying to take global leadership in 5G standardisation. The two formed in July 2013 a partnership to set global standards for 5G. According to iTersNews (2013) during Korean President Park Geun-hye's state visit to China, Korea's 5G Forum and China's IMT-2020 Promotion Group signed a MoU, to co-operate on 5G technology standardisation, research projects and 5G spectrum resources.

Yoon Jong-lok, South Korea's vice-minister with the Ministry of Science, ICT and Future Planning (MSIP), told a press briefing: 'We hope that Korea and China would become an epicentre of 5G technology to open up fresh huge market opportunities around [the] Yellow Sea, the most densely populated region.' However he said other organisations were welcome to join their effort.

Meanwhile Japan kicked of its national 5G research initiative, ARIB 2020, in September 2013 and in December South Korea, China and Japan joined forces on 5G standardisation, according to a report in Korea's etnews.com (etNews 2013).

UK creates 5GIC

In the UK, 5G research is centred on 5GIC, an initiative of the Centre for Communication Systems Research (CCSR) and the University of Surrey that started in October 2012 with an announcement (University of Surrey 2012) that CCSR and the University had secured £11.6m of UK Government funding for the centre and expected to receive a further £24m from industry participants.

The organisation was formally created in November 2013 when the list of participating organisations that had contributed more than £30m was given as: Aeroflex, AIRCOM International, BBC, BT, EE, Fujitsu Laboratories of Europe, Huawei, Ofcom, Rohde & Schwarz, Samsung, Telefónica and Vodafone (University of Surrey 2013).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

A new purpose built facility to house the 5GIC is being built on the University of Surrey's main campus. It is expected to be completed in January 2015 and will be home to 150 researchers and around 100 PhD students.

EU's 5G PPP and METIS 5G initiatives

On 17 December 2013 the European Commission announced (EC 2013) 5G PPP: Advanced 5G networks for the Future Internet (5G), one of eight new public private research partnerships. It aims 'to stimulate the development of network internet infrastructure to ensure advanced ICT services for all sectors and users.'

The EU will invest around €700 million in the 5G PPP by 2020 and expects this to be matched by the private sector partners in the venture.

This is not the first EU backed initiative on the 5G front. On 27 November 2012 the EU launched METIS (Mobile and wireless communications Enablers for the Twenty-twenty Information Society), a consortium of 29 partners spanning telecommunications manufacturers, network operators, the automotive industry and academia. Its aim is "to respond to societal challenges for the year 2020 and beyond by laying the foundation for the next generation of the mobile and wireless communications system."

METIS is co-funded by the European Commission as an Integrated Project under the Seventh Framework Programme for research and development (FP7). It will receive €16 million ($A24m) of its €27 million ($A41m) budget from the EU.

METIS brings together the biggest mobile infrastructure vendors - Alcatel-Lucent, Ericsson, Huawei, Nokia and Nokia Solutions & Networks (Nokia Siemens Networks at the time) - along with major carriers Deutsche Telekom, Docomo, Telecom Italia and Telefónica, motor manufacturer BMW and numerous academic institutions.

The main objective of METIS is to lay the foundation for, and to generate a European consensus on, future global mobile and wireless communications system. In a press release the EU said: 'The METIS overall technical goal is to provide a system concept that supports: 1000 times higher mobile data volume per area: 10 times to 100 times higher number of connected devices; 10 times to 100 times higher typical user data rate; 10 times longer battery life for low power machine-to-machine-communications; five times reduced end-to-end latency.'

Metis' specific goals are much more modest. It aims to 'provide valuable and timely contributions to pre-standardisation and regulation processes, and ensure European leadership in mobile and wireless communications.' It hopes to achieve these goals by April

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

2015 when it is scheduled to be wound up, leaving further work to established standardisation and regulatory bodies.

Intel leading US 5G co-operation

In contrast to the activity in Europe and Asia, 5G research co-operation in the US appears to be minimal and lead not by any government body but by one company, Intel.

Intel's initiative is modest ($US3m only) and appears to be the only one of its kind (Gigacom 2013). Moreover, Intel seems to be keeping its initiative fairly low-key. The only information it has put out is two blog posts, one short post (Intel 2013a) in July 2013 announcing the initiative, and a second with rather more detail (Intel 2013b) that lists the goals of the project.

Intel said it would invest at least $US3 million to support wireless research at more than 10 universities around the world including Stanford University, ITT Delhi and Pompeu Fabra University in Barcelona. Research topics will include how to improve quality of service via context awareness, wireless device power efficiency and enabling new radio spectrum.

The initiative, named as an Intel Strategic Research Alliance, includes industry partner Verizon, but Intel has given no details of Verizon's involvement.

The NGMN Alliance

The major mobile operators in February 2014 launched their own 5G standardisation initiative (ngmn 2014), through the Next Generation Mobile Networks (NGMN) Alliance, a body formed by a group of international network operators in 2006 that has to date been focussed on LTE standardisation.

The NGMN said that its board – CTOs from 19 leading international operators – has made a decision to focus the future NGMN work programme on defining the end-to-end requirements for 5G, in recognition of the fact that the scope of 5G extends significantly beyond the radio access layer.

It said the initiative would deliver key operator requirements to guide the development of future technology platforms and related standards, create new business opportunities and satisfy future end-user needs. It intends to work in close collaboration with all industry partners and other relevant initiatives and within the well-established NGMN processes.

The first major outcome will be an industry white paper to be delivered before the end of 2014 to support the standardisation and subsequent availability of 5G from 2020.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

The Wireless World Research Forum

Another inhabitant of the 5G ecosystem is the Wireless World Research Forum (http://www.wwrf.ch/) whose stated goal is 'to encourage research that will achieve unbounded communications to address key societal challenges for the future.' It has been in existence since 2001 and claims to be 'the unique forum where the wireless community can tackle the key research challenges.'

It lists its steering board as being: Alcatel-Lucent France; China Mobile; DoCoMo Eurolabs; Huawei Technologies; Nokia and Nokia Siemens Networks (now Nokia Systems and Networks). Otherwise, its membership is not made public. According to its LinkedIN profile (http://www.linkedin.com/company/wireless-world-research-forum) it has over 140 members from five continents, representing all sectors of the mobile communications industry and the research community.

It does not appear to have any formal role in the evolution of 5G standards but says: 'By searching out the issues, flagging them up to opinion leaders, and then working with our liaison partners, and you, to deal with them, we drive the development of the Wireless World.'

It has produced a series of white papers (see http://www.wwrf.ch/outlook.html) on various aspects of future wireless technologies under the umbrella title of 'Visions and research directions for the Wireless World.'

What will 5G mean for users?

This is perhaps the most intriguing question of all. Apart from the introduction of video calling and multimedia messaging in 3G, from the user's perspective the evolution from 2G to 4G has been all about speed – increased downstream, and upstream, bandwidths that have enabled mobile networks and devices to offer a whole gamut of appealing content and services – accompanied by significant reductions in costs per Gigabyte that have made these services affordable.

Other significant improvements in the transition from 3G to LTE have been greatly reduced latency, high definition voice and the introduction of end-to-end IP in the transition from 3G to LTE.

Much higher bandwidths and further reductions in latency are being bandied about by the promoters of 5G. South Korea has mentioned a goal of 1Gbps for its first 5G trials in 2017. Huawei says: 'a 10Gbps individual user experience . . . will emerge between 2020 and 2030' (Huawei 2013). By contrast, LTE-Advanced, which is already in commercial operation, has a theoretical maximum downstream bandwidth of 3Gbps.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

NTT Docomo claims to have already demonstrated 10Gbps uplink bandwidth in December 2012 using 400MHz of bandwidth at 11GHz from a moving vehicle (the transmission distance was not specified). It also suggests that latency will be reduced to 1mS from the 5mS of LTE.

Some 5G researchers have ambitions well beyond 10Gps: infinite capacity, or at least the perception of it. This is the stated goal of the UK's 5GIC research centre at the University of Surrey. According to Rahim Tafazolli, head of the University's Centre for Communication Systems Research, a rate that is always sufficient to meet the user's needs would create the perception of infinite capacity.

There has to date been relatively little discussion about the economic benefits that might accrue from widespread deployment of 5G. A 2012 study undertaken by Deloitte and the GSMA (Deloitte 2012) concluded that a doubling of mobile data use would lead to an increase of 0.5 percentage points in the GDP per capita growth rate across the 14 countries studied and that countries with a higher level of data usage per 3G connection had seen an increase in their GDP per capita growth of up to 1.4 percentage points.

The most intriguing suggestions about what 5G will mean are not directly related to speed and latency, nor to economic benefits but rather centre on an as yet only vaguely defined idea of network intelligence. Tod Sizer, wireless research leader at Alcatel-Lucent's Bell Labs, in a blog post points out that, by the time 5G arrives, it is likely that fixed line telephony will be just about dead and that 5G will be 'THE communication of the future and not just the wireless radio solution' (Sizer 2014). Therefore, he says: 'There are two major improvements that we need to bring to communications: flexibility to tailor the network to the application, the person, where they are, and what their needs might be; and to optimise the full end-to-end performance between a user and the person or application with which they are communicating.'

A child of today, in her twenties in the next decade, will, he says, expect 'a network that adapts to her, rather than forcing her to adapt to the network, and with a performance that is seamless and always meets her expectations, wherever she happens to be.'

His colleague Michael Peeters, CTO of Alcatel-Lucent's Wireless division, put this another way (in conversation with the author in November 2013). 'Today the end user adapts to the service that is available. For me 5G is exactly the other way round. The communication service will adapt to what the user needs. Having the network figure out what you are doing and adapting is the grand vision for 5G.'

ZTE (2014) expresses a similar view but in a more technology-oriented way: 'Research on 5G will be focused on user experience, rather than simply increasing network capacity. … In

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

order to deliver improved user experience, 5G researchers need to develop new user-centric service provisioning models that are informed by usage and service patterns. Acquiring deeper insights about users will enable researchers to formulate key performance indicators (KPls) for 5G networks that will drive order-of-magnitude improvements in network capacity, bandwidth maintenance, peak data rate, latency reduction and high-accuracy indoor location monitoring. ... Users will expect consistent on-demand access to services including office applications, social networking tools, e-commerce and online financial services platforms.'

The marketeers are clearly going to have a field day with this. In fact they already have. This quote is from a videoproduced by US telco Sprint:

> *'Where is the smart network? The network that is constantly acting and reacting, customising and tailoring itself to each person engaging with it. A network that is self-aware, that is sentient adjusting millisecond by millisecond to the microdemands of all the people tapping in to it... [A network] that automatically [knows] how to maximise the experience for everyone and every thing using it.'* (Sprint 2013)

Trouble is, this is not a vision of the future but a promotion for Sprint's LTE network, Spark, being rolled out today!

Conclusions

The essential differences between the capabilities of 5G, compared to those of the previous generations of mobile network technology, are contrasted in Table 1.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

Table 1 – Comparison of 5G with previous generations of mobile network technology. (Source: Ericsson)

Generation	Theoretical maximum downstream data speeds	Latency*	Technology	Years of introduction (approx.)	Key features
1G	-	-	AMPS, NMT, TACS	1980-1990	Voice or slow data using voice channel modems.
2G	14.4kbps	-	GSM, D-AMPS, CDMA	1990-2000	Narrowband data using the voice circuit + SMS text messaging
2.5G	114kbps	~700mS	GPRS	2001-2004	Addition of packet data enables phones to be used for web browsing, but latency is very high
3G	31.Mbps peak	200 - 400mS (edge) ~120mS (WCDMA)	CDMA2000 (1XRTT, EVDO) UMTS (WCDMA) Edge	2004-2006	Videocall and multimedia message support
3.5G	168Mbps (dual carrier HSPA+)	60-80mS	HSPA, HSPA+	2006-2010	Data is IP end to end
3.9G	300Mbps	~10mS	LTE, WiMAX	2009 --	LTE boost speeds, spectral efficiency, reduces latency.
4G	3Gbps	<5mS	LTE-A, WiMax 802.16m	2013 --	LTE-A uses spectrum aggregation and other techniques to increase bandwidth.
5G	10Gbps (maybe)	~1mS	Evolution of LTE-A, others to be determined	2020 (Maybe)	5G will use multiple radio access technologies for different use cases.

* Latencies are approximate times for network switching and routing and do not include distance-based propagation delays.

Frequency usage is a different matter. 5G is much less confined to particular bands of radio spectrum than its predecessors. Figure 1 (courtesy of Ericsson) shows which different bands of frequencies are likely to be utilised by 5G, from 300 MHz to 300 GHz, in different service applications.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

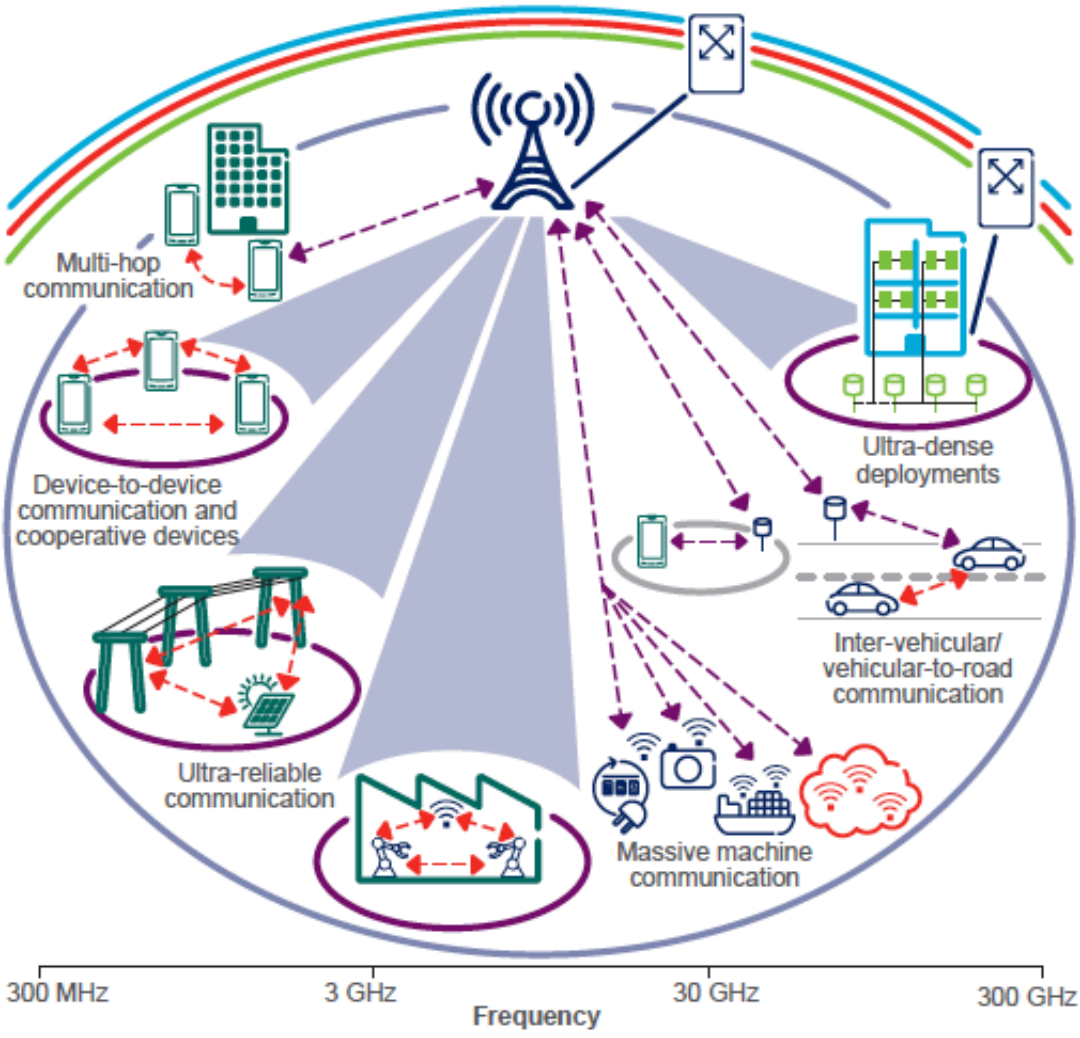

Figure 1 – 5G will use a variety of different radio access technologies across a broad range of frequencies to cater for many more device types and many different use cases. Source: Ericsson

It's clear that the evolution of mobile technologies is accelerating. Korean telco SK Telecom is credited with being the first to launch a true commercial 4G (ie LTE-A) mobile service, in June 2013 (Telecompaper 2013). That was 10 years after the ITU kicked off its 4G standards initiative and just under three years after the standards were finalised.

The industry is talking of having commercial 5G networks in operation in six years, and there are no standards yet in sight. Also, arguably, the technology advances needed to achieve the goals of 5G will be greater than those that underpinned the evolution from 3G to 4G.

In other words, while 5G might seem to be too far in the future for anyone outside of its narrow specialism to be giving it much attention, that situation will change within a couple of years.

If all goes to plan the mobile industry will deliver the super-smart 5G network with near-zero latency and 'infinite' capacity that adapts to the users' needs, but it will most likely be entrepreneurial and creative individuals who come up with ways to exploit these features,

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

grow new industries and disrupt others. So it's probably not too early for some of the thinking behind 5G to be reaching a wider audience.

It's possible that the industry will fail to achieve the technical goals it has set for 5G but also a failure to achieve consensus on standards would be a significant setback.

Already two camps are emerging: one Asia-based and one Europe based with the global vendors in both camps. Ideally these will come together to create truly global standards, minimising costs through larger volumes and maximising the rate of innovation.

However markets in Asia will be large enough to 'go-it-alone', and they have done so in the past. Japan had its own 2G standard, PDC, which at its peak had 80 million users (Wikipedia 2014b). China developed its own 3G technology, TD-SCDMA, with some success. It was adopted by the dominant 2G era operator, China Mobile, which by early 2013 had 100 million users. However this technology choice has been blamed for the loss of its market lead over other telcos that had adopted the global 3G standards (techinasia 2013).

References

Deloitte 2012. Press Release November 20, 2012. GSMA and Deloitte Release Comprehensive Research into the Impact of Mobile Telephony on Economic Growth' Available at: http://www.gsma.com/newsroom/gsma-and-deloitte-release-comprehensive-research-into-the-impact-of-mobile-telephony-on-economic-growth/

EC 2013. Eight contracts to sustain European SMEs. Available at: http://www.europarlamento24.eu/eight-contracts-to-sustain-european-smes/0,1254,107_ART_5231,00.html

Ericsson 2013. Ericsson White Paper. June 2013. "5G Radio Access". Available at: http://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf

etNews 2013. The CJK triangle-formation leads the 1,000 times faster 5G. 03 Dec 2013. Available at: http://english.etnews.com/communication/2878780_1300.html

FMCF 2013. China's Future Mobile Communications Forum. 03 June 2013. **5G** Communications Technology Outlook. Available at: http://www.future-forum.org/en/onews.asp?id=4113

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.28

Gartner 2013. 'Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020', 12 December 2013, Available at http://www.gartner.com/newsroom/id/2636073

Gigacom 2013. '4G didn't pan out for Intel, so now it's looking ahead to 5G." 09 July 2013. Available at: http://gigaom.com/2013/07/19/4g-didnt-pan-out-for-intel-so-now-its-looking-ahead-to-5g/

Huawei 2013a. 'Huawei to Invest $600M in 5G Research & Innovation by 2018'. Available at: http://www.huawei.com/ilink/en/about-huawei/newsroom/press-release/HW_314871

Huawei 2013. *5G: A technology vision*, Huawei White Paper. Available at: http://www.huawei.com/ilink/en/download/HW_314849

IDC 2014a. Press Release 29 January 2014. 'IDC Top 10 Predictions on China Smart Connected Device (SCD) Market'. Available at: http://www.idc.com/getdoc.jsp?containerId=prCN24652114

HIS 2014. '4G smartphone market in China set for explosive 1,500% growth this year', 28 January 2014. Available at: http://press.ihs.com/press-release/design-supply-chain/4g-smartphone-market-china-set-explosive-1500-percent-growth-year

Intel 2013a. Chip Shot: Intel, Universities Explore 5G Wireless. Available at: http://newsroom.intel.com/community/intel_newsroom/blog/2013/07/18/intel-universities-explore-5g-wireless

Intel 2013b. Next Generation Wireless Communication (5G): Transforming the Wireless User Experience. July 15, 2013. Available at: http://blogs.intel.com/intellabs/2013/07/15/next-generation-wireless-communication-5g-transforming-the-wireless-user-experience/

iTersNews 2013. Korea, China Join Forces to set a global standard for 5G Mobile Technology". 05 July 2013. Available at: http://itersnews.com/?p=39694

ITU 1998. 'The ITU takes mobile into the Third Millennium'. Available at: http://www.itu.int/newsarchive/press/PP98/PressRel-Features/Feature4.html

ITU 2003. 'Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.' Available at: http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1645-0-200306-I!!PDF-E.pdf

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

ITU 2010. 'ITU paves way for next-generation 4G mobile technologies', 21 October 2010. Available at: http://www.itu.int/net/pressoffice/press_releases/2010/40.aspx#.Uu4pZv1Ym34

ITU 2013. 'Liaison statement to external organizations: Study on IMT vision for 2020 and beyond', 18 February 2013. Available at: https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=https%3A%2F%2Fmentor.ieee.org%2F802.16%2Fdcn%2F13%2F16-13-0044-00-WGLS-ls-from-wp5d-study-on-imt-vision-for-2020-and-beyond.docx&ei=jqD6UtnoNsb5kAWN24GIAw&usg=AFQjCNHTw6434Zyc6McYyIkUi1prgxNr2w&sig2=PAQk-XxYxJ9N2LlZaAwHhg

Korea IT Times 2014. The 5G Forum Launches Its Journey into the Era of Ultra-Connectivity. March 10th, 2014. Available at: http://www.future-forum.org/en/onews.asp?id=4113

Le Maistre, Ray. 2012. 'Hua.wei Snatches Ericsson's Crown'. lightreading.com. 24 July 2012. Available at http://www.lightreading.com/huawei-snatches-ericssons-crown/d/d-id/697230

ngmn 2014. Mobile Operators work together to define requirements for "5G" . Available at: http://www.ngmn.org/uploads/media/2014_02_24_NGMN_Press_Release_-_NGMN_Alliance_to_Deliver_5G_Operator_Requirements.pdf

NSN 2011. *2020: Beyond 4G Radio Evolution for the Gigabit Experience*' Henney, Sue. 2002. personal communication, at http://nsn.com/file/15036/2020-beyond-4g-radio-evolution-for-the-gigabit-experience

Samsung 2013. 'Samsung announces world's first 5G mmwave mobile technology', 13 May 2013. Available at: http://global.samsungtomorrow.com/?p=24093#sthash.OYeXRQxA.dpuf

Sizer 2014. 'What would our children want from 5G?' Available from: http://www.alcatel-lucent.com/blog/2014/what-would-our-children-want-5g

Sprint 2013 .Introducing: Sprint Spark" Available from: http://faster.sprint.com/feature_post/introducing-sprint-spark/

techinasia 2013. China Mobile Finally Has Over 100 Million 3G Subscribers". March 20, 2013. Available at: http://www.techinasia.com/china-mobile-has-100-million-3g-subscribers/) Ericsson. 2013. *5G Radio Access*, Ericsson White Paper, June 2013, at http://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.28

Telecompaper 2013. SK Telecom launches first LTE-A services. Wednesday 26 June. Available at: http://www.telecompaper.com/news/sk-telecom-launches-first-lte-a-services--951793

University of Surrey 2012. ccsr_welcomes_5g_innovation_centre_funding_success. Available at: http://www.surrey.ac.uk/ccsr/news/stories/ccsr_and_ee/2012/90980_ccsr_welcomes_5g_innovation_centre_funding_success.htm

University of Surrey 2013. Plans for 5g Innovation Centre in Surrey move on to the next level. 4 November 2013. Available at: http://www.surrey.ac.uk/mediacentre/press/2013/114833_plans_for_5g_innovation_centre_in_surrey_move_on_to_the_next_level.htm

Wikipedia 2014. 'LTE (telecommunication)'. 14 February 2014, at http://en.wikipedia.org/wiki/LTE_(telecommunication)

Wikipedia 2014b. Personal_Digital_Cellular. Available at: http://en.wikipedia.org/wiki/Personal_Digital_Cellular

ZTE 2014. *'5G: Driving the convergence of the physical and digital worlds,* White Paper on next generation mobile technology, *at* http://wwwen.zte.com.cn/en/products/bearer/201402/P020140221415329571322.pdf

Cite this article as: Corner, Stuart. 2014. 'How 5G will be different'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 28.1-28.18. DOI: http://doi.org/10.7790/ajtde.v2n1.28. Available from: http://telsoc.org/journal

Australian mobile broadband network performance

Mobile apps as one possible way to provide consumer information

Shara Evans
CEO, Market Clarity (www.marketclarity.com.au)

This paper explores the ways in which consumers gain information about mobile network performance and coverage, then examines the factors that impact mobile performance, and the challenges affiliated with representing results, which are highly influenced by transient events. The paper then discusses the role that mobile speed test apps and crowdsourcing initiatives can play in measuring mobile broadband performance, and provides an analysis of how the features and methodologies of eight major speed test applications compare and contrast. Lastly, the paper provides a brief review of the US Government's Broadband Mapping Program; and some closing thoughts on lessons for Australia, and in particular how a crowdsourcing initiative could complement the recently announced $100m Mobile Coverage Programme.

Introduction

The Australian Communications and Media Authority (ACMA) recently held a forum on mobile network performance (ACMA 2013), with the objectives of: gaining a better understanding of what is at the heart of consumer complaints about mobile network performance; identifying whether these issues are being sufficiently addressed; finding out what information helps consumers to understand providers' network performance; and, identifying whether current offerings meet consumer needs.

Consumers gain information about mobile network performance and coverage from a number of sources including personal experience, carrier maps, word of mouth (including social networks) and mobile performance applications.

Arguably, the most definitive source of mobile coverage and performance information is provided directly by mobile network operators. However, an examination of information provided by Australian operators shows that consumers are faced with three different kinds of map information when looking at Telstra, Optus and Vodafone service coverage maps. Let us first review the different kinds of information that mobile operators provide with their online mobile coverage tools.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Figure 1 presents a screenshot of Telstra's mobile coverage map (Telstra 2013). In this map, we see that Telstra uses colour coding to provide typical download speed ranges — for instance, 4G (dark blue) can range from 2 to 50 megabits per second (Mbps) downstream. That's quite a big range, but at least it is a range that consumers can relate to, perhaps not in technical detail, but it's commonly understood that 50 Mbps is a lot faster than 2 Mbps.

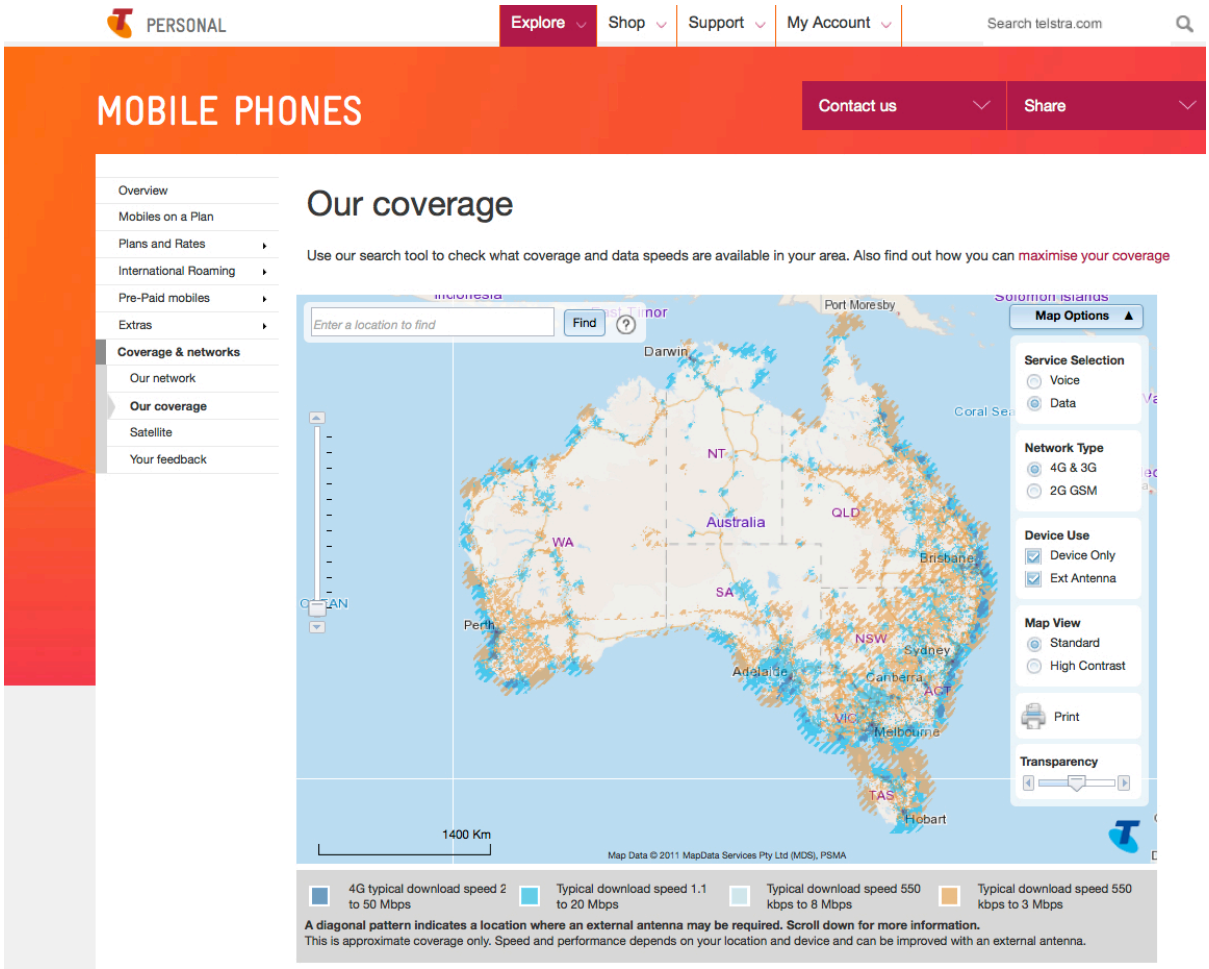

Figure 1 – Telstra Mobile Coverage Map (Feb 2014)

In the online map, Telstra provides typical download speeds ranging from a nationwide view all the way down to a street level view. However, the colour-coded speed ranges are quite large (especially with 4G connections) — meaning that a consumer isn't provided with information that would indicate an average download speed that would be experienced on a consistent basis. However, Telstra's mapping portal provides additional functionality, such as the ability to distinguish between 3G / 4G coverage versus 2G GSM coverage, the ability to view expected speeds with and without the use of external antennas, and to select between voice and data coverage.

Figures 2 and 3 present screenshots of Optus' mobile coverage maps (Optus 2013). Figure 2 shows Optus' 3G dual band, whereas Figure 4 shows 4G. In contrast with Telstra, Optus maps show technology available on an outdoor and antenna basis, as well as future coverage.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

However, typical speeds are not shown and Optus doesn't distinguish between voice and data coverage.

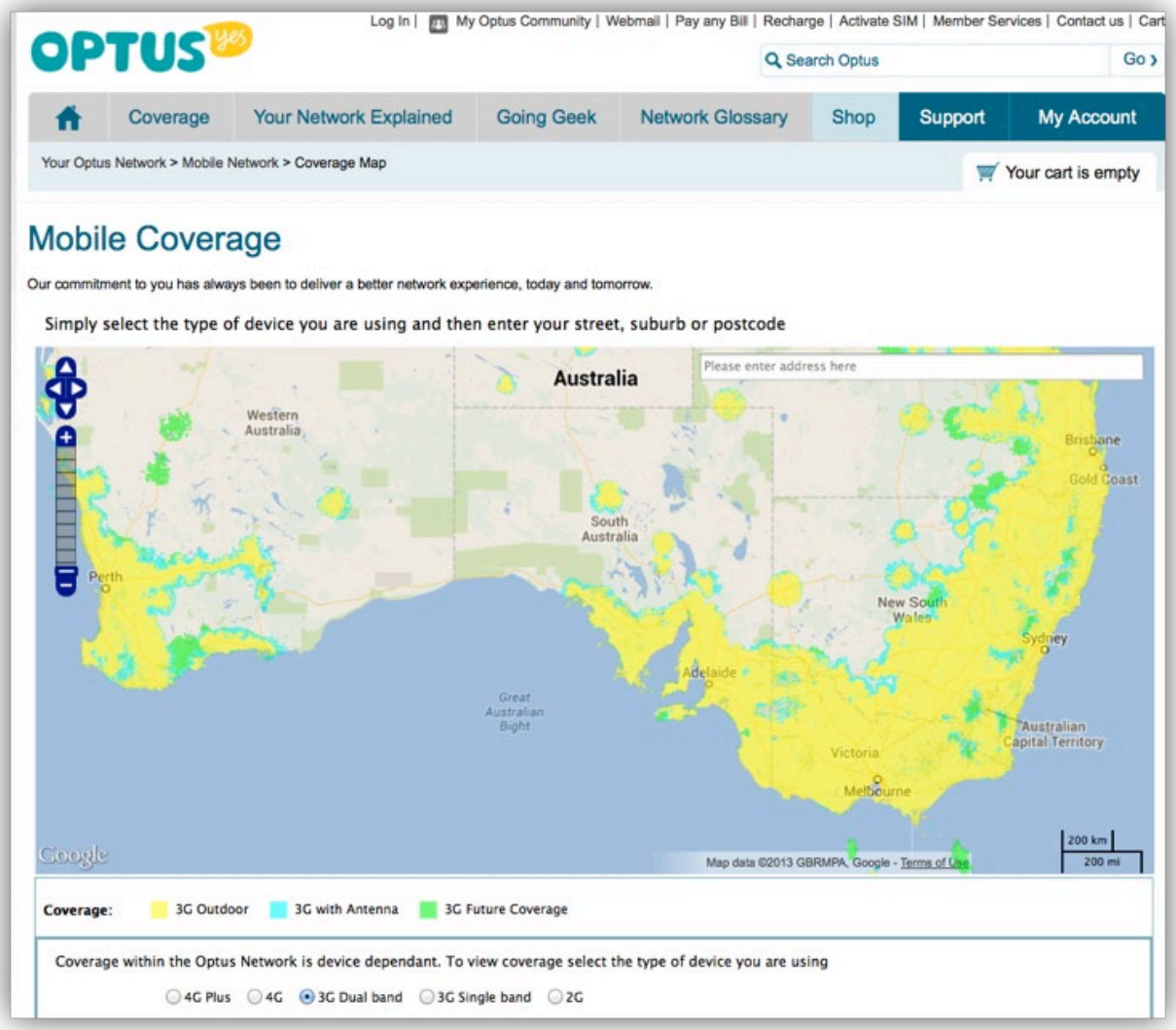

Figure 2 – Optus 3G Dual Band Mobile Coverage Map (Nov 2013)

A typical consumer is likely to have heard the terms 3G and 4G, but they probably don't understand all the nuances, especially with respect to expected broadband speed. Furthermore, the map assumes that consumers know the radio type (4G Plus, 4G, 3G dual band, etc) used within their device, which is required to select the correct map.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

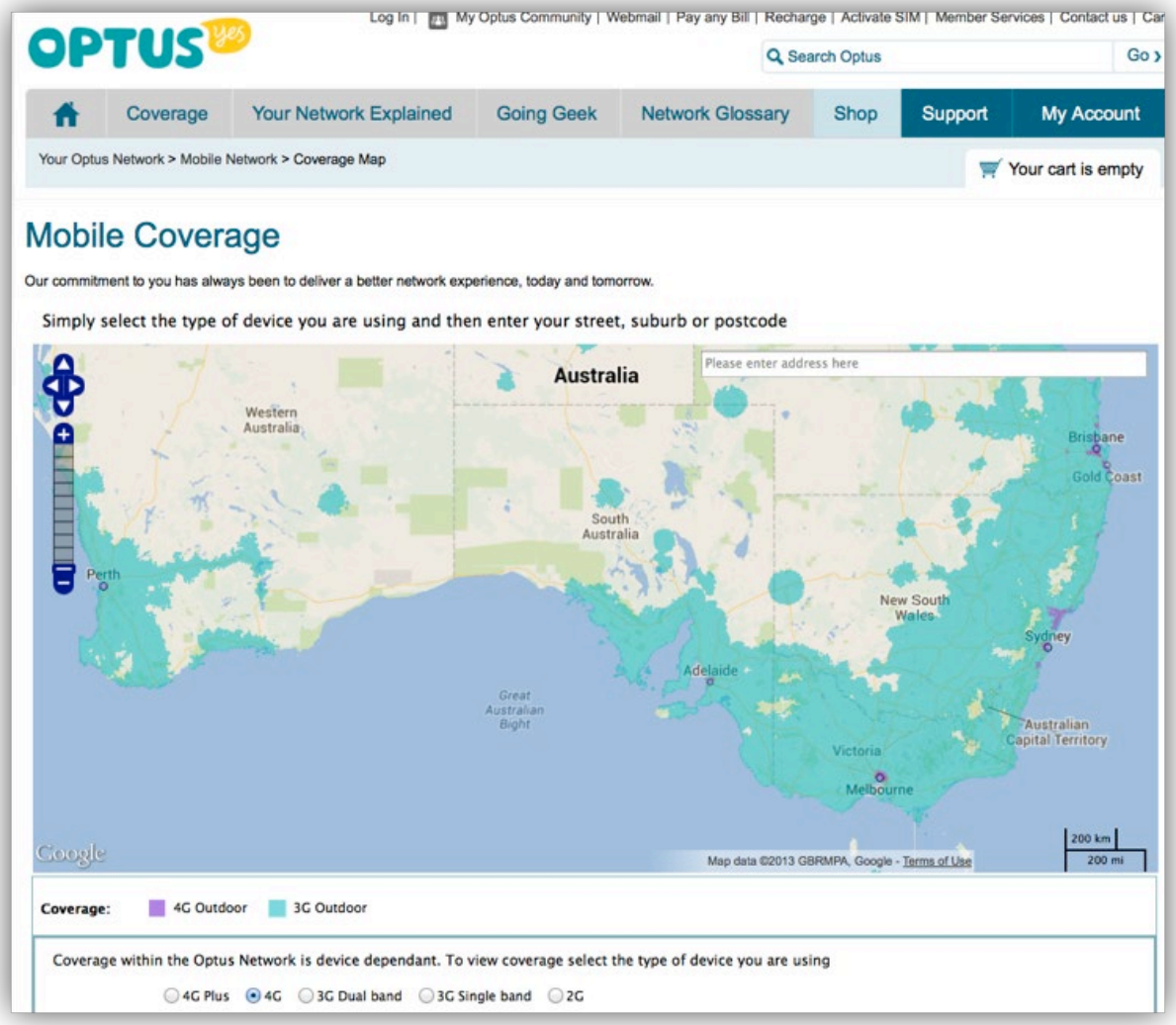

Figure 3 – Optus 3G/4G Outdoor Mobile Coverage Map (Nov 2013)

Figures 4 and 5 present screenshots of Vodafone's mobile voice and data coverage maps (Vodafone 2013). Vodafone voice maps show colour-coded call and text (voice) availability on an indoor and outdoor basis.

Vodafone allows users to toggle between voice and data coverage — providing results based on the specific type of device entered in a given query. This is particularly useful for examining data download speeds, as inherent device capabilities (such as being 4G capable) impact maximum expected speeds.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

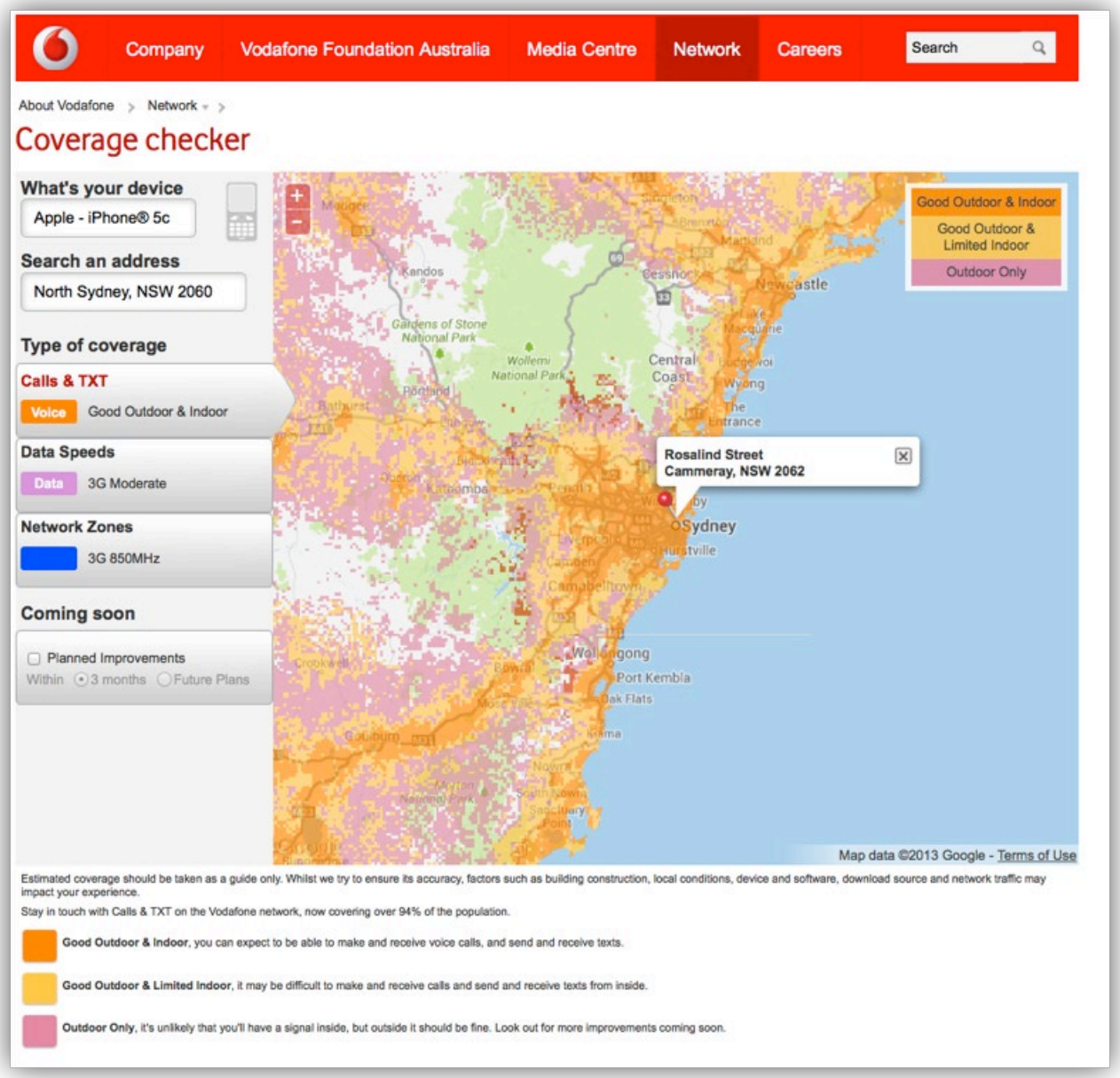

Figure 4 – Vodafone Mobile Voice Coverage Map (Nov 2013)

Data coverage maps provide colour-coded indications of 3G, 3G+ indoor and 4G indoor coverage, with explanatory notes for each technology's speed range. Similar to the Telstra maps, download speed ranges are quite large: for example the range for 4G services spans from 2 to 40 Mbps. However, Vodafone also provides information about average download speeds (for 4G, an average of 15 Mbps).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

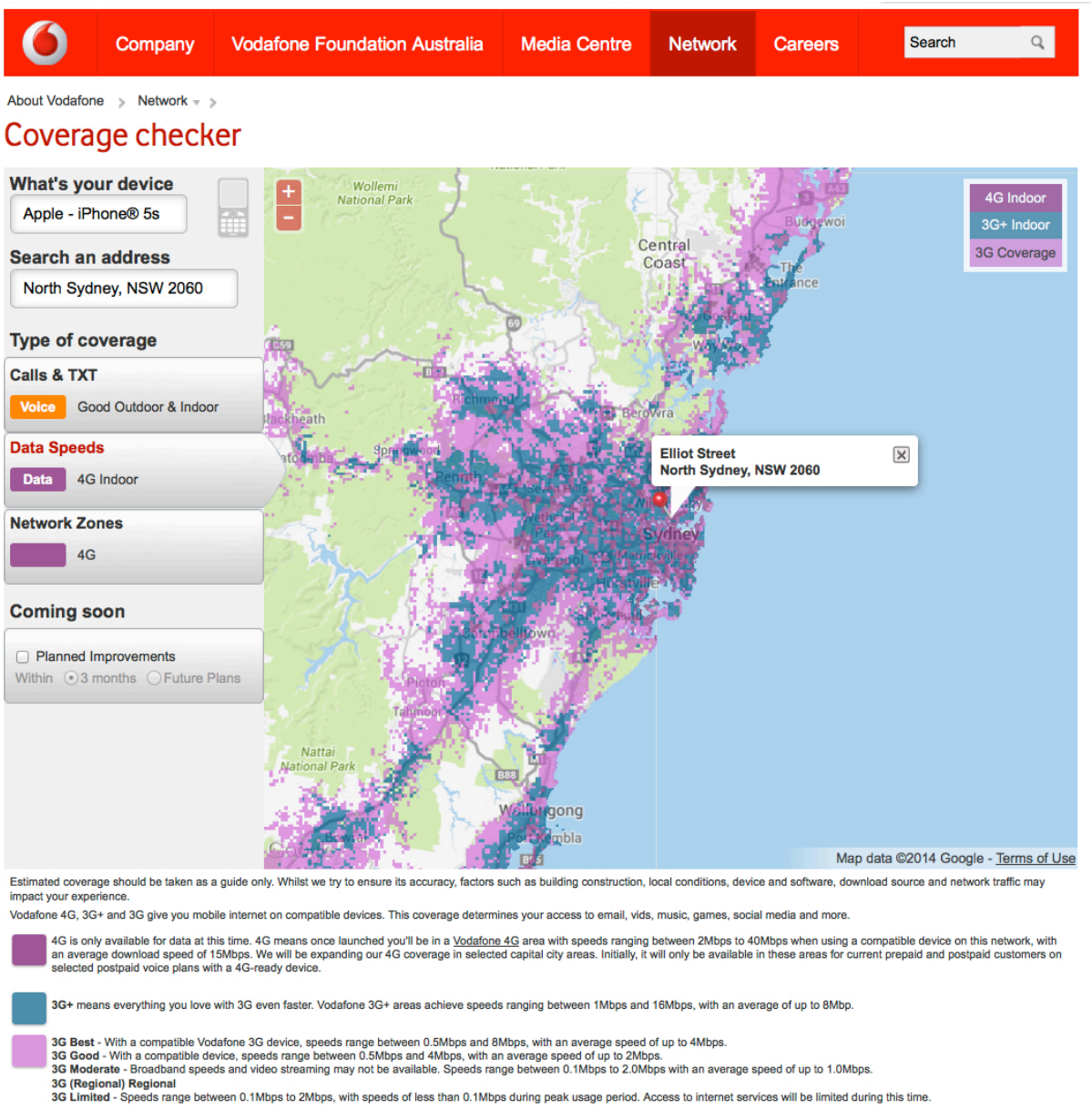

Figure 5 – Vodafone Mobile Data Coverage Map (Jan 2014)

So the consumer is faced with three different kinds of maps when they're looking at coverage and expected data download speeds for each mobile operator's service in Australia. This makes it difficult for consumers to directly compare carrier coverage and expected download speeds, and the maps don't provide any indications of upload speeds, which are increasingly important for many application. However, consumers can zoom down to address level, and get some good information.

Measuring Mobile Broadband Speed

When examining the issue of mobile broadband speed, there are a number of things to bear in mind.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

First, signal strength can fluctuate very, very widely depending on the number of people that are using the service at a particular point in time, interference, the time of day, what kind of handset someone is using (and how sensitive the antenna is), distance from a mobile base station (or repeater), whether the device is being used indoors or outdoors, handoff between cell coverage areas, how a carrier dimensions between voice and data — and a range of technical parameters.

Carriers and vendors routinely map expected mobile coverage based on a wide range of technical parameters including tower, and antenna information, frequency, transmit power, receiver sensitivity, and antenna gain and height. Signal propagation modelling also takes into account interferers such as terrain and vegetation features. It's quite a complex mathematical discipline and it certainly has a role in mapping, and in generating expectations of coverage, but is it the same as actual user experience? Is it precise enough to actually frame consumer expectations?

Would a better way of representing mobile broadband speed expectations be based on the actual speeds measured by end user devices? If so, one of the things to consider is how many tests are required in order to have a statistically valid sample. Is one drive test enough to inform consumer expectations? Are 10 drive tests enough? Are 100? How does that relate to a typical customer's experience? How well does the test sample reflect the variations in network conditions that occur throughout the day? Would it make more sense to enlist a large number of consumers to participate in a crowd sourcing speed test initiative?

Irrespective of the methodology used to determine typical mobile broadband speeds, how do you rank speed: what's fast, what's not fast?

In the US, the FCC has defined a range of bands for broadband downstream speeds (Western Telecommunications Alliance 2009). These bands apply equally to fixed broadband as well as mobile broadband, and they start with first-generation broadband spanning between 200 to 768 kilobits per second (Kbps), and go all the way up to what they call Broadband Tier 7, which is greater than 100 megabits per second (Mbps).

Mobile Pulse (Mobile Pulse 2014), one of the mobile performance app vendors that we'll be discussing below has used the FCC scheme as the basis for analysing and mapping mobile speeds — assigning A to F ratings (each with unique colour coding) to test results. In this schema, any result over 3 Mbps is consolidated into an A rating because this is roughly equivalent to a top-end 3G result. Mobile Pulse uses editable scales, so customers can define different scales to account for a mixture of 3G and 4G technologies. Table 1 provides examples of these grading scales.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Table 1 – Classifying Mobile Broadband Downstream Speeds

FCC Definition of Broadband	
Broadband Tier 7	Greater than 100 Mbps
Broadband Tier 6	25 Mbps to 100 Mbps
Broadband Tier 5	10 Mbps to 25 Mbps
Broadband Tier 4	6 Mbps to 10 Mbps
Broadband Tier 3	3 Mbps to 6 Mbps
Broadband Tier 2	1.5 Mbps to 3 Mbps
Basic Broadband Tier 1	768 Kbps to 1.5 Mbps
First Generation Data Tier	200 Kbps to 768 Kbps
Fails because it doesn't meet the lowest of the tiers	Below 200 Kbps

Mobile Pulse Speed Grades (3G)	
A	Broadband Tier 3 and above (3 Mbps and above)
B	Broadband Tier 2 (1.5 Mbps to 3 Mbps)
C	Basic Broadband Tier 1 (768 Kbps to 1.5 Mbps)
D	First Generation Data Tier (200 Kbps to 768 Kbps)
F	Fails because it doesn't meet the lowest of the tiers (Below 200 Kbps)
Failure	No data connection

Customer Speed Grades (3G/4G)	
A	10 Mbps and above
B	5 Mbps to 10 Mbps
C	2 Mbps to 5 Mbps
D	1 Mbps to 2 Mbps
F	Below 1 Mbps
Failure	No data connection

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Mobile Apps

Apps that run on smartphones and tablets — commonly referred to as mobile speed test apps — can be used to provide information about mobile network coverage and performance to consumers, service providers, policy makers and other interested parties.

Later in this paper, we discuss the methods and tools used by US State and Local Government organisations to test mobile performance. It is useful to briefly examine the mobile apps used by these organisations, many of which are also used in Australia:

- Ookla's Speedtest.net app (http://www.speedtest.net/), which runs on Apple, Android and Windows devices;
- RootMetrics (http://www.rootmetrics.com/), which runs on Apple and Android devices;
- OpenSignal (http://opensignal.com/), which runs on Apple and Android;
- Mobile Pulse (http://mobilepulse.com/), which runs on Apple, Android, BlackBerry and Windows;
- CalSPEED, which runs on Android devices (https://play.google.com/store/apps/details?id=gov.ca.cpuc.calspeed.android) and was custom-made for the California Public Utilities Commission (CPUC);
- SamKnows (https://www.samknows.com/), which runs on Apple and Android;
- Sensorly (http://www.sensorly.com/), which runs on Apple and Android; and
- MyMobileCoverage (http://mymobilecoverage.com/), which runs on Apple, Android, and BlackBerry.

So what are the things that one can look at in an app by way of comparing and contrasting functionality?

The first — and arguably the most important — is whether the testing is done on a manual or an automated basis. In the first instance, to get an app onto a device, a consumer must decide that they want to download a speed test app onto their device in the first instance; or if it's an enterprise, it may be that the enterprise decides that they want to load it on their devices. This implies that a consumer or organisation must first have an interest in measuring network performance; representing a small subset of the potential mobile subscriber population.

Furthermore, most of the apps on the market require users to conduct a manual speed test, and generally speaking people will do so when they're unhappy with network performance,

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

or perhaps if they're playing around and curious. However, there's an alternative, and that's automated testing. It can be done either on a continual basis, such as during drive testing, or on an automated basis at designated intervals. For instance, once an hour, once a day, twice a day, or at whatever interval an admin decides to configure.

Another consideration, particularly for consumers, is data usage monitoring. Many consumers have mobile plans with low data usage allowances. Therefore having some sort of monitoring or data usage threshold in the app is important to prevent consumer bill shock, or depletion of a consumer's monthly data usage allowance.

Battery drain can also be an issue for consumers. Therefore, battery level monitoring is an important safety valve for consumers, especially if the app is doing automated testing. No one wants the unhappy surprise of finding that a speed test app has completely drained their battery, especially if they need to make an emergency phone call.

The next area to examine is the type of performance metrics captured. Generally, all of the apps measure upload and download speeds. Most apps measure latency. A couple will also measure delay variation or jitter, which is useful for understanding real-time video or audio performance. Packet loss is something that's very rarely captured but can be.

Signal strength measurement is interesting. We tend to think of signal strength as the barometer of whether we're going to be able to get a mobile connection and do something useful — but how many times have you had your phone in your hand, seen five bars, and you go to Google Maps, but can't load the map; or you're trying to send an email, and you can't get something through? So signal strength, in and of itself, is not an indicator.

There's a related issue with respect to measuring signal strength; namely that Apple, which has a very large market share, does not pass the received signal strength indicator (RSSI) in its API. So unless one jailbreaks an Apple device, an app developer can't get at it. So what you will find is that app developers measure signal strength in the Android version but are unable to do so for Apple devices.

Another differentiator in the apps is whether or not they provide maps of a particular user's experience (history) or for all users in a given geography. Some developers provide maps inside the app, whilst others have a separate portal. And if there is a web-based portal, it may be open to the public, available only to the provider of the app, available to an enterprise or carrier on a subscription basis, or on a one-off data purchase basis.

Some of the apps allow consumers to report network problems (such as the inability to obtain a data connection) on either a manual or automatic basis. This can be done in different ways. In some cases, consumers are encouraged to push a button to tweet about a problem, or push a button to send something to a carrier (or another entity).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Last but not least are privacy considerations. First off, is there any sort of privacy documentation available within the app? Do you even know what's collected? And if you do know what's collected, is there any information that could identify you as an individual consumer?

Of the eight apps examined in this paper, seven of them run on iOS. (The only app that doesn't run on Apple devices is CalSPEED.) All run on Android; two work on BlackBerry; and two on Windows.

Figure 6 contains an analysis of the performance metrics captured by each of the apps examined for this paper. All of them measure upload and download speed. Six of them measure latency. Delay variation and packet loss were measured by a single app each. Three apps measure signal strength (where allowed by the OS). Five of them provide mapping within the app, and six of them offer maps in a portal, which may be public or private.

One caveat with respect to metrics: what you see in the app isn't necessarily all that's collected by the app. It's just what you, as the consumer, can see. And, this analysis relies on information as presented to a consumer using the app.

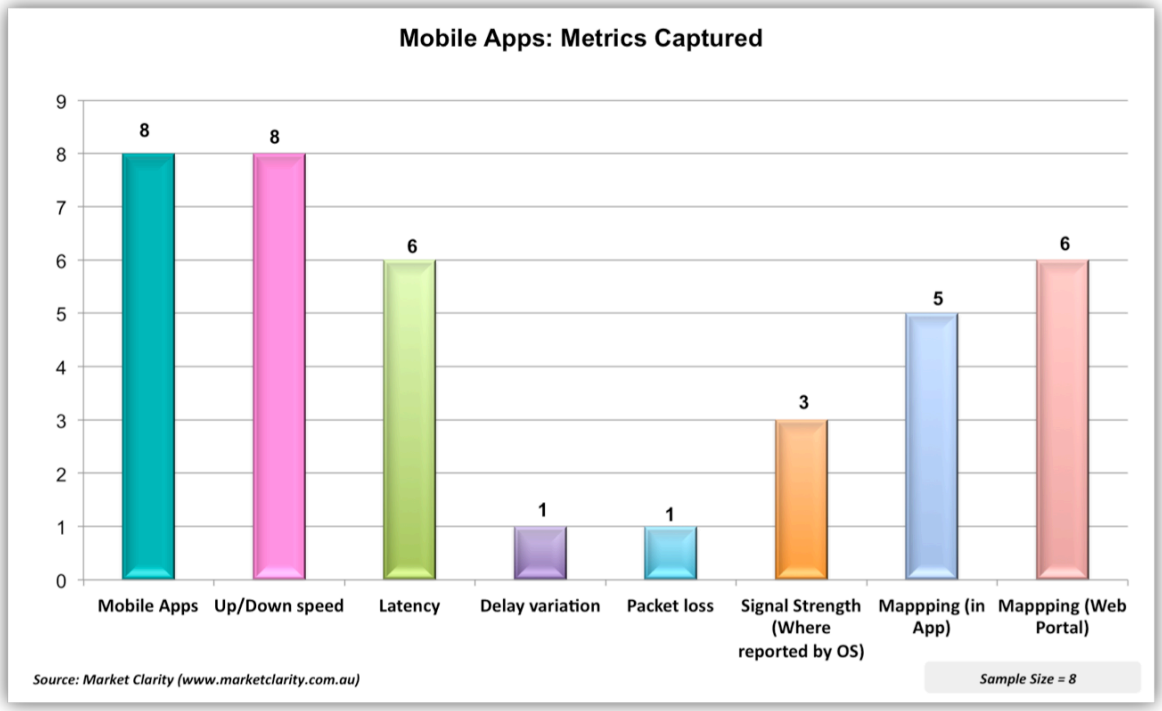

Figure 6 – Examining the Network Performance Metrics Captured by Mobile Apps

In Figure 7, we examine some of the design parameters used by the mobile network performance testing apps. As can be seen, only one app (Mobile Pulse) is able to do automated testing. Mobile Pulse is also the only app that includes battery usage and data usage thresholds (and monitoring).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Interestingly, all of the apps measure cellular network performance, but only six of them measure WiFi.

Six of the apps had a publicly available privacy policy. However, it would appear that half of the apps were actually collecting data such as IP addresses, SIM card information (phone number), unique handset identification numbers, and other personal identifiers. Given the geospatial tracking inherent in mobile network performance testing, this is particularly worrisome.

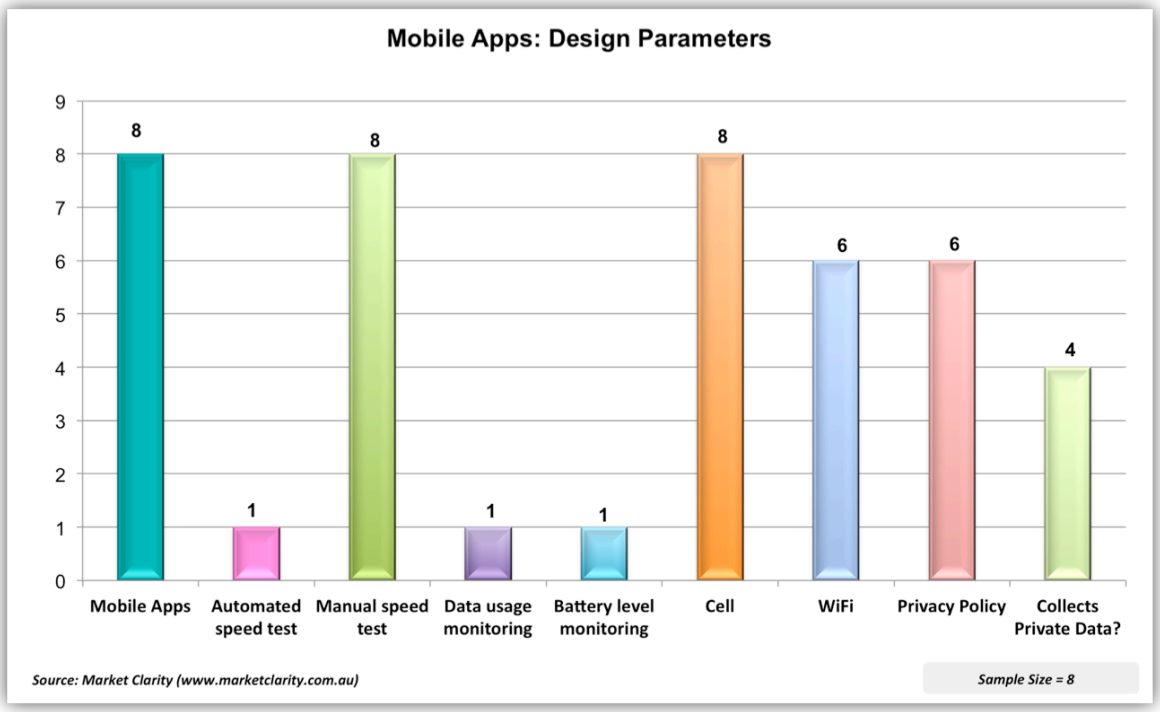

Figure 7 – Examining Design Parameters used by Mobile Apps

Another aspect of the discussion on mobile network performance reporting has to do with the testing methodologies in use. It is beyond the scope of this paper to provide a complete discussion. However, to give you a view on some of the complexities inherent in network performance testing, and why you might get different results from different apps it is useful to provide a simple example.

One of the common design differences has to do with the number of parallel HTTP threads an app is using. If you were using a browser to access web-based information, the browser would typically use multiple threads. Therefore, a number of consumer-oriented apps use four parallel threads in their testing. By contrast, if you were downloading a document it would typically use a single thread. It depends on the target market as to which of these parameters a particular app designer might decide to use (or configure).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

A further design consideration has to do with discarding data. Some of the apps examined for this paper discard anywhere from the 10 to 30 percent of sample outliers. But in doing so they're actually discarding valuable test results, which provide a view of how well the networks are performing.

To summarise, some key testing considerations include:

- Protocol: typically HTTP over TCP
- Upload / download file size and test length (impact on consumer mobile broadband plans)
- Number of upload and download threads (depends on type of application being emulated)
- Methodology for latency measurement
- Discarded data (can skew representation of consumer experience)
- Selection of speed test server
- Server availability
- Methodology to initiate test (manual or automatic)

As can be seen there are a large number of design factors that can impact mobile network performance measurement — as well as factors such as fluctuating signal strength, interference, number of subscriber connections and device characteristics.

Work is currently being done within the IEEE 802.16.3 Mobile Broadband Network Performance Measurements committee (IEEE 2013) to develop standards that will specify procedures for characterising the performance of mobile broadband networks from a user perspective.

Examining US Federal, State and Local Government Mobile Broadband Performance Mapping Initiatives

In order to understand mapping options that may be useful in the Australian context, it's useful to look at overseas initiatives.

In 2008, the US Federal Communications Commission (FCC) approved a broadband mapping plan to examine fixed and mobile broadband availability by speed. The US$293 million mapping project was part of a much larger project (US$7 billion) for a National Broadband Plan that had, among other goals, bringing high speed Internet service to rural areas. Commencing in February 2009, under the auspices of the National

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Telecommunications and Information Administration (NTIA), grants were awarded to the 50 States, 5 Territories, and the District of Columbia.

The program covers both fixed and mobile broadband, although the discussion in this paper will be limited to aspects pertaining to mobile broadband mapping.

Under the National Broadband Map (NBM) program (NTIA a)[1], each grantee (US State or Territory) was able to design its own data collection and verification methodology as inputs into submitting the resulting maps and datasets back to the federal government for consolidation into a national map. The first maps were published in February 2011, and are updated on a six monthly basis (although it appears that the latest update reflects data current as of December 2012 (NTIA b).

As with most programs that allow this type of flexibility many different methodologies were used but they followed a similar trend. The first thing they would do is request information pertaining to network coverage and speeds from the service providers in their areas — typically 3 to 6 mobile operators. Network information was generally provided in GIS shapefile format, Excel format, or a combination of formats. They would then correlate network data with US census blocks and create maps. The States would then try to validate the data through a variety of mechanisms, including drive tests, statistical modelling, crowdsourcing mobile network performance data, and purchasing data from the mobile app vendors that we discussed earlier in the paper. In addition to the federal mapping portal, each State also developed their own mapping portal, and they're all different — surprise, surprise. Here are a few examples of the programs undertaken by the States.

- In addition to obtaining data from mobile operators, Utah utilised a drive testing validation methodology — analysing results from six national carriers (UTAH BROADBAND a), (UTAH BROADBAND b). They drove over 6,000 miles — gaining a snapshot in time of mobile broadband speeds, signal strength and technologies. After collection, the drive test data was used to assess operator data and was used in verification discussions with the mobile providers. It's worth noting that every one of these carriers also conducts its own drive tests, but they don't share this data because it's deemed to be proprietary.
- In California, they started with GIS or tabular data from the mobile operators, and then conducted their own statistical modelling (California PUC a). Like other States, California obtains GIS coverage shapefiles from providers; or if not available tabular data containing tower and antenna information. Wireless parameters were used to model the service area, and from that create a shapefile. Individual radio unit specifications were used to measure performance based on frequency, transmit

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

power, receiver sensitivity, antenna gain, and height. Signal coverage patterns were produced for each individual unit taking into account terrain and vegetation features that might hinder signal dispersion.

California also partnered with the California State University to develop the CalSPEED app (described earlier), and then paid students to do drive testing for them. In 2013, they also released a public crowd-sourced version of the app (California PUC b).

As can be seen from their website, California has a wide range of data that can be downloaded. In the April 2013 dataset (the latest available when researching this paper) the author was able to download a spreadsheet that contained 9,800 drive test samples, which contained a range of relevant information.

- Delaware also started their investigations with data requests to the mobile operators, but adopted a slightly different verification methodology (Delaware Broadband Project 2013). The State's verification process included researching the providers' websites to verify that the advertised speeds on the websites were consistent with those documented by the providers as part of their submission to the State. In addition, the verification team made phone calls to some of the providers in order to further verify service availability and speeds. Following this process, the data was sent back to the providers for their review and acknowledgement of the data as being accurate.

  After the original field verification testing done in 2010, further verification was done only on receipt of updated information from the providers in the State. For example, areas previously verified, which had no reported changes in technology or speed, were not re-verified as part of subsequent rounds of verification. In December 2012, State team members spent five days performing field verification functions – testing cellular networks at 46 locations, conducting approximately 110 speed tests of cellular based wireless broadband provider networks.

  Delaware also has a web-based speed test portal (Delaware Speed Test), which it encourages the public to use. However, it allowed the author to conduct a test from Australia across a DSL network, whilst allowing the author to indicate that the speed test was conducted via a mobile network. (The author sincerely hopes that this test result was discarded.) Furthermore, Delaware's online mapping portal was not working properly on numerous occasions when the author examined the website (Delaware Interactive Map).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

- In addition to geospatial analysis and drive tests, a number of State governments are conducting large-scale crowdsourcing programs. Many, such as the State of Colorado, use Mobile Pulse because of its automated testing features.

  Mobile Pulse has numerous data collection modes, including a crowd source privacy mode that doesn't collect any consumer data. States also deploy the application in an enterprise mode, using it in police cars, fire trucks and other government vehicles. This app is gaining a lot of traction with US Government entities because of the very large test samples obtained via automatic data collection.

  For example, Figure 8 shows Mobile Pulse testing in Colorado during a six-month period. In one small areas of the State (the light blue grid below the pop-up showing typical speeds) there were close to 55,000 test results. That's a large sample, especially when compared to the 9,800 drive tests that the author was able to download for the whole state of California during a similar six-month period.

  US States are turning to crowdsourcing on a large scale, using automated test tools, because it generates a lot of data. Many of the large US drive testing companies have also deployed this app, running it in continuous data collection mode.

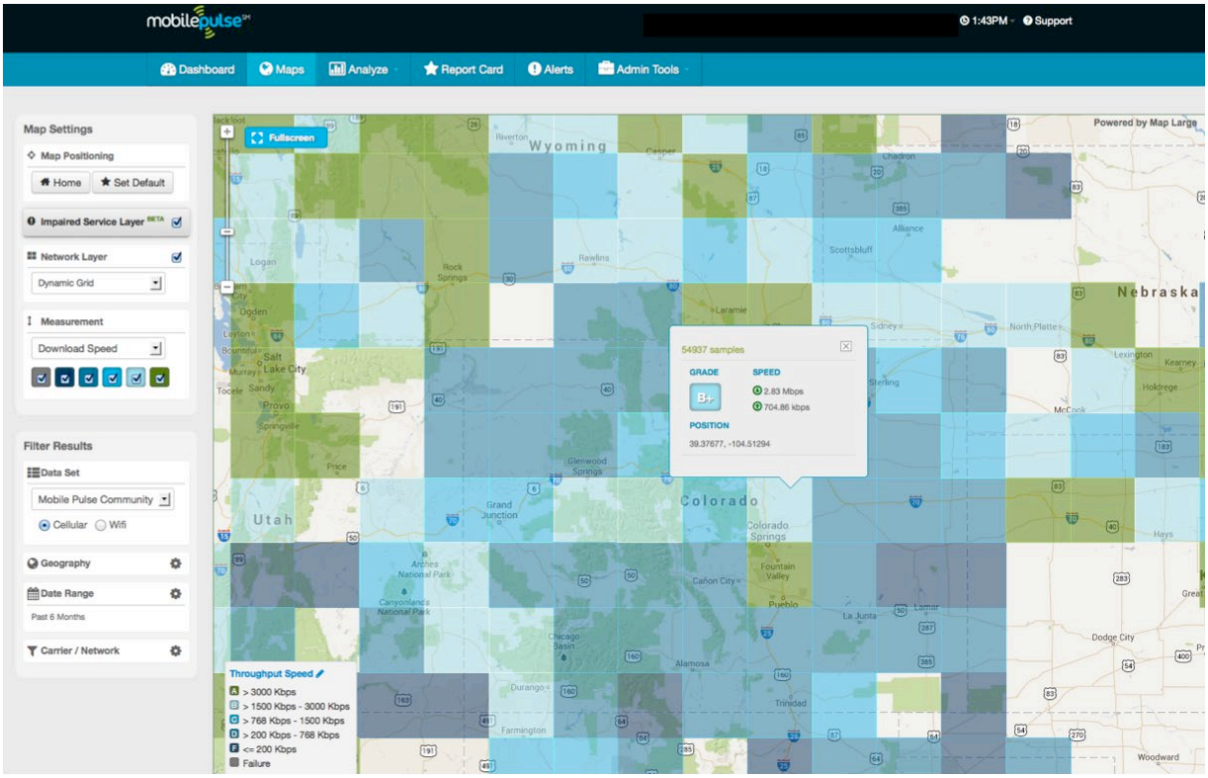

Figure 8 – Mobile Pulse: Tests Conducted in Colorado (October 2013) (Mobile Pulse 2013)

There are many aspects of the US broadband mapping initiative that can be directly applied to similar programs in Australia and elsewhere. What is perhaps most interesting (although

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

not surprising) is a view of speeds reported by the carriers versus the actual speeds recorded by the different States using a wide variety of methodologies.

Figure 9, is from the US mapping portal (NTIA), and it shows a comparison of speed test results versus advertised speeds as reported by the carriers. Green dots indicate speeds that were faster than the carriers indicated, and red indicates slower speeds than the carriers reported.

Unfortunately, this Figure is not specific to mobile tests – the mapping site doesn't specify which technologies the result applies to, or allow selection by technology. However, this map provides an overall impression that the results of State testing produced results that tended to be slower than the advertised speeds. Although not show here, a similar map charting speed test results against typical speeds reported by carriers had a slightly more positive result in that there was a greater preponderance of green dots (faster results) on this map.

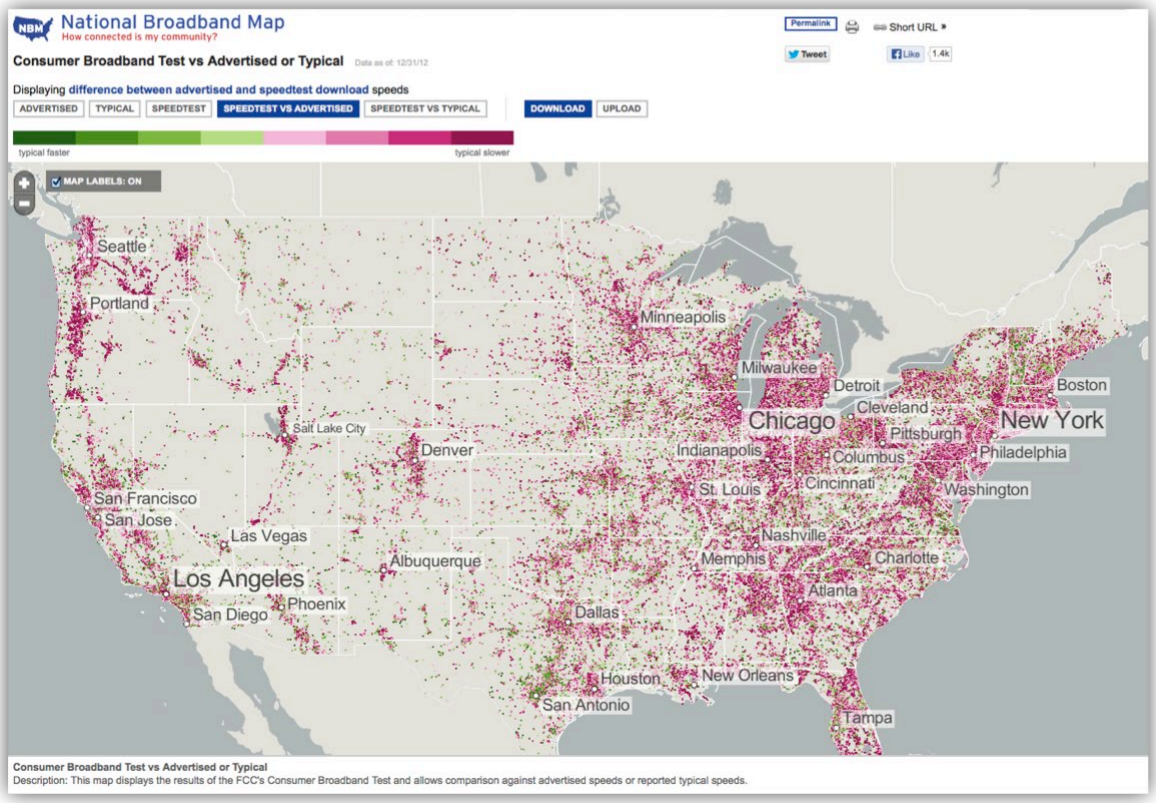

Figure 9 – US National Broadband Map: Speedtest vs Advertised (All Technologies)

Concluding Thoughts

In the US, the federal government provided grant funding for the States and Territories to collect and map fixed and mobile broadband performance data. A wide range of methodologies were used for this purpose — including drive testing, data purchases (from mobile performance app vendors) and crowd source programs to correlate and map out real-

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

world coverage in their area — with the results stitched together into a national coverage map.

With respect to the varying methodologies in use, one can argue that this is good or bad. It certainly demonstrates that there is no single method in use in the US (or elsewhere in the world). From the perspective of providing a national map, it is this author's view that a single methodology would have provided greater consistency in the national dataset, and would have eliminated duplication (and costs) affiliated with each State and Territory producing their own mapping portal in addition to the national mapping portal.

One of the interesting things, though, is that the mobile operators cooperated with the States. They provided GIS shapefiles and tabular data in Excel format, as well as a range of performance data — usually showing theoretical speeds, rather than real world averages. Generally, because the States also provided the information back to the mobile operators, they found it a very useful cooperative process.

Could a similar program work in Australia? In this author's view it could.

However, consumer privacy issues are really important, and this needs to be carefully considered in any program.

Consumer data usage and bill shock protection is another important issue. We wouldn't want to see millions of Australians download a mobile performance app onto their smartphone or tablet to help with a national crowdsourcing initiative, and end up with an unexpectedly large mobile service bill — or find that they've used their full data allowance on the crowdsourcing initiative.

In this author's view a large dataset is needed to provide a valid sample, and a large-scale crowdsourcing initiative could certainly provide this. Furthermore, automated, periodic testing at regular intervals (rather than manual speed tests) would provide results that are consistent with a typical consumer experience.

There are a number of methodology issues that remain unanswered. For instance, how do you represent data sets with variable results? Should any samples be discarded? If there is a large-enough dataset, using average (mean) or median results to represent typical upload and download speeds is certainly a valid way of representing mobile service performance expectations. By further segmenting the dataset by time of day, consumers would gain further useful information that could inform purchase decisions. And, mobile operators would gain useful insight into network performance from the perspective of an end user, with the myriad of devices deployed in the real world.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.25

Having spent much of 2013 looking at this issue, it is this author's view that consolidated mapping based solely on theoretical potential maximum speeds is not very useful. As shown in this paper, real world mobile network performance varies widely, and is also impacted by the measurement methodology in use. Nonetheless, a consolidated map that impartially shows real-world results from all of the mobile networks would provide some very useful information to consumers.

Would Australian mobile operators cooperate with this type of program? Maybe. To the extent that data is already published, it is likely to be made available to an analysis program.

The Australian Government has recently announced a $100m Mobile Coverage Programme (DoC 2013), which would require that each base station and group of base stations proposed for funding be assessed against a range of criteria. Certainly a crowd source mapping program would provide useful information to all parties, and assist in prioritising the specific geographic locations where funding would be applied.

References

Australian Communications and Media Authority. 2013. Reconnecting the Customer: Mobile Network Performance Forum, 14 November 2013. Available at http://www.acma.gov.au/theACMA/About/Events/Mobile-Network-Performance-Forum/mobile-network-performance-forum.

California Public Utilities Commission. nd. California Broadband Availability Maps and Data. Available at http://www.cpuc.ca.gov/PUC/Telco/Information+for+providing+service/Broadband+Availability+Maps.htm

California Public Utilities Commission. nd. " CPUC Unveils Mobile Speed Testing Application; Begins Round of Broadband Testing Throughout State". Available at http://www.cpuc.ca.gov/NEWSLETTER_IMAGES/0513ISSUE/CPUCeNewsletter_0513_full.html

Department of Communications, Australian Government. 2013 . Mobile Coverage Programme. Available at http://www.communications.gov.au/mobile_services/mobile_coverage_programme

Mobile Pulse. 2014. www.mobilepulse.com

Neville, Anne. 2011. Official FCC Blog. State Broadband Initiative – NTIA, "The National Broadband Map," 17 February 2011. Available at http://www.fcc.gov/blog/national-broadband-map

U.S. Department of Commerce. nd. National Telecommunications and Information Administration. NTIA's State Broadband Initiative, National Broadband Map. Available at www.broadbandmap.gov.

U.S. Department of Commerce. nd. National Telecommunications and Information Administration. NTIA's State Broadband Initiative, National Broadband Map Datasets. Available at http://www2.ntia.doc.gov/broadband-data

Optus, Nov 2013, https://www.optus.com.au/network/mobile/coverage

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.25

State of Delaware. 2013. Broadband in Delaware - About the Project. Available at http://www.broadband.delaware.gov/about.shtml and Delaware Department of Technology and Information, Contract No. DTI-08-0013, Delaware Broadband Data and Development, Spring 2013 Data Submission White Paper (March 2013)

State of Delaware State of Delaware. 2011. Interactive Map. Available at http://www.broadband.delaware.gov/map.shtml

State of Delaware State of Delaware. nd. Internet Speed Test. Available at http://www.delawarespeedtest.com/

Telstra Corporation. 2013. See http://www.telstra.com.au/mobile-phones/coverage-networks/our-coverage/ (Nov 2013)

The State of Utah. nd. Broadband Project, About the Interactive Map. Available at http://broadband.utah.gov/about/about-the-interactive-map/

The State of Utah. nd. Broadband Project, Utah Mobile Broadband 'Drive Test' Data Available for Download, http://broadband.utah.gov/2011/10/13/utah-mobile-broadband-drive-test-data-available-for-download/ and http://broadband.utah.gov/map/

Vodafone. 2013. Coverage Checker Nov 2013 and Jan 2014. Available at http://www.vodafone.com.au/aboutvodafone/network/checker

Western Telecommunications Alliance. 2009. FCC Definition of broadband, as cited by Western Telecommunications Alliance to US Dept of Commerce, NTIA, American Recovery and Reinvestment Act of 2009 submission, April 2009.

Notes

1. Information is available in both the mapping portal, as well as a range of file formats available for download (http://www.broadbandmap.gov/data-download). It appears, however, that the website does not support download requests coming from IP addresses outside of the US. In order to research this paper, colleagues in the US kindly downloaded relevant materials requested by the author, which was then supplemented with information directly available from each State or Territory's broadband mapping portal.

Cite this article as: Evans, Shara. 2014. 'Australian mobile broadband network performance: Mobile apps as one possible way to provide consumer information'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 25.1-25.20. DOI: http://doi.org/10.7790/ajtde.v2n1.25. Available from: http://telsoc.org/journal

The new NBN policy's Achilles heel

Peter Gerrand
University of Melbourne

While most critiques of the Coalition Government's National Broadband Network (NBN) policy have focussed on the wisdom of its Fibre to the Node technology choice, a more fundamental weakness in its NBN election policy promises to make it a financial debacle if not corrected. This editorial spells out the many negative consequences of the Government's policy to remove the NBN Co's current monopoly in providing fixed broadband access infrastructure: to the federal budget, to the competition framework in telecommunications, to a forced premature sale of NBN Co, and to the affordable rollout of high-speed broadband access across the nation. The Minister of Communications is urged to correct this policy element rapidly, in the national interest.

"Uh oh – spoiler alert!" William Robey ©2014

Introduction

The NBN is currently in the doldrums. Senior staff at NBN Co continue to leave the company, and Communications Minister Malcolm Turnbull has launched yet another audit review into the actions of the previous government (*Stock and Land*, 7 March 2013). While

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

the rollout of the terrestrial and satellite-based radio implementations of the NBN continue as previously planned, the Minister has apparently departed from an election pledge (*The Examiner*, 17 August 2013) to honour all existing contracts to roll out fibre to the premises (the FTTP solution). Hence the recent demonstration by 30 contractors in Tasmania, who had invested in expensive new machinery to lay fibre, and now find their contracts to be worthless (*ABC News*, 27 Feb 2014).

Understandably the debate over the Abbott Government's new NBN policy (especially in this Journal) has tended to concentrate upon the costs and benefits of its fibre to the node (FTTN) policy in contrast to the previous FTTP policy or other technical solutions, e.g. (Eckermann 2013), (Gregory 2013), (Watkins & Lillingstone-Hall 2014) . After all, the future international competitiveness of Australia is allegedly at stake. But the Achilles heel of the Liberals' election promise on the NBN lies not with the short-termism of their technology choices. It lies in their policy decision to remove NBN Co's monopoly over the supply of fixed broadband infrastructure in the access network. The implication of this policy to undermine NBN Co's financial performance was first pointed out by the author on 10 April 2013 (Gerrand 2013) as part of a general critique of the then Opposition's NBN policy, launched on the previous day (Liberal Party 2013). This point has subsequently been argued more vigorously and, dare I say, more eloquently by industry commentators Paul Budde (2014) and Alan Kohler (2013, 2014).

I will now argue that the removal of the NBN Co's wholesale monopoly will not only push NBN Co's business case permanently into the red, it would also have several other significant negative consequences for the federal government. Or, to avoid that contingency, it would cause the Government to back off completely from its commitment to a ubiquitous high-speed NBN, and tempt it to an early sale of NBN Co to the private sector, if necessary at a fire-sale price, to move its liabilities off the federal budget. The more sensible approach will be for the Government to leave NBN's current wholesale monopoly intact.

The Coalition's NBN election policy

At the launch of the Liberals' NBN policy on 9 April 2013 (Liberal Party 2013), the then Opposition Leader Tony Abbott commended Mr Turnbull's policy as being 'very high quality work' and that it 'will provide a real commercial return' (*Delimiter*, 9 April 2013). It was indeed a commendably comprehensive election policy even if Mr Turnbull's paid consultants had done what consultants are always good at: inputting into their modelling the best case conditions (of costs, revenue and service performance) for their client's preferred solution and the worst case conditions for the alternative policy – in this case, that of the then Government's. But by ignoring the effect of cherry-picking by NBN Co's competitors, the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

consultants failed to predict that, under this new policy, NBN Co will be doomed to run at a loss.

For some reason, perhaps driven by ideological preference rather than prudent economics, the Liberal's NBN election policy threw out the most essential economic underpinning element in the existing NBN's policy – that of giving NBN Co a wholesale monopoly in the provision of fixed high-speed broadband access infrastructure. Thanks to that essential monopoly condition, the NBN can cross-subsidise broadband rollout in the poorest and the least densely populated areas of Australia.

And thanks to that essential monopoly, NBN Co can weather the storms of aggressive price control by the regulator (the ACCC), or disappointments in forecast revenue, or blow-outs in forecast costs. Because everywhere that the monopoly NBN infrastructure is in place, revenues will flow into the far foreseeable future from its Retail Service Providers; and by having access to sufficient profitable locations, NBN Co's business will eventually break even – assuming that its wholesale pricing is regulated accordingly. At that point, with most of its network costs sunk, it will start generating an increasing annual profit for its long-term investor, the government. The penetration of broadband services across the community will rise, either slowly or rapidly, to eventually near-saturation levels, as occurred for the former standard telephony service in the 1990s and is now occurring in the mobiles market. The NBN pay-back period for the government may exceed early forecasts – say 12 years or even 15 years, instead of ten – but eventually, provided the wholesale pricing is well regulated, the project will produce a net positive return on investment.

But, some may ask, why must removal of the NBN's monopoly invariably cause it to run permanently at a loss?

The effect of cherry picking in the broadband infrastructure market

Once the NBN access infrastructure monopoly is broken, many entrepreneurial carriers will see the opportunities to cherry-pick the most profitable locations, such as for new apartment buildings or office blocks. In fact, TPG notably jumped the gun shortly after the September 2013 federal election by announcing its plan to build its own wholesale broadband network in built-up city areas, thereby relying on the Coalition Government's new policy before it had been tested in parliament, let alone legislated (*Australian Financial Review*, 18 September 2013). TPG's subsequent acquisition of AAPT in December 2013 for $419M was seen as further positioning itself to take advantage of the new government's NBN policy, while in the meanwhile claiming to have found a legal way around the current anti-cherry picking provisions.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

The Minister's eventual public response to the TPG announcement (*Australian Financial Review*, 4 February 2014) suggests that he is well aware of what is at stake, and is waiting for the six month review of the cost and benefits of his NBN policy by a further panel of experts to decide which way to jump (Turnbull 2013). In the meantime NBN Co Chairman, Ziggy Switkowski has shown himself well aware of the potential revenue loss to his company (*CommsWire*, 13 March 2014).

Of course, if TPG is allowed to break the monopoly, the larger broadband infrastructure providers such as Telstra, Optus, NextGen and iiNet will feel entitled to follow. This will mean that NBN Co will be left with the least profitable segments of the metropolitan markets to serve, while being encumbered with serving highly unprofitable segments of the rural and regional market. Its annual losses could reach or exceed $2 billion per year, based upon worst-case revenue for the Coalition's current NBN business case (Liberal Party 2013), year on year until roll-out of the Government's proposed Fibre to the Node network is complete.

The implications of negative RoI for the government

If NBN Co under the anti-monopoly policy becomes as much a lemon as Aussat was in the 1980s under its no-compete-with-Telecom policy, its losses will mount up as a significant expense item in the government's annual Budget Operating Statement. But, because of the accounting convention whereby this item is treated as a 'below the line item' in the Operating Statement (Dalzell 2012), it will not embarrass the government politically by pushing the Budget Deficit – that headline figure – further into the red. On the other hand, the NBN's net losses will directly affect the government's overall fiscal balance – as you would expect.

Parliamentary Library researcher Brian Dalzell (2012) points out that: 'A (fiscal) deficit indicates that the government is drawing on resources from other sectors in the economy'. In other words, the longer that NBN Co remains loss-making, the longer the NBN *itself* needs to be cross-subsidised – ultimately by the rest of the economy. Gone are the days of the expected 7% long-term Return on Investment (RoI) from a self-funding national infrastructure project.

Just how long Federal Treasurers and Federal Ministers of Finance from either side of the political divide would be prepared to tolerate such a financial albatross is easy to guess.

The impact of the broken monopoly on regulatory policy

Beyond the ongoing financial damage which the Coalition's current NBN policy will do to the Government's budget lies the collateral damage of regulatory confusion. Once Telstra feels obliged – in the interests of its shareholders – to follow TPG in leveraging its great assets in network deployment to offer fixed broadband access infrastructure in competition with NBN

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

Co, the whole issue of unfair advantage of the dominant retail provider being also a dominant provider of wholesale broadband access will emerge again. This was the issue which bedevilled the industry for the duration of the Howard government, stifling competitive broadband infrastructure investment, and which most of the industry believed was neatly solved by Labor's 2009 NBN policy: Telstra was effectively paid out $11 billion for vacating the copper access network, with a no-compete clause on most wholesale broadband fixed infrastructure access via other technologies.

How to heal the Achilles' heel?

The Abbott Government has several options:

The most obvious choice is to revise its policy, in order to maintain the NBN monopoly on fixed access infrastructure – which requires no legislative change. The advantages are manifold: a reduction in the NBN's losses that would otherwise keep dragging down the federal budget; a long-term positive return on investment that will provide ever increasing federal revenue once the break-even year is reached; the opportunity to use NBN Co for cross-subsidisation of wholesale prices, thus keeping voters in the regions – and in the outer suburbs of our large cities – onside.

Furthermore, it will maximise the value of NBN Co when the Government moves to sell it off to the private sector (a policy which I would argue is not in the national interest, but it is one which suits the current major parties' neo-liberal philosophies).

An alternative choice for the Government is to stick to its anti-monopoly policy, driven by the desire to keep faith with its supporters as well as those corporations, such as TPG, which have already made investment decisions based on the assumption that the election policy will indeed be implemented.

In that case the Government will need to deal with the downsides detailed above.

To avoid the resultant drag on the federal budget of the order of $2 billion p.a. for several years, the government will be motivated to sell off NBN Co as soon as possible.

However, NBN Co will be unsellable while it maintains the liabilities inherent in the Abbott Government's current NBN policy – i.e. in providing a truly national rollout of high-speed fixed broadband infrastructure while running at a loss. To make NBN Co saleable, the Government would be forced to significantly dilute its obligations to provide a universal high-speed broadband service – most likely by heavily increasing the user-pays component.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

Conclusion – the need to correct that policy blunder

This article has described in some detail why the intention to break NBN Co's current wholesale monopoly is the Achilles heel in the Turnbull-Abbott election policy – and needs urgent revision.

This is not a lone voice. While the author drew attention to this weakness in the policy first on 10 April 2013 (Gerrand 2013), other industry analysts have agreed (e.g. Budde 2014). Allan Kohler has argued eloquently for the abandonment of this policy in two columns (2013, 2014). In fact Kohler has memorably described the Turnbull NBN policy in these terms:

> *'It will, in short, be a donkey, a money sinkhole, a political noose, and an end-of-career nightmare for a mild-mannered nuclear physicist who might end up wishing he'd stayed at the opera.'* (Kohler 2013)

The current article goes further in drawing attention to the additional implications if this policy is not corrected – especially the implications for Australia if, as a consequence, NBN Co is sold off prematurely, freed of its current obligations to provide broadband access infrastructure across the country, in order to make the company saleable.

Such a sell-off would simply create another Qantas – a privatised entity legally obliged to give first priority to serving its institutional shareholders, while being hobbled by a caveat on foreign ownership to placate an increasingly disgruntled electorate. And just as the Qantas Board has been forced since its privatisation to abandon unprofitable rural and international services, a privatised NBN Co, having to compete with carriers with much deeper pockets, will inevitably be forced to ditch any further attempts at cross-subsidies to provide equity in access to outer suburbs and regional population centres.

In short, unless the Minister for Communications acts to correct this fundamental error in his NBN policy, we will live to see another great Australian policy disaster. The most important objective of the NBN, the only one that justifies government investment of the order of $30 billion or more, will be abandoned: that is, to make Australia internationally competitive – across the nation, not just in central business districts and technology parks – in its ability to succeed in the new digital economy.

References

ABC News, 'Tasmanian NBN contractors seek compo over fibre optic rollout changes', ABC News online, 27 February 2014, at http://www.abc.net.au/news/2014-02-26/tasmanian-nbn-contractors-seek-compo-over-fibre-optic-rollout-c/5285112

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

Australian Financial Review [David Ramli and James Hutchinson]. 2013. 'TPG fibre plan challenges NBN', 18 September 2013, at http://www.afr.com/p/australia2-0/tpg_fibre_plan_challenges_nbn_v10TzlbnSJEHWqPQ70CZ3K

Australian Financial Review [David Ramli]. 2014. 'Turnbull queries TPG bid to skirt NBN', 4 February 2014, at http://www.afr.com/p/business/companies/turnbull_queries_tpg_bid_to_skirt_FRzXpQsdo1IkyjjqSRV5EI

Budde, Paul. 2014. 'No NBN cherry picking – another step in the right direction', BuddeBlog 10 February 2014, at http://www.buddeblog.com.au/frompaulsdesk/no-nbn-cherry-picking-another-step-in-the-right-direction/

CommsWire [David Swan and Graeme Phillipson]. 2014. 'Ziggy fires TPG warning shot' *f CommsWire*, No. 1295, 13 March 2014, at www.commswire.itwire.com

Dalzell, Brian. 2012. 'The national broadband network and the federal government budget statements', Australian Parliamentary Library Background Notes, 13 January 2102, at http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2011-2012/NBNBudgetStatements

Delimiter. 2013. 'Coalition NBN policy launch: Full video', 9 April 2013, at http://delimiter.com.au/2013/04/09/coalition-nbn-policy-launch-full-video/

Eckermann, Robin, 2013. 'Getting some reality into debates about NBN FTTP'. *Australian Journal of Telecommunications and the Digital Economy*, Vol 1, No 1, Article 13. http://doi.org/10.7790/ajtde.v1n1.13

Gerrand, Peter. 2013. 'The Coalition's NBN policy is a triumph of short-termism over long-term vision', *The Conversation*, 10 April 2013, at http://theconversation.com/the-coalitions-nbn-policy-is-a-triumph-of-short-termism-over-long-term-vision-13333

Gregory, Mark. 2013. 'A flexible upgrade path for the Australian National Broadband Network', *The Australian Journal of Telecommunications and the Digital Economy*, Vol.1 No.1, Article 17, November 2013, at http://doi.org/10.7790/ajtde.v1n1.17

Kohler, Alan. 2013. 'The NBN Board has run away. Why?', *Business Spectator*, 23 September 2013, at http://www.businessspectator.com.au/article/2013/9/23/information-technology/nbn-board-has-run-away-why

Kohler, Alan, 2014. 'Sorry Malcolm, the NBN must be a monopoly', Technology Spectator, 3 March 2014, at http://www.businessspectator.com.au/article/2014/3/3/technology/sorry-malcolm-nbn-must-be-monopoly

Liberal Party. 2013. 'Fast, affordable, sooner. The Coalition's plan for a better NBN', 9 April 2013, at https://www.liberal.org.au/fast-affordable-sooner-coalitions-plan-better-nbn

Stock and Land [Lia Timson], 2014. 'Malcolm Turnbull starts fifth NBN audit', *Stock and Land*, 7 March 2014, at http://www.stockandland.com.au/news/metro/national/general/malcolm-turnbull-starts-fifth-nbn-audit/2690792.aspx

Turnbull [The Hon. Malcolm Turnbull MP, Minister for Communications]. 2013. 'Panel of Experts to conduct cost-benefit analysis of broadband & review NBN regulation', 12 December 2013, at http://www.minister.communications.gov.au/malcolm_turnbull/news/panel_of_experts_to_conduct_cost-benefit_analysis_of_broadband_and_review_nbn_regulation#.UyVAI9yyKMW

The Examiner [Ben McKay]. 2013. 'Turnbull confirms NBN will honour contracts', *The Examiner*, 17 August 2013, at http://www.examiner.com.au/story/1711548/turnbull-confirms-nbn-will-honour-contracts/

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.32

Watkins, Craig; Lillingstone-Hall, Kelvin. 2014. 'The FTTdp Technology Option for the Australian National Broadband Network', *The Australian Journal of Telecommunications and the Digital Economy*, Vol.2 No.1, March 2014, at http://doi.org/10.7790/ajtde.v1n1.6

Cite this article as: Gerrand, Peter. 2014. 'The new NBN policy's Achilles heel'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 32.1-32.8. DOI: http://doi.org/10.7790/ajtde.v2n1.32. Available from: http://telsoc.org/journal

The FTTdp technology option for the Australian National Broadband Network[1]

Craig Watkins
Informative Technology Innovations

Kelvin Lillingstone-Hall
CEO, OAK Telecom

Fibre to the Distribution Point (FTTdp) is a broadband access network technology that encompasses fibre to the street lead-in pit at the front fence, with an average copper lead-in length of 30m. FTTdp promises very high VDSL2 capability, with easy upgrading to G.fast or individual FTTP (Fibre to the Premises) on an on-demand basis. The network capability of FTTdp is thus very close to the capability of a full FTTP deployment. Cost savings compared to FTTP promise to be substantial – a possible $12 billion in savings for the Australian National Broadband Network – due to the use of existing copper pair lead-ins, thus avoiding civil engineering works for each individual fibre lead-in. Indeed, there is reason to expect that the initial cost of FTTdp deployment will be comparable to that of FTTN (Fibre to the Node). FTTdp has additional benefits of reduced copper maintenance and limited ongoing upgrade costs compared to FTTN. Significantly deeper fibre network penetration is potentially cost-neutral (or better) with FTTdp when compared to the FTTN baseline due to elimination of time-consuming activities involved with FTTN deployment. The reduced street impact of FTTdp is also important.

Introduction

It is undeniable that bandwidth demands of all users are steadily increasing. Likewise there is broad agreement that current access networks, primarily ADSL, HFC (Hybrid Fibre Coax), and 3G and 4G wireless, need substantial augmentation or improvement to meet latent and evolving demand from the broad user base. The vision of the NBN is to supply access network capacity to meet this demand now, and well into the decades ahead. This includes various customer needs for symmetric and asymmetric services, one-way and two-way applications, support for multiple individual data and video channels from a multitude of world-wide sources, and various Qualities of Service.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

Naturally, the selection of technologies to provide bandwidth capability in the NBN context is highly dependent upon projections of demand growth. While we can easily agree that continued growth in bandwidth demand is effectively guaranteed, it is a much more complex task to find agreement on exactly where NBN Co design targets should be, even looking only as far as 2020. Extending this horizon to 2025 or 2030, results in extreme variance of opinion on future bandwidth demands (projections vary from 100 Mbps to 10 Gbps or more).

We can look to the emerging reality of 4K television, coupled with the present reality of multiple video streaming to a single premises, to determine a lower threshold of 100 Mbps as an absolute minimum network design capacity to be delivered on the 5-year time-frame. The 100 Mbps figure has received widespread support in recent years as a realistic – and yet somewhat aspirational – target, including from the FCC (US Federal Communications Commission). However, widespread rapid uptake of 4K TV may make even this figure seem low. If there is an economically feasible way to supply a significant increase in base-level capacity over this figure, then we must give it due consideration.

FTTP (Fibre to the Premises) supplies sufficient capacity to rise to the challenge of any future demand scenario. Single-mode optical fibre provides bandwidth capability, in conjunction with suitable selection of active electronic termination devices on either end, to meet any conceivable throughput demand. If costs were not a concern, FTTP is the obvious choice. The reality of the NBN Co deployment is that costs are an issue. The NBN Co Strategic Review report points to international costs of FTTP for countries 'most comparable' to Australia, being in the range of $1100 to $1300 per premises (NBN Co 2013: page 13 and 78). From page 61 of the same report, we can calculate an average FTTP cost in the NBN Co context of $4200. Limiting the focus to brownfields, the amount becomes $4970. Introducing the $12 billion savings from the 'Radically Redesigned FTTP' (from page 17), these amounts become $2880 per premises average, and $3260 for brownfields.

FTTN (Fibre to the Node) and FTTdp (Fibre to the Distribution Point) are options to reduce the NBN Co deployment cost. FTTN has been considered in some detail by NBN Co as part of the Strategic Review process. FTTdp has been introduced to readers of this journal in the recent paper by Mark Gregory (Gregory 2013). A worthwhile discussion on the use of copper technologies for the last customer access link is also contained in the recent paper by Robin Eckermann (Eckermann 2013). The papers by Gregory and Eckermann are well worth detailed study for those interested in obtaining a broad perspective on the NBN technology issue. We expand on the earlier FTTdp exposition provided in the Gregory paper, by focussing solely on very short-loop FTTdp (fibre to the street lead-in pit), and presenting further discussion on costs and benefits.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

FTTN very clearly does not provide the level of network capability of FTTP. FTTN can provide a level of capability that satisfies low bandwidth demand increase scenarios (and a reduced need from high-demand premises). We observe a trend of downplaying bandwidth evolution scenarios in those contributions that suggest FTTN as a sensible approach for the nation (NBN Co 2013: page 79). For higher bandwidth demand growth projections, it is clear that the risk involved with mainstream FTTN deployment is very real (Watkins 2014).

Obviously, the difficulty with the FTTP approach is not the network capability provided, but the expense involved in deploying fibre all the way to premises. This in turn relates to costly tailored civil engineering works associated with each premises fibre lead-in. Clearly both costs and benefits must be carefully assessed when evaluating which technology to deploy. This complex task faces the NBN Cost Benefit analysis currently under way, with the expert panel having been recently appointed (Minister for Communications 2013).

The cost-benefit analysis is complicated enough if only two options of FTTP and FTTN existed. The need to fully consider HFC networks promises significant challenge to the expert telecommunications technology input able to be recruited for the task. A key consideration here is properly understanding the capabilities and limitations of the HFC technology, now and into the future. (HFC originated as a broadcast medium for selected video channels, and is now being applied to on-demand delivery of content from millions of channels world-wide, as well as two-way voice and video conferencing.) We must assess the impact of evolving bandwidth demand on the shared HFC network elements, and understand the expenses involved with infrastructure upgrades to maintain capability commensurate with the number of users and demand statistics. A detailed long-term technology road-map must be produced (in rough form at least) if any sensible determination of the cost-benefit equation is to be made for HFC. As HFC coverage is proposed to account for up to 30% of the premises in the nation, it is clear that these considerations must not be taken too lightly.

Ignoring the HFC question for the present, FTTdp can be seen to have network capability benefits closely aligned to that of FTTP, while (potentially) being cost-comparable to (or better than) FTTN. As such, proper consideration of the FTTdp option is likely to greatly simplify the overall cost-benefit analysis. The possibility is very strong that FTTdp may be found to provide a comprehensively robust and economic NBN technology solution. Making a sensible determination on this issue will again require expert telecommunications technology input supplied to the cost-benefit analysis team.

There is little argument that FTTP is the only sensible choice for greenfield deployment. FTTP is also the only sensible choice where it can be deployed economically (with aerial FTTP needing careful consideration in this regard), due to the robust and flexible nature of a

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

full fibre solution. However, a significant majority of premises to be covered by the NBN are in brownfield development areas, and as such present more challenge to the physical deployment effort. In this paper we focus solely on the brownfield deployment scenario.

The paper aims to outline some of the key cost and benefit considerations for a FTTdp deployment. We do this by comparison to FTTP and to FTTN. Discussion of benefits is in the context of projected future bandwidth demand scenarios and a long-term focus. Cost consideration is necessarily crude, but we attempt to supply reasonable estimations in conjunction with cost data extracted from the NBN Co Strategic Review report (NBN Co 2013).

A Definition of FTTdp

Fibre to the Distribution Point (FTTdp) is a broadband access network technology, encompassing fibre to the street lead-in pit at the front fence. FTTdp is often deployed in conjunction with a wider FTTP deployment. In this setting we expect FTTdp to interoperate smoothly with the wider FTTP protocols such as GPON (Gigabit Passive Optical Network). In general we can define FTTdp as having copper lengths less than 200m. This is the sense in which Swisscom is deploying FTTdp (Swisscom 2013) in areas away from major urban centres. The NBN Co Strategic Review report introduces FTTdp as an augmentation approach for a FTTN deployment (copper length not stated, but assumed to be up to 200m). FTTdp in the present paper implies taking fibre to the street distribution pit, leading to an average copper loop length of around 30m.

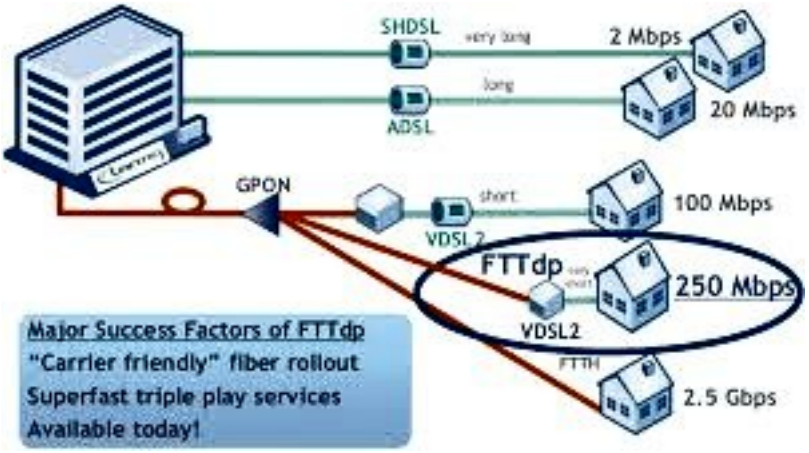

Figure 1 – The FTTdp Option (Image Credit: Lantiq)

Generally the public has a solid understanding of what FTTN represents, but there is less universal understanding of FTTdp. A Telstra pillar or major connection point is clearly identifiable as a node in the FTTN context, although more generally the term 'node' applies to any network connection point. For FTTN we are dealing with upwards of 50,000 nodes across the country, with an average of more than 200 premises per node.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

The FTTdp option is associated with the 'final' copper network distribution point, and the deployment of weather-protected micro-node devices reverse-powered from the premises. Such micro-node devices may serve up to 16 premises in medium density urbanised environments, or 4 premises in a standard suburban environment. We can visualise a FTTdp deployment as placing micro-node devices everywhere the FTTP NBN model would have positioned a 12-port fibre multi-port connector (NBN Co 2012). From these Telstra lead-in pits or overhead poles, the final twisted pair copper lead-in is used. The average copper length in this FTTdp network approach is thus seen to be very short, perhaps 30m, allowing full exploitation of VDSL capabilities such as profile 30a (providing 100Mbps symmetric service over a single pair).

VDSL2 obtains maximum performance with shorter copper lengths, and the very short length of this type of FTTdp deployment enables network capacity to meet the needs of most users for many years, even under scenarios of continued rapid bandwidth demand increases. FTTdp in association with lead-in pit micro-node deployment, allows maximisation of the possibility for bonding pair use and minimisation of crosstalk influences.

G.fast and individual FTTP on-demand upgrades, enable the network to readily cater for those users with even higher levels of connectivity demand. VDSL2 profile 30a is able to provide symmetric 100Mbps down/100Mbps up over short copper lengths (the 30 MHz bandwidth provides limited benefit in the FTTN application, and is generally not used in that setting). Bonding and phantom mode promise significant benefit, and 250 Mbps downstream is commonly associated with short-loop FTTdp.

Some Misconceptions

A common misconception is that FTTdp technology is not ready for deployment. This misunderstanding is most likely related to the subconscious association of G.fast with FTTdp. For maximum benefit G.fast requires very short lengths of copper (less than 80m). The higher frequencies used in G.fast also make it extremely susceptible to crosstalk. New vectoring approaches promise to provide significant improvements here, but it is far from clear how practical G.fast will be in situations where there is a large component of crosstalk (Spruyt 2013). This consequently suggests that G.fast (without vectoring) is ideally deployed in the FTTdp setting where there is limited crosstalk due to reduced prevalence of shared lead-in (Brown, L 2012; Brown, T 2013; TechWeek 2013).

G.fast is not yet ready for widespread FTTdp deployment, although it will soon be, with ratification of the first release of the standard expected any day, and hardware implementations to be available by the end of 2014. By contrast, VDSL2 is most certainly ready for FTTdp deployment. Both Lantiq (Lantiq 2013) and Alcatel-Lucent have weather-

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

protected micro-node equipment using VDSL, reverse powered from premises. Huawei, Adtran, and other major suppliers, either have current product offerings, or are likely to soon have product offerings available in quantity. More recent market entrants such as Sckipio (G.fast) are likely to contribute to a highly competitive market in the near future.

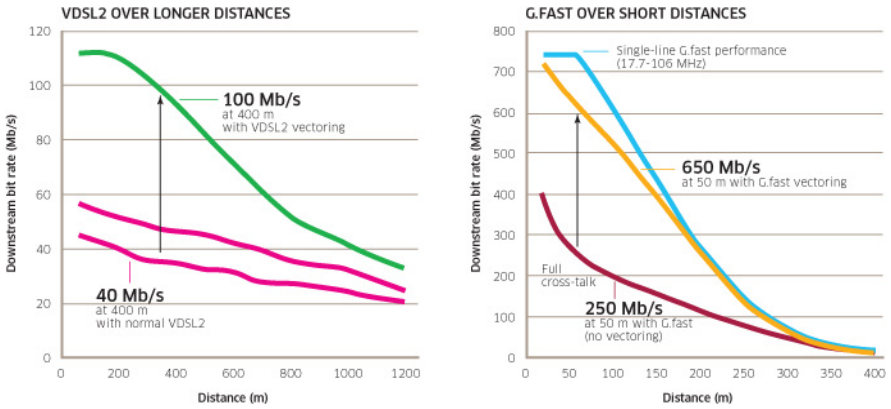

Figure 2 – VDSL2 and G.fast Throughput (Image Credit: Alcatel-Lucent)

The high bandwidth capability of VDSL2 (up to 250 Mbps) for short copper loop lengths translates to throughput capability that will serve the vast bulk of premises for many years into the future, even with scenarios of rapid bandwidth demand increases. For higher-demand premises, individual G.fast upgrade or FTTP upgrade are real options and can be provided for moderate cost due to the simplicity of the plug-and-play equipment upgrade for the G.fast option, and the short fibre deployment length in the FTTP case.

FTTdp thus provides robust and flexible capability, and can be deployed now. A determination of whether it is the most sensible deployment option compared to the other options of FTTN and FTTP must be made on the basis of weighing comparative benefits with costs. Crucially, network benefit can only be properly assessed with a sensible appreciation of network demand projections. FTTdp provides overall network capability very close to that of FTTP, for all but the most severely extreme projections of bandwidth demand. Even here, the fact that the core fibre FTTdp network is readily adaptable to widespread FTTP deployment, means there is very little chance of wasted deployment effort in the scenario where mass upgrade to FTTP occurs in a very short period (the extreme growth projection scenario). The worst case would appear to be scrapping a few hundred dollars' worth of CPE (Customer Premises Equipment) and micro-node equipment per premises, after they have already served the bulk of their anticipated deployment lifetime.

Another misconception is to rely too heavily on looking at overseas deployments of FTTdp to provide a reliable indication of where FTTdp might add value in the Australian NBN context. Recent NBN history clearly points to the fact that the local cost equation is quite different from that in many overseas environments. In particular, widespread deployment of FTTdp is

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

not expected in those nations where construction of fibre premises lead-in drops is economic. In the Australian context the $2100 currently quoted (NBN Co 2013: page 61) for the average brownfield premises lead-in drop connection (mainly due to the tailored civil engineering works required for each individual lead-in and a need to professionally install CPE) is both a large financial outlay, and prevents skilled resources from undertaking other network construction activities, ultimately causing a substantial NBN deployment timetable impost. The reduced cost and time for FTTdp connection translates to large overall NBN Co cost and time benefits. The differences are substantial enough to turn what appears to be a weak option (full fibre FTTP) into a very strong option (FTTdp).

The Evolution of Bandwidth Demand

Direct extrapolation of past consumer access technology bandwidth increases can lead to some astounding projections for future bandwidth demand, including the suggestion that average consumers will require 10 Gbps connectivity within the next decade. These varied projections come from application of Nielsen's Law with small variations of input data (Nielsen 1998). If this proves to be the reality of bandwidth demand evolution, then it is immediately clear that FTTN would be a misstep for the nation at this point in time. However, it is far from clear whether the trends of past consumer access bandwidth supply, extrapolated into the future, give us any reliable estimate of access bandwidth demand in even 5 years (never mind 10 years).

We must delve deeper into the issue of bandwidth demand evolution in order to produce forward estimates that can be relied upon for access network capacity provisioning considerations.

Communications network convergence has been an expectation for a long time, and may now be showing signs of becoming a reality. Consideration of bandwidth demand for Ultra HD 4K video provides a worthwhile proxy for anticipation of broader network bandwidth demand over the next few years. Netflix has recently announced 4K streaming at 15.6 Mbps (CBS News 2014), but we must conservatively estimate the bandwidth demand for 4K video to be between 20 and 25 Mbps. The future impact of 3D 4K TV or 8K TV is difficult to predict with certainty. However, the reality of 4K screen price reductions will see multiple 4K devices in what may be considered average premises within a very short number of years. The NBN must be able to deliver multiple 4K streams to a single premises, as well as facilitate conference video scenarios for multiple simultaneous users. Simultaneous video streaming, from multiple video sources world-wide, is already a reality for many.

Consideration of multiple 4K video streams is a suitable proxy for broad downstream data bandwidth demand, but upload data rate requirements are likely to vary dramatically from

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

premises to premises. Some small enterprises will require more symmetrical upload versus download capacity. With VDSL deployment there is restriction to a single fixed ratio between upload and download due to the necessity of minimising crosstalk implications from the frequency bands employed for the different data directions. The variation in distance from the node, in the FTTN case, creates the situation where this limitation is likely to cause difficulty for some premises. The situation is quite different for FTTdp, with maximum VDSL upload and download capacity effectively supplied to all premises.

The Cost of FTTdp Deployment

Naturally FTTdp involves a significantly deeper deployment of fibre into the access network than does FTTN. However, the cost of this greater fibre deployment is balanced against the higher capital expenditure for FTTN of copper remediation, time-consuming copper patching installation work at the node, the provision of large street cabinets (and associated risk of damage from errant vehicles), the provision of 240 volt power and battery banks to all nodes, the need for cabinet cooling, and more involved deployment cut-over practices. We perhaps do not even need to take the operational expenditure differences into account for working with a greater proportion of the legacy copper network for a cost comparison to become decisive. Distribution of fibres from the node to the distribution point lead-in pits is a non-trivial task, but offers substantial work flow advantages that a centralised FTTN deployment activity schedule does not.

Ultimately, detailed analysis is required to determine which is the cheaper option, when directly comparing FTTdp to FTTN (of the type requiring access to unpublished NBN Co costs). A direct comparison between FTTdp and FTTP is perhaps a simpler undertaking due to the similarity of work effort required in both cases. This allows an indirect comparison of costs between FTTN and FTTdp.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

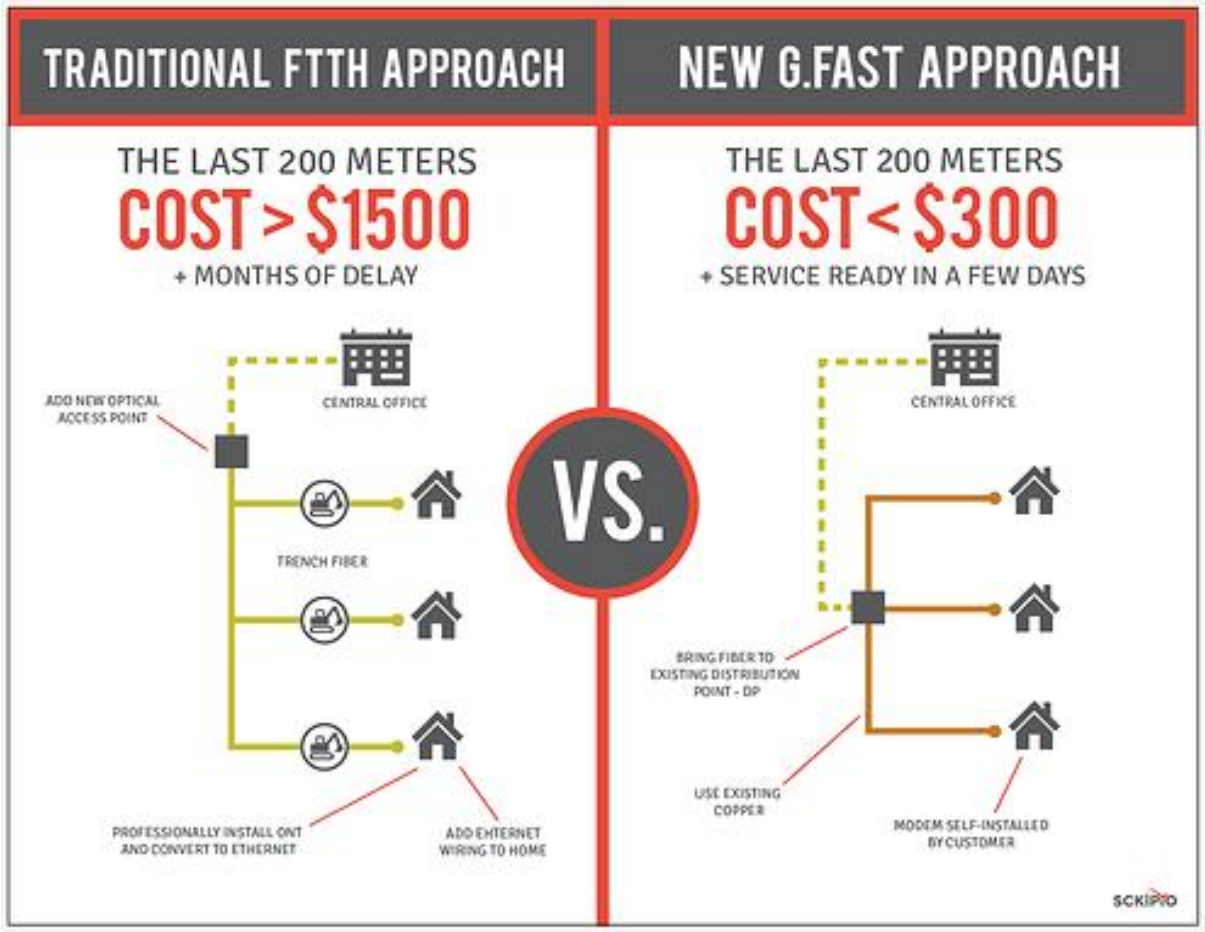

Figure 3 – FTTdp compared with FTTP (Image Credit: Sckipio)

Figure 3 from Sckipio, presents a cost comparison for the FTTdp situation. We have mentioned above how the Australian NBN costs differ markedly from the international experience. However, Sckipio seem to be suggesting that even with the emerging G.fast option for FTTdp (still not a fully mature technology option), the cost of FTTdp is a substantial reduction on the cost of FTTP. We need to ask what corresponding costs should be assumed for the parts of the access network not included in Sckipio's final 200m calculations, but it is likely that the cost of FTTdp even in their estimation is not far above that of the $350 to $700 international FTTN range given at page 78 of the NBN Co Strategic Review report.

The larger cost of the civil work network components in the Australian setting make any cost comparison vastly different to that presented by Sckipio. However, the cost of the FTTdp customer connection in the Australian NBN setting involves only a portion of the work performed for the $300 cost suggested by Sckipio above (being supply and installation in the pit of the micro-node device). This Figure therefore provides a crude, but nonetheless useful, reference point for FTTdp connection costs (exclusive of the fibre network construction cost).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

The NBN Co Strategic Review document (page 61) indicates an average customer connect (lead-in drop plus CPE installation) cost per premises for FTTP of $2100 for approximately 7 million brownfields premises (under the 93% FTTP model). This figure is a significant portion of the $4970 cost for brownfield FTTP extracted from the NBN Co Strategic Review report as outlined in the introduction section. While practically no detail is provided in the NBN Co Strategic Review related to the 'Radically Redesigned FTTP' Scenario 2, there is little expectation of any impact on the customer connection cost in this scenario. The exception is the cost of CPE, quoted to be $80 to $110, likely passed to the RSP (NBN Co 2013: page 82). Subtracting this, the approximately $2000 customer connection cost is then seen as a significant portion of the average $3260 FTTP brownfields cost under Scenario 2.

FTTdp effectively eliminates this $2000 cost of individual tailored civil engineering works at each premises, replacing it with the FTTdp connection cost at the street pit. A device must be installed in the pit and connected to the copper pairs coming from the premises which share the pit (for the NBN Co suburban layout this is an average of 4 premises).

A generous allowance of $800 in equipment costs and $800 for multiple installer visits to the street pit, translates to $1600 in total, for an average of $400 per premises. This represents a saving of $1600 per premises over the quoted costs for FTTP, amounting to $11.2 billion in capital expenditure savings for both Scenario 1 and 2 as presented in the NBN Co Strategic Review report.

These savings come with little impact on revenue or operating costs. Should service adoption rates exceed the 70% used as a conservative estimate, the FTTdp business case improves even further. The marginal cost of connecting additional customers to a FTTdp network is very small (involving no additional network equipment and a few additional minutes of work time if performed as part of the primary connection process, and a single-person-crew attention to a task taking minutes only if performed at a later stage).

Widespread FTTdp deployment based on Scenario 2 must be analysed in more detail on the promise of this simplistic cost analysis. However, the more sensible approach is to consider the adoption of HFC and FTTB (Fibre to the Building/Basement) such as starting from Scenario 4 as a baseline. Here the lower number of FTTP premises in Scenario 4 translates to a reduced saving from the FTTdp approach, amounting to $6.2 billion.

This modified Scenario 4 then looks very favourable in terms of costs compared to all the other technology mix scenarios presented in the Strategic Review document. The network capability benefit, including the vital benefit of network flexibility to handle higher rate CIR (Committed Information Rate) services, high demand users, and higher traffic demand

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

profile increases, is significantly improved compared to other scenarios involving substantial FTTN deployment.

Note the capital expenditure shown on page 17 of the NBN Co Strategic Review report does not show a significant decrease from Scenario 2 to Scenario 4, which it presumably should if the substantial savings from the FTTP radical redesign have been carried across to Scenario 4. Assuming 50% of the Scenario 2 (FTTP radical redesign) savings are applicable to Scenario 4, the capital savings would amount to $6 billion. The total FTTdp savings of just over $12 billion brings the total FY11-24 cumulative capital expenditure for FTTdp to $28 billion. The figures NBN Co use and supply have significant uncertainties, and this number has even poorer accuracy, due primarily to a lack of published cost information from NBN Co. However, the potential saving is enticing enough to warrant closer analysis by NBN Co.

Additional FTTdp Benefits

In addition to obtaining extremely high VDSL performance, the FTTdp approach eliminates upwards of 90% more of the copper network compared to FTTN (on a lineal pair measure basis). The elimination of the vast majority of copper pair connections is a major advantage, even if we assume that there is no major network-wide corrosion problem with poorly sealed joints or a major issue with faulty gel sealant material.

Passing the cost of CPE more directly to end users, most logically through RSPs (Retail Service Providers), is unlikely to meet with significant objection under the FTTdp model. VDSL modem equipment is expected to be readily available at reasonable prices from a large number of suppliers, as is clearly the case today for ADSL modems. (The same claim can be made with FTTN, but CPE equipment costs for FTTP presents some concern with how these are likely to be passed to customers and not act to slow service uptake, especially if this cost also includes the necessary professional installation of the FTTP CPE.)

Cut-over from a telephony/ADSL connection to an NBN FTTdp connection can easily be accommodated by a single person mobile unit needing to work only at the lead-in street pit location. Workloads in any one area can be balanced by scheduling, with new CPE posted or delivered to end-user premises ahead of the scheduled time of disconnecting the old CPE and connecting the new equipment.

Micro-node devices, certified by NBN Co for use on the NBN, can be installed and tested as part of the FTTdp fibre deployment or on an as-needed basis for connections. Both approaches have pros and cons, and an optimised approach may involve a mixture. (Presumably equipment can be installed in lead-in pits as part of the fibre deployment where there is a high likelihood of services being ordered, determined from data on existing ADSL and phone connections and other sources.) In either case, the skill set required for premises

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

connection is modest and mobilisation of a large workforce of individual contractors, certified by NBN Co to work on the customer end of the NBN, is a realistic expectation.

The FTTdp approach encompasses reduced LFN (Local Fibre Network) fibre counts and substantially reduces the size of splitter cabinets required (FDH, Fibre Distribution Hub, enclosures). This opens the prospect of splitter infrastructure being retracted into pits, away from vandals, errant vehicles, and falling branches. The reduction in impact of street furniture is a major positive consideration compared to the FTTN approach. Large cabinets for FTTN present a very real site location problem that altered legislation does not 'solve'. NBN Co and the government cannot expect to win the hearts and minds of the masses by ignoring genuine public concerns.

The benefit of reduced LFN fibre counts is unclear in terms of impact on deployment costs. Presumably smaller and lighter cables are somewhat easier to pull or blow through conduits, in addition to general handling and transport benefits. Small incremental differences in costs can translate to large savings over the size of the NBN project. The complexity of the task of accurately patching LFN fibres at the FDH is reduced dramatically when there are only 50 or so fibres to contend with compared to 600 in the NBN Co FTTP approach.

On the downstream side of the splitter (LFN) there is the potential to use loose tube fibre bundles from 6 to 24 fibres (corresponding to the 72 to 288 fibres in the initial FTTP approach). A single fibre goes to each micro-node device. In reality some additional fibre capacity would be included in the bundles. For FTTP upgrade the micro-node device is replaced by a small splitter (a dual-stage optical splitter FTTP implementation thus results). Micro-node devices with integrated splitters are clearly not difficult to envisage.

The small size of a connector for a single fibre compared to a 12-port multi-port enables some flexibility in terms of the LFN deployment. Presumably a major component of the cost in the LFN deployment is not pulling the fibre itself, but ensuring that multi-ports present at the right locations in the pits.

Suggestions of major potential LFN deployment cost savings from FTTdp are speculative, but warrant close examination. NBN Co is able to supply the detailed cost information required to properly delve into such matters and should undertake a comprehensive analysis. Some of these cost savings may already be exploited by the radically redesigned FTTP Scenario 2, presented in the NBN Co Strategic Review report.

FTTdp Upgrade Options

A FTTdp deployment involves deep fibre penetration into the network. Any network upgrade is largely a premises-by-premises decision. There is no need for another additional major

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

nation-wide network construction process with the FTTdp approach. Upgrades to G.fast or FTTP can occur on an individual premises basis in accordance with demand, facilitated by a thriving ecosystem of small contractor specialist installers. The very high capability of short-loop VDSL in the FTTdp setting (including use of bonding and phantom mode), implies a small initial demand for individual capability upgrade. (This is important as it does not withdraw resources from the ongoing main network build.) Over time, with increasing network demand growth, we would expect a steady stream of premises wishing to upgrade their connectivity. The volume of upgrade activity will obviously be dependent upon actual bandwidth demand growth. High capability of the initial VDSL FTTdp deployment ensures that a large number of premises will continue to be well served by the initial technology deployment for the longest possible time.

The coming G.fast option ensures that the gap between VDSL performance and the investment involved with individual FTTP upgrade is bridged. However, it remains to be seen whether G.fast will be practically viable enough to warrant implementation in more than a small number of situations. Again, the robust capability provided by VDSL in the FTTdp context ensures that there are a number of years ahead, prior to G.fast implementation needing to be considered for more widespread deployment. By then G.fast implementations will be mature, and cost and performance considerations of the technology will be more readily understood. Any potential G.fast FTTdp deployment must be balanced against the relatively modest cost of individual FTTP fibre deployment (note that this premises fibre lead-in drop is largely through property controlled by individual premises owners, and distributing control of this fibre connection to premises owners is likely to result in optimised cost outcomes).

It should be noted that G.fast is capable of interoperation with VDSL by choosing to limit the G.fast deployment bandwidth to commence above the 17 MHz or 30 MHz VDSL profile band. In the FTTdp scenario it is also conceivable that all users connected to a micro-node would be upgraded to G.fast at a single time, thus not requiring interoperability and using the full bandwidth for G.fast. However, it is pointless to speculate on what is likely to be the most sensible approach to an upgrade problem not likely to emerge for a few years, if at all.

We need to contrast this flexible upgrade capability of FTTdp with the prospect for FTTN. Due to the large copper lengths and shared lead-in of FTTN, G.fast has little scope for provision of significant benefit. Likewise, VDSL profile 30a, bonding, and phantom mode offer little potential gain in the FTTN setting. The high cost of individual FTTP upgrades from a FTTN node is likely to suppress latent demand for such upgrades. As dissatisfaction with FTTN capabilities grows, we can expect to see ad hoc deployment of fibre past the node.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

Whether an ultimate decision is made to deploy FTTdp or FTTP, it is not clear whether the ad hoc fibre deployment investment can be fully exploited.

Additional Cost-Benefit Considerations

Crucially, the requirements of high-demand users are met by the FTTdp build, effectively to the same level they are met with FTTP. We must not be tempted to think that high-demand users represent only a small percentage of the total user base of the NBN and that their requirements should only be weighted in proportion to their number. The NBN represents important national infrastructure. Communications networks are inextricably linked to the modern global, and rapidly evolving, economy. A significant proportion of high-demand users are likely to be involved with ventures that represent a growing component of the national economy. High technology web companies are part of this equation, but greater use of networks is implicit in almost every sector of our modern economy.

Business investment in smaller organisations can be expected to be predicated on reliable network connectivity that promises to grow with the business. A fibre-on-demand model for individual FTTP connection in a FTTN deployment meets some of the generic requirements of business customers, but it presents uncertainties related to high cost and installation time (being dependent on arranging a tailored major fibre installation by NBN Co). While these issues do not pose a major threat to many businesses, they are likely to be significant concerns for others. The FTTdp model provides baseline capability that will suffice for the majority of customers, adding simple upgrade options. As such, it instils communications capability confidence for businesses, providing a communications technology roadmap that can be relied upon.

The prospect for uniform retail product offerings across the breadth of the NBN is significantly greater with FTTdp than with FTTN. The extra complexity of not being able to supply a largely uniform retail product set with FTTN has business cost implications for RSPs.

Deployment of new overhead or underground HFC infrastructure is not likely to be materially different in cost and time compared to provision of FTTdp. With the latter option there is a significant simplification in the premises connection as this can be implemented from the lead-in pit. FTTdp must thus be properly considered for use in HFC black spot areas. Neither FTTN nor FTTP offers the strong cost-benefit equation of FTTdp for such use.

For very small gaps in HFC coverage (hardly describable in terms of a black spot), running new HFC infrastructure is likely to be the only sensible option.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

Conclusion

The 2013 Australian federal election campaign presented an FTTP option against FTTN. The former has been criticised as too costly, while the latter may not provide a sufficient 'future-proof' capability. Following the lead of Gregory (2013), this paper presents the third option of FTTdp. It is suggested that FTTdp may provide network capability close to that of full FTTP, with cost similar to FTTN. FTTdp may provide optimal ability to meet the unknown, yet high, anticipated bandwidth demand of the future, with comparatively low initial capital outlay.

Widespread deployment of FTTN runs a very real risk of supplying inadequate network capability, and provides limited flexibility in meeting large premises-to-premises demand variation. FTTP on the other hand appears to have failed to meet most promises of deployment cost and timetable (in the Australian NBN context).

FTTdp can be viewed as a middle-ground solution for brownfield NBN deployment. (For greenfields there is strong reason to suggest that FTTP is the only sensible choice.) The very short copper lengths of FTTdp imply that VDSL rates will be high enough to meet the needs of all but the most demanding users for the immediate future. G.fast also promises a convenient upgrade path. An on-demand, user-pays fibre lead-in drop model completes the equation in terms of flexibility and network longevity. The small FTTdp node devices are powered from the premises over the copper, and there is no need for large (and unpopular) street cabinets. The likely availability of multiple lead-in pairs for many premises allows pair bonding and phantom mode for maximal VDSL2 (or G.fast) performance. Splitter fan-out is significantly reduced compared to FTTP, allowing the possibility of street furniture greatly reduced in scale, including solutions where the splitter frame is retracted into a pit. Greatly reduced LFN fibre counts compared to the default FTTP model used by NBN Co to date, introduces the prospect of substantial network deployment cost savings on the LFN side in addition to major savings on the customer connection.

Mainstream FTTdp NBN deployment must be thoroughly analysed. In contrast to FTTN it promises a single network build, long-term solution. The fibre drop portion of FTTP is eliminated due to the use of existing copper pair lead-ins, translating to a substantial deployment cost saving. FTTdp has the advantage of eliminating somewhere up to 90% of the legacy copper network compared to FTTN. Importantly, the majority of the copper joints are eliminated.

If we start from a baseline assuming the use of HFC, similar to Scenario 4 in the Strategic Review, the saving from FTTdp (based on little more than back-of-the-envelope analysis) is approximately $6.2 billion (with a potential further $6 billion saving in already-identified

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

NBN Co fibre deployment initiatives). While the cost equation is appealing at this simplistic level, a decision to pursue a FTTdp trajectory versus a FTTN one must clearly be made on the basis of a consideration of both costs and benefits. Here the network utility provided by FTTdp is a large improvement over that provided by FTTN.

The cost savings of the FTTdp approach correspond to a workforce saving that translates to more skilled resources being available to accelerate the network deployment timetable.

Primary use of FTTdp is likely to lead to some revenue upside compared to the FTTN case, due to the higher connection throughput and the greater ability to offer high CIR products. The revenue upside could be substantial in FTTdp should subscriber numbers be driven upward. For FTTP, similar revenue increases come at additional large customer connection costs that simply do not apply in the FTTdp case.

A more sophisticated analysis such as that performed for the other technology options in the NBN Co Strategic Review report may indeed determine that widespread FTTdp is the obvious technology choice from all angles: chiefly cost, time, revenue, and capability (benefit).

Polarised views will continue to plague the NBN initiative while FTTN is selected as the primary deployment technology. We can expect that within as little as three years, one side of this debate will be able to point to enough external developments to quieten objection from the other side. The risk in FTTN is that we may be on the wrong side of the equation, with migration to FTTdp or FTTP required on such a short time-scale that in hindsight, FTTN becomes a clear misstep. FTTdp holds the promise of eliminating the vast majority of any polarised debate from square one (and may do so with no additional cost implications). The nation must honestly investigate this option.

References

Brown, L. 2012. 'G.fast for FTTdp'. Available at: http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B0000320009PPTE.ppt, retrieved January 12, 2014

Brown, T. 2013. 'UK G.Fast trial gives hope to Australian copper networks'. *Australian Financial Review*. Available at: http://m.afr.com/p/technology/uk_fast_trial_gives_hope_to_australian_oki4JLC5zr3VTbozq8J6uJ, accessed January 8, 2014

CBS News. 2014. "Netflix app to stream 'Ultra HD' 4K video on new TVs". Available at: http://www.cbsnews.com/news/netflix-app-to-stream-ultra-hd-4k-video-on-new-tvs/, accessed January 14, 2014

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.26

Eckermann, Robin. 2013. 'Getting some reality into debates about NBN FTTP', *Australian Journal of Telecommunications and the Digital Economy* 1(1) pp. 13.1-13.19, DOI: http://dx.doi.org/10.7790/ajtde.v1n1.13. Available at: http://telsoc.org.au/journal, accessed January 14, 2014.

Gregory, Mark A. 2013. 'A flexible upgrade path for the Australian National Broadband Network', *Australian Journal of Telecommunications and the Digital Economy* 1(1) pp. 17.1-17.7, DOI: http://dx.doi.org/10.7790/ajtde.v1n1.17. Available at: http://telsoc.org.au/journal, accessed January 14, 2014

Lantiq. 2013. 'Fibre-to-the-Distribution-Point (FTTdp)'. Available at: http://www.lantiq.com/uploads/media//2013_Lantiq_Aethra_FTTdp_Solution.pdf, retrieved January 21, 2014

Minister for Communications. 2014. 'Panel of Experts to conduct cost-benefit analysis of broadband and review NBN regulation' Available at: http://www.minister.communications.gov.au/malcolm_turnbull/news/panel_of_experts_to_conduct_cost-benefit_analysis_of_broadband_and_review_nbn_regulation#.UwV0TdSSyhM, accessed January 6, 2014

NBN Co. 2012. Network Design Rules. Available at: http://www.nbnco.com.au/assets/documents/network-design-rules-2012.pdf, retrieved January 8, 2014

NBN Co. 2013. Strategic Review, Final Report (with redactions). Available at: http://www.nbnco.com.au/content/dam/nbnco/documents/NBN-Co-Strategic-Review-Report.pdf, retrieved December 12, 2013

Nielsen, Jakob. 1998. 'Nielsen's Law of Internet Bandwidth', available from http://www.nngroup.com/articles/law-of-bandwidth/, accessed January 12, 2014

Spruyt, P; Vanhastel, S. 2013. 'The numbers are in: Vectoring 2.0 makes G.fast faster'. Alcatel-Lucent Techzine. Available at: http://www2.alcatel-lucent.com/techzine/the-numbers-are-in-vectoring-2-0-makes-g-fast-faster/, accessed February 9, 2014

Swisscom. 2013. 'Swisscom chooses Huawei as supplier for its FTTS expansion', Press Release, February 12, 2013, Available at: http://www.swisscom.ch/dam/swisscom/en/ghq/media/MM/2013/20130212_MM_Huawei_FTTS_Ausbau_en.pdf, accessed February 20, 2014

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.26

TechWeek Europe. 2013. 'BT To Trial Huawei G.fast FTTdp Copper Broadband Technology'. Available at: http://www.techweekeurope.co.uk/news/huawei-gfast-fttdp-copper-bt-129855, accessed January 8, 2014

Watkins, C; Lillingstone-Hall, K. 2014. 'Technology Considerations for the Australian National Broadband Network (NBN)'. Available at: http://www.aph.gov.au/DocumentStore.ashx?id=710cc710-251a-4246-b9dc-30a6a5551c36&subId=32304, retrieved February 3, 2014

Endnotes

1. The authors contributed a substantial document to the Senate Select Committee on the National Broadband Network on the 31st of January 2014 (Watkins 2014). The most significant recommendation of that contribution was the need to properly investigate the option of Fibre-to-the-Distribution-Point (FTTdp) as a major NBN deployment alternative. This short paper aims to focus solely on the FTTdp option and highlight key considerations of the technology.

Cite this article as: Watkins, Craig; Lillingstone-Hall, Kelvin. 2014. 'The FTTdp technology option for the Australian National Broadband Network'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 26.1-26.18. DOI: http://doi.org/10.7790/ajtde.v2n1.26. Available from: http://telsoc.org/journal

The Cloud and data sovereignty after Snowden

David Vaile[1]
Co-convenor, Cyberspace Law and Policy Community,
UNSW Faculty of Law

The Snowden revelations have renewed interest in questions surrounding jurisdictional issues about where data is kept (location) and who claims the capacity to direct access to it be given by the entity hosting it (control). While early attitudes to the cluster of technologies marketed as The Cloud generally played down this aspect, and unilateral contracts offered by many major providers declined to specify these parameters for the technical provision of a Cloud service, growing appreciation that assurances of security and confidentiality are no barrier to certain forms of access being granted to third parties in other jurisdictions has rekindled interest. This paper explores the technical and legal issues involved from the perspective of an Australian business interested in both customer and government attitudes, and discusses how moves to implement jurisdiction location and control preferences have been characterised as Data Sovereignty and Digital Protectionism by differing interests.

Contents

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

1. Introduction

> *'Then data sovereignty, privacy and security—the importance of trust. ... We conducted a survey [in 2010] of 500 consumers in Australia. ... [T]he number one thing was that Australians were the most extreme in their responses [in] five out of six categories compared to any other country in the world. The only country more extreme about the data was Germany.*
> ...
>
> *Australians didn't trust the government with their data: only 20 per cent trusted the government. They trust IT companies [even] less than the government. ...*
>
> *Australia was the most extreme out of the countries we [surveyed] about keeping data on shore. The data needed to be kept in Australia. So it's not just some rule that APRA's made up or the Privacy Commission's made up. It actually reflects Australian consumers' attitudes to data. They want to keep it here'.* (Baty 2011)

What have become known as the Snowden revelations started in June 2013 with stories in the *Guardian*, *ProPublica*, *Washington Post*, later *New York Times* and *Der Spiegel*, and more recently the new online vehicle *First Look*. The scope of the extracts from a cache of tens or hundreds of thousands of files copied from NSA sources by Edward Snowden is remarkable. They purport to reveal an international network of surveillance practices by members of the Anglophone "Five Eyes" intelligence and national security "community" that extend far beyond popular understandings of the controlled and specific powers to tap telephones for law enforcement purposes dramatized by TV's *The Wire*. Critical attention has focused on what seems to be an omnivorous global dragnet based on warrantless, suspicionless mass surveillance programs with ominous names such as BOUNDLESS INFORMANT, collecting digital metadata and some content data both by the legal means we consider below, and by other technical means that bypass the need for cooperation from the Internet backbones, cloud hosts and telecommunications utilities pressed into service by those legal means.

The revelations have bolstered the need to re-assess issues of 'data sovereignty' in the Cloud (an online service delivery method the technical models for which are set out below). These issues, discussed in this paper, had already been coming to attention in countries around the world, including through scholarly work such as that of Dan Jerker Svantesson (2013) and

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Christopher Kuner (2010) and attention in EU's Article 29 working party and OECD medical informatics circles, but the frequent absence of concern for the expectations of "non-US persons" in the debates following the exposures have confirmed the need for caution, both in relation to the actual practices revealed, and to the potential for similar hazards in other jurisdictions not similarly exposed, and other business practices in cross-border Cloud services. The time for a more traditional, sober analysis of liabilities, risks and benefits has arrived. The carefree, boundless honeymoon of the Cloud is over.

While the Australian Law Reform Commission and parliamentary committees the mid-2013 developments mean renewed attention in Australia is being directed to issues arising from storage of business and personal data in the Cloud, building on trends already identified in the industry insider Baty's view quoted above, coming to us from a more innocent, pre-Snowden era. We investigated questions such as the following:

- How can Cloud services be used safely, and when can they be dangerous?
- What is 'data sovereignty' in the Cloud? Does anyone know or care about legal jurisdiction over data in the Cloud, or is 'cyberspace' somehow beyond such administrivia, as customers are implicitly invited to imagine by some Cloud proponents?
- What happens if you ignore data sovereignty in the Cloud? Does it really matter where data is stored, or by whom?
- Will you be able to rely on Cloud data stores when you need them? Will you be able to protect them against unwelcome adverse access or retrieval by parties other than the data owner and their authorised agents?
- In a court case, could you prove and exercise your/the owner's rights to control, access or delete data held in the Cloud?

The Australian Communications and Media Authority chair explains data sovereignty as "the ownership of data and access to data stored in countries, other than the one where the end user resides, including relevant redress mechanisms and the capacity of citizens of Australia to take action or seek redress against cloud providers in other jurisdictions" (Chapman 2013).

Many organisations' document or data management policies may not yet adequately cover *data jurisdiction,* the key issues of *where it is located* and *who has the capacity to control it*, nor recognise challenges thrown up by a somewhat chaotic, rapidly-evolving cloud services environment increasingly integrated with 'Big Data' capacities (Mayer-Schonberger & Cukier 2013).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Governments and regulators seeking to "drive confidence among businesses and users that cloud service contracts will be designed with relevant risks and benefits that have been appropriately weighted and addressed—'balanced' (Chapman 2013) — may also have to pay more attention to the 'risk' side of the equation in this jurisdictional area. A feature of many Australian Cloud policy and strategy documents[2] appears to be an almost boosterish urge to encourage and foster Cloud take-up for its own sake (no doubt welcome to the ears of cloud providers): identifying the benefits, but tending to leaving the hazards, especially those related to jurisdiction, un-named or relegated to a footnote (DBCDE 2013; AGIMO 2013). Confidence may be better served by a more detached, fine-grained risk/benefit assessment of the match between your own data's sensitivity and needs, and the willingness and capacity of Cloud services to deliver reliably, including the potential effects of where they are located and by whom controlled, and the regulatory regimes that become important when things go wrong.

This paper looks at issues affecting data sovereignty in the cloud, and their implications for managing the potential risks and rewards of handling new cloud services safely. The focus is the Australian jurisdiction, but the principles in government policies, standards, case law and even legislation are increasingly being reflected in different jurisdictions around the world. Some countries play a more central role in the cloud industry than others; we offer international equivalents and comparisons to put the differences and similarities in context.

How do cloud legal issues in relation to jurisdiction or location differ from those arising from conventional outsourcing or hosting?

It is easy to exaggerate the difference a Cloud makes. In many ways, the issues start from the same foundation. Traditional hosting or server hire contracts involve use of someone else's storage or computers. "But it would normally have been clear who you were dealing with and where your rented resources were. Such arrangements were also unlikely to have been established on a casual or informal basis. With cloud computing, however, the location(s) of your data [and under whose jurisdiction they fall] may be unclear, possibly even unidentifiable and it is also much easier to set up such an arrangement. The ease with which cloud resources can be allocated and reallocated makes it more likely that it will be done without an appropriate review of the relevant legal issues." (QMUL 2010)

Why are cloud sovereignty and data jurisdiction important?

Most documents are now digital and networked

Once removed from the physical constraints of hard copy, networked digital documents can be copied and moved between locations or jurisdictions with trivial effort.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Foreign litigants and governments have a much easier time getting access to your data if it is within their jurisdiction

While there are international or inter-country arrangements which enable access in or from other countries, most countries favour access requests made in relation to local documents, or documents under the control of entities over whom they have jurisdiction.

Laws in other countries may be quite different from those in your own country.

Third party legal access options, including detailed comparisons of mechanisms for such access under Australian jurisdiction and under that of the main cloud hosting forum, the US, are complex, so we discuss some examples in section 4 below.

Cloud data storage contracts may be on terms unfavourable to users, or silent on key issues

Particularly for Web-grade IaaS (Infrastructure as a Service; see below for cloud acronyms), service provider business models may rely on excluding liability for matters which may be within their control. Typical SaaS (Software as a Service) host models may also depend escaping liability for such matters.

Some countries or jurisdictions may have worse IT, security or privacy protections for your data than Australia; or their protections may be harder for local subjects or owners to use

The evolution of business, legal and technical support for adequate online security, confidentiality, privacy and/or data protection vary greatly from country to country. International agreements such as the *Convention on Cybercrime* from the Council of Europe (CETS 185, in force in Australia from March 2013) arose to address this in some areas, although recent developments in aggressive surveillance and associated moves by agencies to undermine cryptographic standards have suggested that it may have paradoxical effects in others, potentially reducing security and confidentiality against the intervention of foreign agencies. Many countries (although probably the minority of major cloud participants) are not a party to relevant agreements; some of them also have quite underdeveloped legal coverage of online issues generally, and may not support a robust confidentiality and privacy regime.

And those who are parties to a Convention may have varying implementations of its model laws, and differences of focus between enforcement and confidentiality. The US and Italy for instance have exposed their citizens to fewer of the more extreme effects of the Convention than has Australia, meaning that rights and obligations may not be symmetrical (differing attitudes to strictness of requirements for dual criminality, or to weakening the need to prove a mental element in certain cybercrime offences are examples).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Practical IT security implementations, or the degree of protection of Australian-owned data from third party access, will vary according to these and other local factors. This is a major feature of the paper.

Increased scrutiny and professional liability

Inability to either produce data in response to legal request, or to protect it from unwanted demands from third parties, may create a significant governance impact. Such an outcome, in the worst case, may mean not only is the future of the organisation at risk, but also the personal reputations (or even the civil or criminal liability) of those directors or executives who lead it.

Strategic importance to the organisation: methodical solutions needed

The judicial gaze has begun to focus upon the entire stores of information held by companies, and how companies deal with, and secure or fail to secure, those stores. Governments increasingly require transparency around IT security failures (data breach notification); a version of the 2013 Privacy Alerts bill to amend the *Privacy Act 1988* (Cth) to make such notification mandatory, consistent with expectations in many US and EU jurisdictions, may yet be reintroduced. And every Internet user has been alerted, by the media at least, to the risk of their data being subject to access by unwanted parties (albeit at some risk of 'data breach fatigue' if they are not given practical response options).

Corporations that do not have in place strategic, comprehensive and reasonable data storage, location and jurisdiction policies, methodically and consistently adhered to in implementation, chance a fate serious in its potentially destructive outcomes, if the ire of judicial, regulator or market condemnation falls upon them. While many escape serious consequences (Telstra's recurrent large scale breaches come to mind), the risk of such condemnation remains.

What is cloud data?

Companies and individuals generate a plethora of digital documents, all of which are now candidates for, or generated by, cloud storage. For example:

- Images and recordings from mobile or other devices
- Imaged versions of original paper documents
- Files (including word processing, spreadsheets, presentations)
- Email (including email messages, instant messages, logs and data stores)
- Databases (including records, indices, logs and files)
- Logs (including accesses to a network, application or Web server, customer tracking or profiling)
- Transaction records (including financial records)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

- Other forms of meta-data
- Web pages (whether static or dynamically constituted)
- Traditional audio and video recordings and streams
- App data sets
- Software itself may constitute a significant cloud data holding
- Access control information and passwords

2. Types of Cloud Services

Different cloud models implement varied technical and processing attributes, and raise a range of different legal and policy issues around data sovereignty.

Cloud Service Models

Cloud computing services come in three main "Service Models", which vary according to the extent of the stack managed by the vendor compared with that under the control of the customer, and thus the level of interaction between the cloud service and the data it is holding.

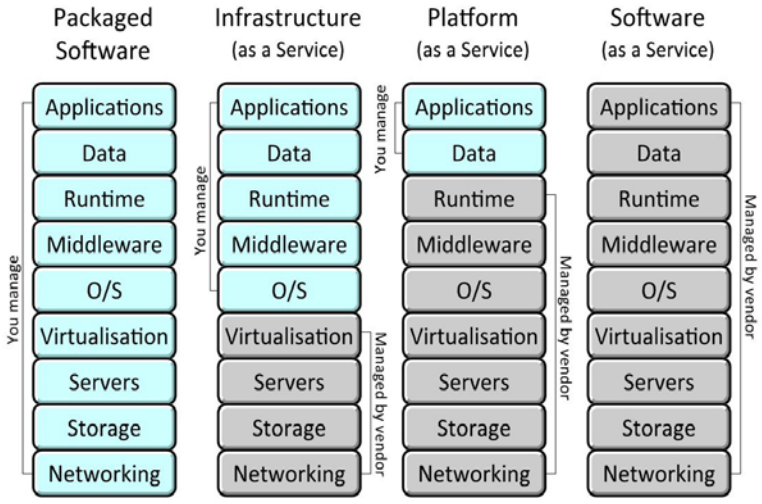

Figure 1. Cloud Service Models ***(Ludwig 2011, after Microsoft)*** [3]

Infrastructure as a Service (IaaS)

Here the relationship and interaction between the cloud service and the data may be small or minimal. With "Infrastructure as a Service", the service is limited to the provision of the infrastructure needed.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Platform as a Service (PaaS)

Interaction is medium when the cloud provider furnishes hosting and a platform, but not the specific applications running on it. This model is known as "Platform as a Service."(Gilbert 2010)

Software as a Service (SaaS)

The interaction may be large or frequent in "Software as a Service." The SaaS customer has access to a wide range of capabilities; the cloud provider furnishes hosting, storage, platform, as well as software applications for immediate use with the customer's data. Many consumer Cloud offerings like FaceBook, Google Docs, Apple iCloud or Microsoft OneDrive include core SaaS features.

Other Service Models?

Some commentators (Gilbert 2010) suggested other Cloud Service Models but the ones set out above appear to be a useful core set for most purposes.

Cloud Delivery Models

Cloud computing capabilities can be implemented and used in four main "Delivery models": Public, Private, Hybrid, and Community. The choice of delivery model has significant effect on the nature, content, and terms of the Cloud contract, and associated risks.

Public Cloud

The public cloud infrastructure is made available to the public, or a large industry group, and is owned by an entity selling cloud services. It is potentially the lowest cost model, especially if at the 'Web-grade' rather than 'Enterprise Grade' end of the assurance spectrum. This is more accessible to small entities, but the terms and negotiability of the contract usually offer limited comfort. Most Amazon Web Services fall into this category, as do many offerings from Google, Facebook, Apple and Microsoft.

Private Cloud

The private cloud infrastructure is operated solely for an entity. It may be managed by the entity or a third party, and may exist on-premises (presumably avoiding sovereignty or jurisdiction issues) or off-premises (which could be anywhere). It is more attractive to larger entities and government because of their greater capacity to manage their part of the investment and support required.[4] Many of these are not publicly visible, because they do not need to be.

Hybrid Cloud

The hybrid cloud infrastructure combines private, community, or public Clouds that remain unique entities, but are bound together by standardized or proprietary technology that

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

enable data and application portability, such as when cloud bursting for load-balancing between clouds. Many of the public cloud providers also offer private options, and can integrate the two. Data of different categories or sensitivity may thus be hosted in different delivery models, or indeed in different locations or under the control of different entities.

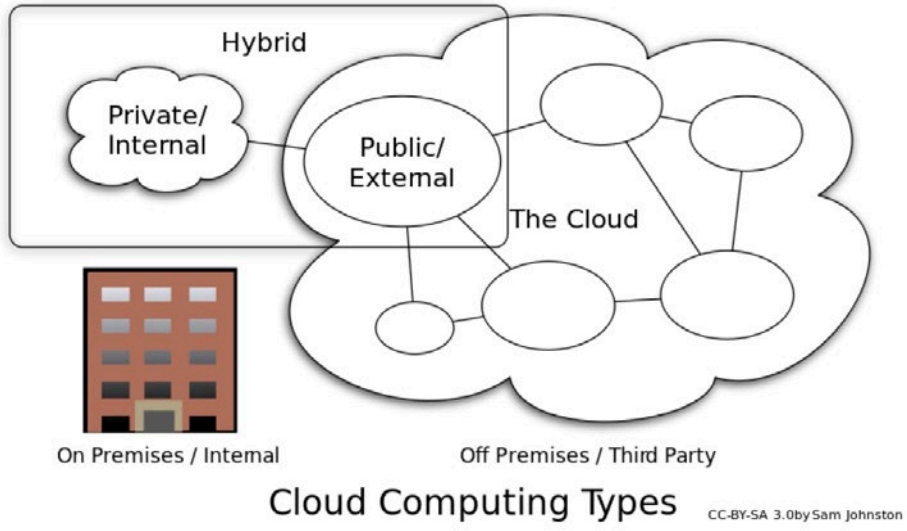

Figure 2 – Types of Cloud Computing [5]

Community Cloud

This approach is less common, typically used by government. A community cloud infrastructure is shared by several entities, supporting a community that has shared concerns, such as the same mission or policies, or similar security requirements or compliance considerations. It may be managed by the entities or a third party, and may exist on or off premises. (Gilbert 2010) Many government cloud installations are candidates for such a model.

Some features and risk attributes are shared by all Cloud models, while others are more applicable to particular models. We only refer to a particular model if it is relevant for a particular risk or feature. Often by default it will be public Cloud delivery model, although off premises private clouds.

Real world: A mix of models and risks

The issues under consideration when we look at an actual Cloud implementation instance will vary depending on the service, the business, and the data held by the service. Most customers in reality use a combination of cloud service models depending on the type of service needed, the utility of the service offering, and the risk of the data.

- For example, in an Infrastructure as a Service (IaaS) arrangement, the service provider would not be expected to have any access to data at all.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

- Some service providers also provide SaaS where all data is encrypted from the customer's desktop: this means data is not accessible by the service provider either.

This question of who can see the data, and on what basis, is important to the overall risk of putting data in the cloud, and should be a focus of analysis. Service and Delivery Models are a useful framework for this, but it is critical to understand the details of data access, and weigh up the actual risks of a particular Cloud implementation.

A related issue is important for discussions about access to data by regulators (including those discussed in the Third Party Access section below): as a practical matter, law enforcement is unlikely to know that a particular company has data in one of the many cloud services operating in a jurisdiction, under whatever Model, so the best way to get data from a company may be to just directly order that the company deliver it up!

Where the data is stored or hosted in a jurisdiction but the legal entity is absent from it, the risk that the cloud data will be located and accessed by law enforcement may be higher or lower than if they were present, depending on configuration, contract and control details. (However, if the revelations in the documents leaked by whistleblower Edward Snowden are accurate, this risk is probably often higher than earlier appreciated, given the apparently omnivorous appetite for metadata surveillance by members of the 5 Eyes group, and possibly others.)

It is also useful to give close attention to the characteristics of the data, and the risks that different categories of data carry: only some classes of data are actually dangerous if lost. There is of course typically the embarrassment of a data breach: note the recent finding by ACMA against AAPT (ACMA 2013), the new penalties, and actual and proposed new disclosure obligations in the *Privacy Act 1988* (Cth)[6].

But it is also important to ask, how often is money or valuable data actually lost? The Verizon Data Breach Report (Verizon 2013) has examples with detail of the types of breaches and the proportion where the information lost actually could cause loss. The incidence of loss, and the security response appropriate, will vary from case to case. (The Privacy Amendment (Privacy Alerts) Bill 2013,[7] the disclosures starting June 2013 (Greenwald 2013; Gellman and Poitras: 2013) and still continuing regarding secret NSA, GCHQ and related surveillance programs for data mining telecom and Internet providers, and the *Australian National Cloud Computing Strategy* (DBCDE: 2013)[8] combine to elevate cloud computing to the top of risk management considerations.)

Having outlined the Models by which Cloud services can be categorised, and considered some of the real world complications which show that the devil is in the detail rather than

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

the model, we turn now to the question of the exposure of data to third party access in the main Cloud hosting jurisdiction, the US.

3. Data Sovereignty Risk Management Issues

There are many practical reasons a company or agency might be cautious about having its data transmitted beyond its own national borders, or held by entities under another jurisdiction's supervision.

Offshore data centres in distant locations are obviously more difficult to monitor than local ones. Moreover, some parts of the world are simply more vulnerable to natural disasters, wars, so-called "acts of God," or government intrusions.[9] Chief among the multitude of concerns about cloud computing is the fear that a business could have its data transferred to or into the control of an undesirable jurisdiction, without its knowledge or approval, and become subject to unacceptable exposures and legal obligations.

The concept of "data sovereignty", introduced above, refers to both specific data sovereignty laws limiting cross-border data transfer, as well as the more general difficulty of complying with foreign legal requirements that may be more onerous, less clear, unknown to the user, or even in conflict with the user's own country's laws. If the server location or control is not disclosed by the cloud provider or if it is subject to change without notice, the information is more vulnerable to the risk of being compromised. Uncertainty on this point is a risk factor in itself.

In addition, some nations' data sovereignty laws require companies to keep certain types of data within the country of origin, or place significant restrictions on transmission outside the country of origin. Some jurisdictions' privacy laws limit the disclosure of personal information to third parties, which would mean that companies doing business in those countries might be prohibited from transferring data to a third-party cloud provider for processing or storage. (It is worth noting the proposed secret TransPacific Partnership agreement reportedly appears to feature a specific provision prohibiting participants, such as Australia, from enshrining data location restrictions, and the equivalent Atlantic proposal includes similar constraints on domestic law. On the other hand the Article 29 Working Party has suggested that the EU consider restrictions; and they have been mooted by EU ministers and data protection commissioners post-Snowden.)

Information stored in a cloud environment can conceivably be subject to more than one nation's laws. Indeed, the legal protections applicable to a single piece of data might change from one moment to the next, as data is transferred across national borders, or to the control of a different entity. Depending on where the data is being hosted or by whom it is

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

controlled, different legal obligations regarding privacy, data security, and breach notification may apply.

Where there is a lack of specificity, a business will often feel compelled to err on the side of caution and adhere to the most restrictive interpretation. (Others may assume that 'industry practice' will suffice, and the OAIC *APP Guidelines*[10] of March 2014 tacitly accept a less restrictive approach. However ACMA's history of penalties suggests caution has a place.)

In some circumstances, this may mean that large categories of data should not be allowed to be transmitted beyond the country's geographic borders, or outside its jurisdiction. As a result, some businesses are employing a hybrid cloud strategy which involves contracting with multiple cloud providers that maintain local data centres and comply with the separate, local legal requirements for each country.

The complexity of these various data sovereignty laws may make businesses reluctant to move to a cloud – especially a Public cloud, as described above – where it cannot restrict the geographic location or jurisdictional control of its data, and where the characteristics of data warrant such caution.

In concept, using a public cloud on a multinational scale should be highly flexible and cost-effective for a business. One of the attractions is the promise of effectively outsourcing a range of costs and risks. However, t data sovereignty restrictions to which a company may need to adhere in relation to some of those risks can create a daunting challenge.

Despite the notable benefits, many companies can be reluctant to utilize cloud technology because of fears regarding their inability to maintain sovereignty over the data for which they bear significant legal responsibility. (See also sections below on obligations and third party access.)

The Australian Experience

The new Australian Privacy Principles created by the November 2012 amendments to the *Privacy Act* 1988 (Cth), appear to significantly change the test for personal data transferred out of Australia.

- The prior Principles required "reasonable efforts to ensure comparable security," which is difficult to qualify or quantify.

- The new Principles require the outsourced third party service provider "comply with Australian law," and there is greater expectation that the details of foreign jurisdictions in which personal data is hosted be disclosed

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

While there remains in the APP Guidelines (OAIC 2014) an emphasis on reasonableness, the new standard is potentially tighter, and the disclosure of diverse foreign locations hosting personal information of Australians potentially impacts reputation[11]. Thus, there may be an incentive to consider hosting in-country, or under a regime that is known to be even more rigorous and safe in practice than Australia's. In January 2013 it was announced that CERT Australia would soon be part of a new Australian Cyber Security Centre, which aims to develop a comprehensive understanding of cyber threats facing the nation and improve the effectiveness of protection, which have raise the bar for expectations of effective security in Australia (although it is too early to tell if this will eventuate, given the potential effect of other developments in the Snowden material raising questions about official involvement in moves to undermine security).

The use of cloud technology in Australia is in flux, as regulators hurry to keep up with the evolving technology and increasing popularity of cloud solutions. Moreover, Australia's information security law is comprised of a bewildering amalgam of federal, state and territory laws, administrative arrangements, judicial decisions, and industry codes, (Connolly and Vaile: 2012)[12] so evaluating the impact of cloud sovereignty issues in this context becomes difficult. Changes are due in 2014[13].)

Nevertheless, cloud computing is definitely on the rise in Australia. A recent study reported that more than half of the subset of Australian companies examined spend at least ten per cent of their IT budgets on cloud services, and 31% of companies spend over 20% of their budget on cloud solutions (Frost and Sullivan 2012).

Australian banks and insurance companies are regulated by the Australian Prudential Regulation Authority (APRA), and are required to consult with APRA in connection with outsourcing computing services offshore. Other Australian businesses are required to comply with the Privacy Act and the Australian Privacy Principles, which prohibit the transfer of personal information to a third party outside Australia unless that country has equivalent laws or the entity takes reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information for the data (OAIC 2014, Chapter 8) [14]. Many state and territory privacy laws contain similar expectations.

The regulating bodies of some Australian industries, such as banks and insurance companies, may, as a practical matter, require that data be hosted exclusively within Australia. (APRA 2010)[15]

Organizations in Australia, such as defence bodies, education providers, and healthcare organisations, may be required to adhere to the requirements of the Australian Government Information Management Office (AGIMO) to the extent they are directly acting for federal

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

agencies. AGIMO has set out issues to be considered by agencies that are exploring cloud services (AGIMO 2011) [16]. These agencies generally prefer to use data centres within Australia in order to maintain physical jurisdiction over their most sensitive data. (Many other activities of organisations other than federal agencies may not be required to adhere to AGIMO's guidance, depending on the nature of the contracts involved and of the organisation.)

Some cloud providers in Australia will commit to host services within national boundaries to alleviate these data sovereignty concerns. However, even if the data itself is hosted domestically, it is nonetheless conceivable that some service providing access to the data (for instance, in the case of certain models for offshoring by banks) could be hosted in a foreign jurisdiction, or under the control of another jurisdiction.

The Potential Impact of Foreign Regulatory Requirements

Australian companies considering cloud services should consider legal developments abroad when assessing the relative risks and benefits.

Cloud hosting on a global scale is often based in data centres in places like the US, central Europe or Singapore which offer cost and other benefits. It may often store data connected to EU as well and Australian citizens. Differences between the regulatory frameworks where data is hosted, where hosting companies are based, and where data subjects or data users are based can create complex compliance environments. Some aspects can present a legal risk that cannot be fully offset by contracts or technology alone. (Irion 2012) (See also the Third Party Access section below.)

European Union

The European Network and Information Security Agency (ENISA) launched a report in February 2013 taking a 'Critical Information Infrastructure Protection' approach to cloud computing, which calls for better transparency regarding logical and physical dependencies, such as which critical operators or services depend on which cloud computing services (Dekker 2012) [17].

The European Commission is also considering new data protection requirements that would effectively apply throughout the world, including in Australia, to companies active in the EU market or which host data about EU citizens (EC Directorate-General for Justice 2012) [18]. If these proposals are implemented (Neilsen 2013), cloud providers with EU customers would be required to adhere to such legal obligations for all of their data holdings, including data hosted for Australian customers.

European laws impose some limits on cross-border data transfers. The existing European *Data Protection Directive* obligates entities to maintain the security of certain categories of

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

personal data, and permits the transfer of such information outside of the EU only to those countries the EU considers to have satisfactory data protection laws or if the company to which the data is transmitted agrees to comply with EU law (*Directive 95/46/EC*). As a result, data may not simply be transferred at all to a cloud provider with servers located in countries whose data protection laws do not satisfy EU standards.

US regulators, pointing to increasingly robust proposals for increased regulation domestically, have recently suggested that emerging approaches to data protection in the US are more consistent with the EU approach than is widely appreciated, despite PATRIOT Act access and other emerging issues (Robinson 2013). (EU regulators and politicians appear to remain unmoved, with initiatives in the opposite direction in relation to 'Safe Harbor'.)

EU laws on 'discovery' for litigation purposes, and on national security, may be inconsistent with US laws such as the *USA Patriot Act* in some circumstances (Forsheit 2010). This may lead to confusion or conflict over appropriate responses to requests for access for this purpose.

USA

The United States has no overarching nationwide data protection law (HIPAA, though national, is restricted to the health sector), but it does regulate disclosure of certain categories of personal information to third parties through a variety of laws[19]. The US government asserts extraterritorial claims on data that potentially affect non-US entities through the *USA PATRIOT Act* [20]. These are discussed further in the next section.

Even companies which try to require their cloud providers to keep their data within the geographic borders of their own country cannot assume that they are subject only to their home country's laws because, in certain circumstances, cloud providers may be legally obliged to communicate information, including personal information, to authorities [21] .

For instance, if a company is based in a country which prohibits disclosure of personal information without the subject's consent, it could conceivably violate its own nation's laws if it complies with a demand by the US FBI to turn over information stored in a US company's cloud, or in a cloud data store located within US boundaries. (See the SWIFT case below for an example on this point.)

There has efforts made to deal with these troublesome issues. The US Department of Commerce and the European Commission jointly developed a "Safe Harbor" to streamline the process for companies to comply with the EU's Data Directive[22]. Intended for EU and US companies which store data, the Safe Harbor is available for companies which adhere to the seven privacy principles outlined in the EU Directive. A similar Safe Harbor framework exists between the US and Switzerland[23], among others.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Of particular concern to cloud computing customers are the requirements that data subjects be informed of data transfers to third parties, and be provided the opportunity to opt out. (The 2012 proposals for EU data protection, above, include increased emphasis on effective consent rights for data subjects, so this may continue to be relevant when and if these proposals come into effect in 2014 or later.

There have also been mounting criticisms of the effectiveness of Safe Harbor from a compliance perspective, including by UNSW research associate Chris Connolly. (Connolly 2008) These recently bore fruit in a review of trust schemes associated with it. (FTC 2014)

Data may also only be transmitted under the scheme to third parties who follow adequate data protection principles, thus obligating the cloud customer to ensure that its cloud provider operates responsively. Clearly there have been doubts about the effectiveness of this scheme; the Article 29 Working Party highlighted the question of whether individual/corporate consumers are in a position to understand (ie to give meaningful consent) and enforce such obligations.

More recently, EU concerns about the late 2013 revelations by Edward Snowden have brought the Safe Harbor model into question, given the apparently limited or non-existent constraints it has placed on warrantless suspicionless mass surveillance of non-US citizens. (Rodrigues et al 2013)

The European Parliament, after it adopted the text of the proposed EU General Data Protection Regulation on 12 March 2014, also went so far as to pass a resolution setting forth its findings and recommendations regarding the National Security Agency surveillance program. Among other things, the resolution calls for:

- withholding the Parliament's consent to the Transatlantic Trade and Investment Partnership if European data protection principles are not fully respected;
- suspending the Terrorist Finance Tracking Program until alleged breaches of the underlying data disclosure agreements have been fully clarified; and
- suspending the Safe Harbor Framework immediately, alleging it does not adequately protect European citizens. (Hunton & Williams 2014)

The long term future of the Safe Harbor scheme is thus unclear.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Canada

Canada presents a complex situation, as its data protection legal landscape is a patchwork of federal, territory, and provincial laws. It has laws requiring that certain data stay not just within Canada, but within specific territories and provinces[24]. Of particular interest is Canada's assertion that its privacy laws apply beyond its borders. The Federal Court of Canada held that the PIPEDA law gives the Office of the Privacy Commissioner of Canada (OPC) the right to investigate complaints relating to the flow of personal information outside Canada, regardless of whether the company involved is Canadian[25]. If personal information about Canadian citizens is involved, the country's privacy laws and the OPC's investigatory powers extend across borders to foreign-based companies, though there are of course the sovereignty dilemmas around giving force to such powers.

No uniform standards

Many other countries have proposed or are in the process of developing new laws regulating data privacy and related matters, and there is little hope of a uniform, worldwide standard which companies could confidently follow to ensure compliance.

Data breach notification laws, for instance, vary greatly from one jurisdiction to the next. (Maurushat 2009) Some companies resolve this concern by storing only public data on public clouds, and keeping confidential information within their own control. Nevertheless, even where the data remains within the geographic borders of Australia, it is possible that the cloud provider entity is subject to the laws of another country.

In addition, data which is transferred outside Australia to one or more countries may become subject to a variety of external laws. Business organizations which operate across borders face unique challenges in managing network security risk, and those which use cloud computing technology have even more complicated exposures. A recent Capgemini study revealed that management considers "issues with data sovereignty" to be the second most important factor – just after "fear of security breaches", and before the raft of technical and management issues – in determining whether to adopt a cloud infrastructure (Capgemini 2012).

Therefore, along with concerns about integration and business agility, businesses are starting to realize the serious and complex issues involving data sovereignty in the cloud computing context.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

4. Third party access by legal means: Does it matter where your data is stored, or by whom?

This chapter drills into a core question: the complex of factors and legal issues which influence whether third parties can assert their right to access your data hosted in either a local cloud (in Australian jurisdiction) or in an offshore cloud (typically through services based in the US, the main cloud hosting jurisdiction).

Its observations may help guide your assessment of whether these jurisdictional issues warrant consideration of a 'data sovereignty'-aware cloud policy.

Introduction

For some time, improved global networks and the Internet have enabled hosting service providers to store data in low-cost jurisdictions, or where close proximity to large markets and scale facilities can create economies of scale.

In deciding whether to host data overseas, prudent customers have typically considered the cost of the service, security, and the sovereign risk of the location.

After an initial rush of cyber-libertarian optimism, the wishful thinking of the early 1990s in which 'cyberspace' was somehow beyond the bounds of earthly law, there is a sobering recognition that information is still subject to the laws of the jurisdictions where it is held, or which regulate entities who control or host it.

Data hosting customers need clarity about whether remote hosting will involve transferring data to a foreign legal environment that may bring new risks or create special concerns. In particular:

- does the service provider ensure that the foreign host provides a service that complies with Australian standards for privacy and security?
- what are the implications of exposing data held offshore, or under the control of offshore entities, to examination by foreign law enforcement regimes or litigants?

Government data users in particular feel the pressure of these questions.

Such concerns may be exacerbated by the ability and practice of certain law enforcement agencies to inhibit or prevent owners of the data from knowing that their data has been accessed and is subject to examination.

Focus on these issues has intensified with the advent of "cloud" computing. Information held "in the cloud" may be stored in multiple locations, and in multiple jurisdictions. Cloud computing with global networks obscures the customer's knowledge and control of the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

regulatory risk associated with the jurisdiction/s where the data is held, or by whom it is held.

Where the customer is itself storing and managing the information of third parties, this lack of information represents a failure to achieve transparency. For many customers a failure to fully understand the issues and risks associated with potential foreign access to data held in a global cloud may be illegal.

Many of the commercially available cloud computing services are offered by US-based companies at present, so in this paper we consider the potential scenarios under which a US-based data hosting service provider may be compelled to provide access to stored data to third parties, such as US government authorities and private litigants. We also comment on comparable laws in Australia, and issues raised in relation to European countries.

(While this paper does touch on both US and Australian law and practice, it is not intended as an abstract comparison of the substantive laws of the two countries; this would be a somewhat misleading basis for an Australian company considering relevant business and regulatory risks in the choice between hosting data under Australian jurisdiction or under other those of typical commercial cloud services. We offer a few comparisons with certain Australian provisions as a context for this risk analysis. However, even if local and cloud storage jurisdiction laws were identical, other practical factors are more burdensome dealing with third party claims to access an offshore data store. For instance the costs of legal action, enforceability of remedies, and investigation or monitoring of developments are all more problematic in another jurisdiction since a local entity will often not have any presence there. These are of course to be offset against the hoped-for benefits of Cloud scale services.)

Background

As a practical threshold item, we note that the US government is usually interested only in matters that concern US interests, for example, payment of US taxes, crimes in violation of US laws and threats to US national security. Much of the information held in cloud stores under US jurisdiction on behalf of foreign data owners may be of little interest to them for this reason. But from the examples we consider in this summary, it is apparent that US authorities will not apply particular self-restraint in scenarios involving foreign jurisdictions and US interests.

Compliance obligations under foreign laws on US companies (or their foreign data sources) not to provide data to the US government are not recognized as a defence to information requests by US courts or authorities. Additionally, as many data owners would be aware, US authorities can in most cases also obtain data under international cooperation treaties through foreign governments (as can Australian authorities).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Different Types of Data Requests

Informal requests

US government agencies typically have investigative duties and authority under the statutes or regulations of their establishment. As a result, government agencies can approach individuals and companies (including data hosting service providers) with informal information ***requests***. Many US companies are willing to comply with such requests, to cooperate with the US government on issues of shared interests (*e.g.*, fraud prevention on e-commerce websites) or to avoid contributory liability for illegal activities (*e.g.*, copyright infringement).

Some companies are also obligated to comply with certain information requests. For instance, financial service providers have to cooperate with certain regulatory agencies and provide certain records as a matter of statute, and telecommunication service providers have to provide access for law enforcement purposes under *CALEA*. (BeVier 1999; Kisswani 2012)

But, in the absence of such specific regulatory compliance obligations, individuals and companies do not have to answer to informal information requests from US government authorities.

Summons and subpoenas etc.

Most US government authorities are entitled under specific statutes to issue formal information requests – summons, subpoenas or other forms – which either have to meet certain minimum conditions (*e.g.*, IRS summons) or which are generally permissible so long as there is some relevance of the inquiry to the mandate of the requesting authority and the subpoena does not violate constitutional or statutory limits. For example, grand jury subpoenas issued by US attorneys are generally legal and compelling unless they violate the US *Constitution* or certain limiting statutes. Grand jury subpoenas also contain secrecy restrictions to protect the grand jury process from inappropriate influences.

The applicable limitations in the US *Constitution* and the *Electronic Communications Privacy Act* (*ECPA*) are discussed below in more detail, but for purposes of this summary it is important to note that information requests in the form of subpoenas are generally compelling, unless an exception applies. If an exception applies, the recipient of the subpoena can assert it and demand that the government narrow the scope of the subpoena or withdraw it.

In situations where subpoenas are not available due to statutory limitations, US authorities can be authorized to obtain a formal warrant, which has traditionally required a court order, probable cause and other conditions to be met, and is therefore more difficult to obtain for

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

US authorities. But recent legislation and government practices are believed to have weakened the protections previously afforded by warrant requirements, as further discussed in this article.

Digital Due Process Coalition and demands to limit access

A number of US-based data hosting service providers and other organizations, including Google Inc., Microsoft Corporation, AT&T, and eBay formed the Digital Due Process Coalition[26], which asserts that technological advances have outpaced the *ECPA*, and thus "the vast amount of personal information generated by today's digital communication services may no longer be adequately protected." This organization and various privacy activist groups demand that access to personal data (hosted by data hosting service providers and other companies) by US government authorities be limited. Demands include that the situations where US government authorities need warrants be expanded, that warrants should not be – or be less often – available without court orders, that additional limitations should be imposed to legitimize subpoenas (*e.g.*, by enacting new statutory restrictions or interpreting the US constitution to protect privacy interests), that electronic documents stored in the "cloud" be afforded the same Fourth Amendment privacy protections as electronic documents stored in traditional formats, and that consistent standards be set forth for government access to electronically stored information.

Unless and until such reforms pass, the investigative powers of the US government are limited primarily by the following constitutional principles and laws.

Australian Comparison

There is no similar industry lobbying to tighten privacy laws in this way in Australia, nor coordination with local privacy advocates. The previous Australian government was pursuing a policy of compulsory general data retention by carriers and service providers with a view to making archived information available to law enforcement authorities; this would add to recent changes obliging ISPs to retain certain traffic data on specific request. This policy was consistent with perceived obligations under the Council of Europe Cybercrime Convention. It was opposed by industry, but returned to active consideration as the 2012 'Data Retention' proposals.

The Australian *Privacy Act* 1988 does not prevent a local company from providing personal information to regulatory authorities without legal compulsion if this is disclosed in the Privacy Policy of the company. Some Privacy Policies state that personal information will not be disclosed to regulatory authorities or other third parties without legal compulsion. The concept of 'implied consent' has been used to justify provision where such statements are more ambiguous.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

There are currently few Australian statutory restrictions or conditions on the offshore transfer of data which may become subject to such access. Contractual protections are also of limited value in the circumstances discussed above, especially to data subjects.

Privacy law reform for transferors to generally "remain responsible" after offshore transfer may be of limited benefit[27] to local data owners or individuals once personal data is disclosed as a result of foreign government or litigant compulsion or effective request. (Barwick 2012a)

There has, not surprisingly, been interest in whether more restrictive oversight of transfer of personal data overseas will be needed in order to bolster the responsibility of transferors. For instance, Senator Stephen Fielding (an independent, though with potential balance of power in the Senate at the time) introduced the Keeping Jobs from Going Offshore (Protection of Personal Information) Bill in 2009, which would have required companies to gain customers' written consent before their personal information could be transferred offshore.

The 2012 amendments to the Privacy Act now in force, while not requiring explicit consent, appear more likely under APP 8.1 and s 16C to impose liability on Australian hosts for data breaches which occur offshore in some circumstances. (See also the Privacy Alerts bill 2013, which would have imposed reporting obligations.)

Limitations on Searches and Seizures under the Fourth Amendment of the US Constitution

Generally, the primary limit on the US government's power to obtain personal information is the Fourth Amendment of the US *Constitution*, which prohibits "unreasonable searches and seizures." Under the Fourth Amendment, the government must obtain a warrant supported by probable cause that a crime has been committed, that describes the "place to be searched and the persons or things to be seized," and provides simultaneous notice of the search to the person. Whether a search and seizure is "reasonable" depends on whether the person has an objective "reasonable expectation of privacy" in the item subject to the search (Cate 2007).

The protection afforded by the Fourth Amendment, however, is not absolute, and there are many exceptions to the warrant requirement.

One such exception is for data held by a third party. Under this "Third Party Exception," a person does not have a reasonable expectation of privacy in information he or she discloses to a third party. For example, the government does not need a warrant to seize documents that a person conveys to his or her bank (*e.g.* cheques).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Similarly, the government does not need a warrant to use "pen registers" and "trap and trace" devices, to record out-going and in-coming call information, because information about the number dialled and the time and duration of the call is accessible to third parties, mainly the telecommunications company (Cate 2007).

In the context of electronically stored data, the US government has routinely relied on this Third Party Exception to dispense with the warrant requirement. Federal courts take the view that a person does not have a reasonable expectation of privacy in the subscriber information that he or she provides to an Internet service provider[28]. Therefore, the government was able to obtain the following personal information without a warrant:

1. the name, address, e-mail address and media access control address from Comcast Cable Communications of a person who used Comcast's Internet services in the course of sharing movie files online[29];
2. the information on an individual's computer that was accessible by a peer-to-peer file sharing program[30];
3. the chat account information from Yahoo! of a person who used Yahoo's Internet services to access chat boards[31];
4. the log-in information, including the date, time and IP address of each log-in, from Microsoft of a person who used Microsoft's MSN/Hotmail program[32]; and
5. the contents of an iTunes files library shared over an unsecured wireless network[33].

At least one court took a different approach and held that whether a person has a reasonable expectation of privacy in subscriber information provided to an ISP depends in part on the ISP's terms of service[34].

Australian comparison

The Australian *Constitution* does not have any provision comparable to the Fourth Amendment to the US *Constitution* which would put limits on Parliament's ability to pass search and seizure laws.

Generally, Australian search and seizure laws can be enforced subject only to the process and limitations, typically about procedure and justification or lack thereof, expressed in the relevant legislation itself – legislation which can be amended, such as during the recent 'war on terror' when certain longstanding common law protections were diluted to some extent. (Roach 2010)

The Telecommunications *Act 1997* for instance, discussed below, mentions but does not mandate warrants for s313(3) law enforcement help; reports suggest substantial collection of communications traffic data without warrants, including under the *Telecommunications*

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

(Interception and Access) Act 1979 (Cth). (Nicholls & Rowland 2007; Dobbie 2013)[35]."Doing your best" for 313(1) crime prevention purposes does not mention warrants; its proper ambit is unclear, and seems unlikely to be tested.

The *Privacy Act 1988* may offer some procedural protections, although exceptions permit certain uses and disclosures for law enforcement and related purposes[36].These bypass questions of 'reasonable expectation of privacy' with simple statutory exceptions, and the Privacy Commissioner's policy *Guidelines* to their use. (OAIC 2014) A recent statement from the Privacy Commissioner in response to questions raised by reports of NSA programs in the US indicates a wide interpretation of the effect of obligations under domestic or foreign law enforcement laws in limiting protections under the *Privacy Act*; in the absence of determinations, this is also unlikely to be tested.

USA PATRIOT Act of 2001

Following the terrorist acts of September 11 2001, the Bush administration enacted the *USA PATRIOT Act* of 2001 to expand government powers to obtain data for investigations related to international terrorism and other foreign intelligence matters.

Essentially, this Act had the effect of lowering previous thresholds for the activation of these powers in existing pieces of legislation by amending (a) the *Foreign Intelligence Surveillance Act* of 1978[37], and (b) other legislation governing National Security Letters. These controversial powers are discussed below.

Privacy and library groups also oppose the "library records request" provision of the *Patriot Act* on the grounds that it "leaves open the door for governmental misuse to broadly investigate library and bookstore patron reading habits"[38].

A reality check asking "who cares?" may however be appropriate at this point.

Many business operations think it irrelevant if a government wants to check their data in order to fight terrorism, provided the data is not damaged, lost, misused, or disclosed to competitors. So who would care?

- Governments typically do not want some of their information, of many types, to be accessible by other governments as a matter of principle, national security or sovereignty.
- Some businesses (say, a major miner) do not what their information to be accessible to the sovereign wealth funds (for example) of foreign powers.
- Other businesses may have specific reasons to be cautious about exposure to access, particularly if there is any suggestion of improper or overbroad access to

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

or use of data beyond the purposes for these laws were put in place.

- Some entities may be willing to accept the initial access but remain concerned about further provision of data to other countries once it has been accessed under this method, due to the operation of other international instruments and agreements.

In any case, it may be harder for, say the US government to find information about an Australian entity hosted in a US data centre than it is to access or discover this information via a request from the US to Australia under various cooperation arrangements (below), and the operation of Australian law in response. Such options would limit the practical need to resort to this method.

Australian comparison

Following the Bali Bombings in 2002, Australia adopted a *National Counter-Terrorist Plan* (2003) and made extensive amendments to surveillance and access powers available to Government authorities[39].

These have somewhat less impact than the *USA Patriot Act* for our purposes, as they don't introduce administrative subpoenas *per se*, although there were considerable dilutions of existing protections, some comparable with US changes, and investigators gained extended powers and more streamlined procedures (Lynch & Williams 2006).

In subsequent years further legislative changes have somewhat further reduced the difference between thresholds in the US and Australia (Michaelsen 2010), and Australia's accession to the CoE *Cybercrime Convention* in 2012 requires enhanced cooperation with signatories, including the US, although this may make little practical difference – see below.

Foreign Intelligence Surveillance Act of 1978 (FISA)

The US *Foreign Intelligence Surveillance Act* sets out a specific legal framework for surveillance operations conducted as part of investigations related to international terrorism and other foreign intelligence matters. With the introduction of the *Patriot Act*, the *FISA* was amended so that it now applies where a "significant" purpose of a surveillance operation is to obtain intelligence for the purposes of such investigations, rather than the "sole" or "primary" purpose, as it originally stipulated. More recent amendments have also broadened its use.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

The *Foreign Intelligence Surveillance Act* framework will be activated where there is probable cause that the target of surveillance operations is, or is an agent of, a foreign power. Due to the *Patriot Act* amendments, terrorism is now included within the definition of "foreign power", and there is no requirement that targets of surveillance be engaged in any kind of criminal conduct. In addition, warrants for surveillance operations are issued by the Foreign Intelligence Surveillance Court (FISC), a closed forum separate from the standard federal court system.

Specific powers of law enforcement agencies under the *FISA* (as amended by the *Patriot Act, Protect America Act of 2007, FISA Amendment Act of 2008*, and reconfirmed in late 2012) that may constitute potential risks for those hosting data in the US include:

1. The power of the Federal Bureau of Investigation (FBI) to compel the production of any "tangible thing" for the purposes of an investigation to either obtain foreign intelligence or protect against terrorism or clandestine intelligence activities[40]. The FBI may do so by certifying to an FISC judge that the investigation falls within the bounds of the *FISA* and the judge does not have any discretion to refuse the order if certain procedural requirements are met[41]. Persons against whom such an order is made and/or sought are forbidden from disclosing these facts to any other person except for the purposes of complying with an order and/or seeking legal advice.
2. The power to conduct secret physical searches of personal property for investigations in which foreign intelligence gathering is a significant purpose. The person whose property is searched need not be directly involved and the search may be conducted without a warrant, provided that the Attorney General certifies that there is no substantial likelihood the search will involve the premises, information, material, or property of a US person[42]. Subjects of a special search must not be informed of the fact that it has been or will be conducted, and third parties directed to assist must protect its secrecy.
3. The power to obtain a search warrant in all criminal investigations without providing notice to the subject of the search for up to 30 days, or longer upon application to the Court if the facts justify further delay[43].
4. The power to conduct roving wiretaps on communications lines, which allows for monitoring of several different communications lines across the US[44]. To engage in wiretapping, the government must obtain a warrant from the FISC based upon probable cause that the target is, or is an agent of, a foreign power[45]. Third party communications carriers, landlords and other specified persons must provide access and assistance necessary to carry out the warrant[46]. They must not reveal the fact of the warrant, and must minimize associated disruption to any services they provide to the subject. In the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

case of third party communications carriers, if a law enforcement authority suspects that the subject of a roving wiretap warrant might use a particular carrier's services, the authority is entitled to monitor all communications transmitted by that carrier. Accordingly, there is a risk that information concerning other clients of the carrier might incidentally be captured.

5. The power of the Department of Justice (DOJ) to grant approval for law enforcement agencies to engage in electronic surveillance without a court order for up to one year for the purposes of obtaining foreign intelligence[47]. There must be no substantial likelihood that a US person is a party to the surveilled communications. Any third party carrier involved in transmitting the communications must assist the surveillance if requested, including by maintaining its secrecy[48].
6. The power of the federal government to use "pen registers" and "trap and trace" devices to monitor outgoing and incoming phone calls for the purposes of an investigation to gather foreign intelligence information[49]. In some circumstances, relevant communications carriers may be obliged to assist authorities in installing and monitoring such devices, protecting the secrecy of the investigation and minimizing interruption to any services provided to the subject[50].

In June 2013 the *Washington Post* and *Guardian* published reports of 'data mining' targeting communications of non-US users for national security purposes, with only infrequent high level authorisations, based on broad interpretations of 2008 amendments to FISA. (Gellman & Poitris 2013) It was initially unclear the extent to which such programs, and the many others which followed, would affect business-oriented cloud data services. Several major consumer-oriented SaaS providers were reported to have agreed to participate, which could affect 'BYOD' devices, 'ad-hoc' clouds and cloud-enabled PCs, (Greenwald & MacAskill 2013) although details of the program and its implications remain in dispute at the time of writing, and some of the allegations have been denied.

'Administrative subpoenas' such as National Security Letters (NSLs)

National Security Letters are a type of federal administrative subpoena by which the FBI may, *without* court approval, compel individuals and businesses to provide a variety of records, including customer information from telephone and Internet service providers, financial institutions and consumer credit companies[51]. An NSL may be issued to any person (even if they are not suspected of engaging in espionage or criminal activity) so long as the issuer believes that they may hold information relevant to a clandestine terrorism or other intelligence investigation. The FBI does not need to specify an individual or group of individuals and each request may seek records concerning many people (Cate 2007). For example, nine NSLs in one investigation sought data on 11,100 separate telephone numbers

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

(Cate 2007). Moreover, a recipient of an NSL may not reveal its contents or even its existence[52].

A communications carrier subject to a National Security Letter may be obliged to hand over information about a particular customer, their toll billing records and/or their electronic communications transaction records to the FBI[53]. However, there is no provision requiring a carrier to give the FBI access to the actual content of a client's communications.

National Security Letters have been the subject of considerable legal and political controversy. For example, a number of mandatory non-disclosure clauses have been ruled[54] unconstitutional (and subsequently re-enacted in a different form), and several reports by the US Inspector General have revealed widespread inappropriate use and underreporting by the FBI (Office of the Inspector General 2007).

(In March 2013, Judge Susan Illston of the Northern District of California declared, in a case involving the EFF, that 18 U.S.C. § 2709 and parts of 18 U.S.C. § 3511 were unconstitutional. She held that the statute's gag provision failed to incorporate necessary First Amendment procedural requirements designed to prevent the imposition of illegal prior restraints, and that the statute was unseverable and that the entire statute, also including the underlying power to obtain customer records, was unenforceable. The order was stayed subject to appeal[55]. While it could rein in the NSL model of access to network and cloud data to some extent, it remains to be seen whether this ruling survives appeal; or if it does, whether similar replacement provisions will be immediately re-enacted, resulting in minimal effective change.)

Australian comparison

There is no known direct equivalent of FISA and the very broad NSL administrative subpoena in Australia.

Certain provisions of recent anti-terrorism laws do restrict the capacity of those investigated to communicate this fact to their associates, but in relation to a limited range of specific offences. Certain provisions of the *Telecommunications Act* 1997 (Cth) and *Telecommunications (Interception and Access) Act* 1979, above, refer to national security purposes.

It is unclear what the impact of proposals for increased 'Data Retention' of telecommunications metadata would have if implemented, as no draft legislation was provided in by late 2013, and the Joint committee report declined to recommend it proceed. (JPCIS 2013) It is expected they would oblige increased retention so formal court orders could later be made for access to message contents, without necessarily diluting whatever existing requirements for such orders may be in place. There are however large numbers of warrantless metadata authorisations, over 300,000 in 2012-13, mostly by state police forces. (Attorney-General's Department 2012-13)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Reports in March 2014 suggest retention proponents remain enthusiastic. A Senate inquiry into the operation of the TIA Act, including this issue, is due to report in mid-2014, although with an unreceptive House of Representatives it appears unlikely its recommendations would be enthusiastically adopted.

The SWIFT case

A prominent example of the US government's use of an administrative subpoena is the SWIFT case. The Society for Worldwide Interbank Financial Telecommunication is a Belgian-based co-operative active in the processing of financial messages, with about 8,000 banks as members. On average, it processed 12 million messages a day in 2005. SWIFT operated two primary data centres, an EU site reportedly in Belgium and a mirror site in the US. After the terrorist attacks of September 11, 2001, the United States Department of Treasury (UST) addressed multiple administrative subpoenas to the SWIFT operations centre in the US under the "Terrorist Finance Tracking Program", requesting a copy of all the transactions in SWIFT's database, rather than just the records of individuals who were the specific targets of the government's investigation. (McNicholas 2009) SWIFT complied with the procedures by negotiating an arrangement whereby it transferred data from the mirrored SWIFT database to a "black box" owned by the US enabling the UST to perform focused searches over an extended period of time.

In late November 2006 the EU Article 29 Working Party[56] (the independent advisory body to the European Commission on data protection and privacy) issued an opinion on the processing of personal data by SWIFT concluding that SWIFT and the financial institutions which use SWIFT's services had breached Community data protection law as set out in Directive 95/46/EC, including the transfer of personal data to the United States without ensuring adequate protection and failure to inform data subjects about the way in which their personal data were being processed.

When this controversy developed in Europe, Australia and elsewhere in 2006 after the extent of UST searches over the transactions of European and other citizens became known, European data protection commissioners were ultimately unable to effectively intervene.

Although SWIFT itself is believed to have privately negotiated some constraints on the scope of searches over EU citizen transactions by US agents[57], SWIFT later formalised ostensible compliance with EU law by joining the US 'Safe Harbor' scheme. (The 'Safe Harbor' is a specific type of 'Adequacy Decision' adopted by decision of 26 July 2000 by the EC to allow the free flow of personal data between the EU and the US, in accordance with the EU

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Directive 95/46/EC [58]). This allows limitations on its data protection principles for important public purposes "to the extent necessary to meet national security, public interest or law enforcement requirements"[59]. The episode confirmed the limited options available to foreign data owners in the event of use of such administrative subpoenas.

Electronic Communications Privacy Act of 1986 (ECPA)

The *ECPA* is one of the primary federal statutes protecting the privacy of electronic communications in the US. (McNicholas 2009) Within the *ECPA* are the *Wiretap Act*, which prohibits the interception, use or disclosure of wire and electronic communications, and the *Stored Communications Act* (*SCA*), which regulates access to stored electronic communications. Consumer groups, privacy advocates and companies, including Microsoft Corporation, Google Inc. and E-Bay (the Digital Due Process Coalition) have criticized the *ECPA* as ineffective in protecting privacy in light of technological changes and are calling for the reform of the *SCA*.

The *Stored Communications Act* provisions at issue provide that the government needs to obtain a search warrant to gain access to the contents of an email that is 180 days old or less but can compel a service provider to disclose the contents of an email that is older than 180 days with only a subpoena (Salgado 2010).

Critics contend that the widespread use of email and other documents stored in the cloud are increasingly replacing the traditional ways of storing documents in paper form, on a hard drive or on a CD. They point out that information stored in traditional formats would be fully protected by the Fourth Amendment's warrant requirement, yet under the *ECPA*, "an email or electronic document could be subject to multiple legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient or uploaded into a user's "vault" in the cloud, where it might be subject to an entirely different standard." (Beckwith Burr 2010) Applying consistent standards is further complicated with regard to "Friend Requests, Status Updates and other forms of communication that are neither one-to-one communications, like email, nor public forum posts"[60].

Consequently, "courts have not been consistent in applying the Fourth Amendment's warrant requirement and the *SCA's* 180-day protection for communications in electronic storage to e-mail messages stored remotely on service providers' networks", which creates uncertainty for ISP's and other companies who host content with regard to how the *ECPA* applies to material on their systems[61].

For example, the Eleventh Circuit held that individuals do not have a reasonable expectation of privacy in read e-mail messages stored with an ISP because they "shared" them with the service provider"[62]. In contrast, the Ninth Circuit held that an electronic communication

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

service provider who turns over opened and stored text messages without a warrant or a viable exception is liable under the *SCA* for making an access that was not permitted "as a matter of law"[63]. To confuse matters more, a panel of the Sixth Circuit held that users have a reasonable expectation of privacy in e-mails, only to have its decision reversed by the Sixth Circuit sitting *en banc* on grounds that the plaintiffs did not have standing to sue, but without addressing the constitutionality of the SCA provisions[64].

As a result of the ambiguity in the law, the Digital Due Process Coalition has proposed the following changes to the *ECPA*:

1. Treat private communications and documents stored online the same as if they were stored at home, and require the government to get a search warrant before compelling a service provider to access and disclose the information.
2. Require the government to get a search warrant before it can track movements through the location of a cell phone or other mobile communications device.
3. To require a service provider to disclose information about communications as they are happening (such as who is calling whom, "to" and "from" information associated with an email that has just been sent or received), the government would first need to demonstrate to a court that the data it seeks is relevant and material to a criminal investigation.
4. A government entity investigating criminal conduct could compel a service provider to disclose identifying information about an entire class of users (such as the identity of all people who accessed a particular web page) only after demonstrating to a court that the information is needed for the investigation (Salgado 2010).

Australian comparison

There is no broad Australian equivalent of the 'order to disclose' that is available to US federal government agencies.

However, some Australian government agencies possess similar powers under various legislative schemes. For example, the New South Wales Independent Commission Against Corruption may obtain certain information under State surveillance legislation, and CrimTrac[65] is listed as an 'enforcement agency' under the *Telecommunications (Interception and Access) Act*.

Also note the proposals for 'Data Retention', mentioned above, introduced publicly in 2012. If implemented, these could require retention of communications metadata for periods of two years or more, which would facilitate local access under a subsequent court order.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Section 313 of the *Telecommunications Act 1997* (Cth)[66] contains two relevant provisions which offset the effect of prohibitions on phone tapping etc. under the *Telecommunications (Interception and Access) Act 1979* (Cth).[67] The first is a 'crime prevention' purpose in s313(1) and (2), which requires carriers, carriage service providers and their intermediaries (but probably not cloud data hosts?) to "do their best" to prevent their networks and facilities being used to commit an offence under Commonwealth or state law. Without an obligation to do anything, guidance as to who can request or suggest action, compensation for costs under s314, or guidance as to what might be expected, this is difficult to formally enforce, though there is wide scope for informal pressure. It is the basis for recent informal Internet content blocking, with ASIC IP block requests aimed at fraud pages reported to have inadvertently taken 1,200 and 253,00 non-fraud sites offline in two recent instances (LeMay 2013).

The more significant provision is an enforceable 'law enforcement' purpose in s313(3) and (4), which requires carriers etc. to give such help as is 'reasonably necessary' to 'officers and authorities' of Commonwealth and states to enforce criminal laws and those with financial penalties in Australia, the criminal laws of 'a foreign country', or to protect national security or public revenue. Carriers and carriage service providers are exempt from liability for good faith cooperation with both these provisions. 'Help' includes interception warrants, stored communications warrants, local or foreign preservation notices under the *Telecommunications (Interception and Access) Act*, and requires financial assistance for costs incurred in s314.

Most of the law enforcement data surveillance and interception activities listed in s313(7) applying to s313(3) and (4) are based on warrants and notices, rather than mere requests. But the provision is not limited to these. Under s312 ACMA can issue administrative notices, also under an immunity; and the permissible scope for informal pressure on carriage service providers to 'do your best' under s313(1) and (2) is largely untested. The scope of these sections is thus somewhat uncertain, but clearly requires carrier help at least with reasonable law enforcement requests, including to assist enforcement of foreign laws.

Secret Surveillance Programs

After the events of September 11, 2001, the Bush administration engaged in 'warrantless wiretapping' of phone calls of US citizens for national security purposes. Under this secret surveillance program, telecommunication companies such as AT&T, Verizon and BellSouth assisted the National Security Agency in building a massive database of customer phone records[68].

Once the warrantless surveillance became known, privacy and civil rights groups brought lawsuits against the participating companies and the Bush administration.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

In response, the government enacted a law granting legal authority to the government to intercept certain communications without a warrant, immunity from liability to companies that assist the government with future warrantless surveillance, and retroactive immunity from liability to companies that already participated in the warrantless surveillance program[69].

Other secret surveillance programs, which were ultimately abandoned, include the 'Total Information Awareness' project, which was designed to detect terrorists by scanning large amounts of consumer data, and the 'Computer Assisted Passenger Pre-Screening System', under which the Homeland Security Department proposed to use information from various databases to classify airline passengers according to their level of risk[70].

More recently discussions about the scope and oversight of NSA's PRISM and other programs, above, which came to notice in June 2013, were marked by difficulties experienced by members of Congress and the Senate and cloud business leaders as a result of the secrecy obligations applying to those with official knowledge.

Australian Comparison

There have been no known similar instances in Australia of projects of this magnitude.

In 2012, proposals were advanced by law enforcement and Attorney Generals Department sources for an extensive 'Data Retention' program, noted above. Although details and justifications of the proposal, which was mentioned briefly amongst a range of other suggestions, are scarce, it involves 24 month or longer retention of metadata and traffic data, though apparently not message content, for a variety of purposes including but not only anti-terrorism efforts. As the interactivity of the Internet and web develops, mere metadata has been said to offer increasing information about the content of messages, arguably diluting the distinction between message content and metadata.

If it were implemented in full, it may represent a significant extension of secret surveillance programs in Australia, although oversight mechanisms are as yet unclear.

Data Access Demands in Litigation

The US federal government has a broad range of mechanisms to compel production of information in criminal and civil litigation proceedings, including discovery, administrative subpoenas, grand jury subpoenas and court orders.

Rule 34 of the U.S. *Federal Rules of Civil Procedure* imposes a legal duty on companies to retain all documents that may be relevant to pending and reasonably foreseeable litigation.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

During the discovery process in litigation proceedings, companies must search and produce all relevant records, including electronically stored information.

As a result, many companies have implemented systems that automatically scan and copy all electronic records, and users may not even realize that their documents are being stored for future document production purposes Cate & Eisenhauer 2007.

Australian Comparison

Similar rules apply in Australia.

However, as noted above, there are risks inherent in having data overseas in that, even where same rules apply, the costs of legal action, enforceability of remedies, and investigation or monitoring of developments are all more problematic in another jurisdiction, since a local entity will often not have any presence there, and will not be familiar with the requirements for an effective action against a determined access-seeker. Retaining and communicating with remote legal advisors and pursuing litigation offshore can also be more expensive and likely to result in worse outcomes.

One question that may ultimately turn on the factual details of a specific operation will be the risk that if data is stored in the US or another jurisdiction, an Australian company could potentially be exposed to legal action there on the basis of there being a sufficient connection with the jurisdiction. While in most cases this connection alone may be too tenuous to support a finding of such jurisdiction, further advice on specific circumstances may be necessary to exclude the risk of exposure to a US lawsuit that might not otherwise have jurisdiction, on the basis that the data (assets) are there.

Rule 26(b)(2)(B) provides a limited defence to production of electronically stored data "from not reasonably accessible sources, due to undue burden and cost" but there is not much guidance as to what constitutes sufficient "undue burden and cost." In addition, the party requesting the documents may still obtain limited discovery to test whether the information is truly "not reasonably accessible" (Kessler et al 2008).

The government may also issue subpoenas to require private companies to disclose information. For example, the Department of Justice issued a subpoena to Google Inc. to supply a log of random searches made on Google and Internet addresses as part of an unrelated lawsuit involving the *Child Online Protection Act*. The federal judge ultimately denied the DOJ's request for 5,000 random searches made on Google but ordered Google to surrender 50,000 random Internet addresses. Yahoo! Inc., Microsoft's MSN, and America

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Online Inc., on the other hand, complied with the DOJ's request for both searches and addresses to varying degrees[71].

The SWIFT case above is an example of the use of administrative subpoenas in matters which commence as investigations but may ultimately result in litigation to prosecute offences.

Finally, although the disclosure obligations in US litigation may in some cases potentially conflict with foreign data protection laws, such privacy laws of other countries are generally no defence to the legal obligations of entities to comply with subpoenas, warrants and orders that are lawfully issued and served within the jurisdiction of US courts. In the context of such a conflict between US and foreign law, one court put it this way: "The jurisdiction of American courts is unquestioned when they order their own nationals to produce documents located within this country"[72] (*i.e.* the foreign law is not a relevant consideration).

Access Requests on Behalf of Foreign Governments in Connection with International Assistance

The U.S. has entered into mutual legal assistance treaties with over 50 countries, as well as a mutual legal assistance agreement with the EU. The cooperation under mutual legal assistance arrangements can include substantial sharing of electronic information between law enforcement authorities in the two countries.

For example, in 2006, the US ratified the Council of Europe *Convention on Cybercrime*[73]. This Convention provides for gathering and sharing electronic data and evidence at the request of foreign law enforcement agencies, including:

1. expedited preservation of stored computer data, pending a request for search, seizure or disclosure of data,
2. expedited disclosure of traffic data, when the execution of a request to preserve traffic data indicates that another country was involved in the transmission of the communication,
3. search, seizure and disclosure of stored data,
4. real-time collection of traffic data, and
5. interception of the content of specified communications (Pryce 2006).

They also include an invitation to spontaneously offer data to a foreign state.

In addition, the *Additional Protocol* of 2003 makes publication of racist and xenophobic propaganda via computer networks a criminal offence. This may have impact on systems open to a large local user population.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Companies storing data in the US, therefore, may be subject to requests for data from foreign governments.

Australian comparison

The *Mutual Legal Assistance Treaty*[74] (Treaty) between the United States and Australia came into force 30 September 1999. This provided a bilateral mechanism where foreign law enforcement agencies can obtain access to data posted in other jurisdictions subject to control or supervision by the foreign government.

The Council of Europe *Convention on Cybercrime* was ratified in 2012 by Australia[75]. Key provisions of this convention are set out above, mostly those in Chapter III, Articles 23 and 25, including expedited search, seizure and real-time interception of content.

Australian ratification of the *Convention*[76] will mostly build on the *Mutual Legal Assistance Treaty* as between Australia and the US, and thus may have little additional impact on the exposure of Australian-owned data held in the US to access by other foreign governments (since this is already facilitated by US ratification of the Convention, and to some extent the operation of the Treaty). However, it will clearly increase the exposure of Australian data held in a European 'cloud' to access from other signatories, including those in the US.

Recent reports of plans for European Cloud services with components tied to national borders suggest they may have come about in response to the increased exposure to *USA Patriot Act* requests. It will be interesting to assess the degree to which these initiatives may offer guidance for Australian adaptation to the new environment (Citi Research 2012).

Analysis

When data is hosted overseas, it is subject to the law of the jurisdiction where it is held. Direct local access to data by the host country obviates the traditional process of disclosure and cooperation between national law enforcement agencies. The data is also subject to access under the civil process of the foreign nation.

This will have different implications depending on the nature of the law of the host jurisdiction and, to some extent, the relationship between Australia and the government of that nation.

In considering the example of cloud data hosted in the United States, the differences between the legal environments in Australia and in the US are many and extensive. Although the policy objectives and practical effect of government agency powers are roughly comparable, it is clear that American law is focused on the protection of the US national interest. It may be also inherently more difficult for companies or individuals based in

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Australia to monitor, assess and if necessary seek to restrain the conduct of search, interception or surveillance activities by governments or litigators of a foreign jurisdiction. In addition, the scale of surveillance activity undertaken in the United States, and consequent concerns expressed by industry regarding the extent of expanding government powers, have not emerged in Australia to the same degree (although recent proposals may narrow the gap to some extent).

When the conduct of SWIFT in making its data available to the US Treasury became public knowledge the European Parliament, echoed by some local commentators, declared that it was deeply concerned about the purposes of the transfer of data to the UST, the lack of the procedural protections expected in the source countries, and that such operations were taking place without "the citizens of Europe and their parliamentary representation having been informed." (European Parliament 2006)

While the potential for counterproductive "digital protectionism" deserves investigation, (Bleich 2012; Keane 2012) such concerns with US access to European data hosted on US Cloud services appear to have ongoing effect on plans to implement services which assert European countries' data sovereignty (Walden & Luciano 2011) [77].

In our view, while the picture is complex, and examination of actual hazards and dangers may in some instances show limited exposure to risks worth caring about, the concerns expressed by the European Parliament should resonate with Australian customers considering hosting data in or under jurisdictions such as the United States and elsewhere, and give rise to caution regarding the nature of the information to be transferred, the potential interests of the data owners in relation to that information, and increased needs to fully understand (and, more concretely, disclose to the data owner) the characteristics of the foreign legal environment.

5. A Signals Directorate view of Cloud security

Cloud services, with their massive 'honeypots' of tempting personal and business data and high capacity remote access, pose a serious challenge for IT security protection whether on shore or off, but they can also offer platforms for potentially meeting those threats in certain circumstances more effectively than non-cloud systems.

A full exploration of Cloud security issues is beyond the scope of this paper, and will remain the subject of attention from a significant part of the IT security and research sector (Pavlotsky 2012; Srinivasan et al 2012) but we touch briefly on some of those related to jurisdiction and sovereignty, seen through the prism (pun intended) of the key Australian

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

government security agency, what used to be called the Defence Signals Directorate. (DSD is now called Australian Signals Directorate.)

Cloud Computing Security Considerations – DSD Checklist

A non-exhaustive list of cloud computing security considerations is from section 17 of the Defence Signals Directorate/Cybersecurity Operations Centre, *Cloud Computing Security Considerations* (DSD 2012) [78] with cross references to other paragraphs for more information.

While companies and individuals may have a somewhat lower sensitivity to certain IT risks than some government agencies, and hence some considerations may not apply, these considerations do offer a useful starting point for analysing the degree to which Cloud contracts, and the services provided under them, can address wider business and other security risks (Gold 2012) [79]. A cross beside any of these security considerations does not necessarily mean that cloud computing cannot be used, but the security consideration requires additional contemplation to determine if the associated risk is acceptable. The full list can be found in other works; items specifically relevant to data sovereignty questions include:

- My data or functionality to be moved to the cloud is not business critical (19a).
- My data is not too sensitive to store or process in the cloud (20b).
- I can meet the legislative obligations to protect and manage my data (20c).
- I know and accept the privacy laws of countries that have access to my data (20d).
- Strong encryption approved by DSD protects my sensitive data at all times (20e).
- I retain legal ownership of my data (20i)
- Using the vendor's cloud does not weaken my network security posture (21b).
- The vendor does not know the password or key used to decrypt my data (22a).

In particular, 'Protecting Data from Unauthorised Access by a Third Party' flags two critical issues for data sovereignty:

> **Legislative obligations.** What obligations do I have to protect and manage my data under various legislation, for example the *Privacy Act 1988*, the *Archives Act 1983*, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help ensure obligations are met to the satisfaction of the Australian Government?
>
> **Countries with access to my data**. In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

is the failover or redundant data centres? Will the vendor notify me if the answers to these questions change? Data stored in, processed in, or transiting foreign countries may be subject to their laws. Such laws range from Freedom of Information requests by members of the public, through to government lawful access mechanisms.

For example, a foreign owned vendor may be subject to their country's laws even if the vendor is operating within Australia. If the vendor is subpoenaed by a foreign law enforcement agency for access to data belonging to the vendor's customers, the vendor may be legally prohibited from notifying their customers of the subpoena (DSD 2012, p10). Numerous reports in late 2013 have confirmed the frequent operation of such gag orders in the US, with some IT service providers but not others now campaigning for greater transparency. (Hill 2013)

These two issues may explain why DSD recommends agencies against outsourcing information technology services and functions outside of Australia, unless agencies are dealing with data that is all publicly available:

> *"DSD strongly encourages agencies to choose either a locally owned vendor or a foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders. Note that foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor."* (DSD 2012, p1).

A notable feature is an apparent divergence by other agencies towards a more relaxed attitude to advice to the general public and business on Cloud data security, location and jurisdiction: while many operational federal agencies are anecdotally reputed to be still reluctant for security reasons to host their own key data off shore, some regulatory agencies appear more focused on promoting Cloud use for its own sake, with more limited explicit consideration of the jurisdiction aspects of security, and a tendency to focus on "benefits" alone rather than balancing benefits with costs, and in particular, risks (DoC 2014; AGIMO 2013; DBCDE 2013) [80].

If real, one explanation for this apparent inconsistency (if one assumes that underlying security and confidentiality needs are in fact similar) could be a conflict between industry development and free trade promotion considerations for the broader public on the one hand, and security, privacy and confidentiality priorities for government data.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Such a conflict may explain the ambiguity in such divergent advice, and may also suggest a need for caution on the part of readers more attuned to the primacy of security, confidentiality and privacy.

6. Drivers for a Cloud Data Location and Jurisdiction Policy

This section provides an overview of the sorts of obligations or drivers to host Cloud data in one jurisdiction or another, and suggests one response to issues raised in the paper lies in an organisational policy on the topic. It also considers the special case of personal information, and the potential role of de-identification or the (newly controversial) US-EU Safe Harbor model in dealing with (or evading) constraints arising from privacy obligations.

This paper uses developments in Australian law as a starting point for examining these obligations, but the issues raised often have more general application. We also refer to parallel or relevant European and US law. Similar challenges are emerging in these jurisdictions, and in others around the world.

It remains to be seen whether the competing trends for international harmonisation or for local diversification of legal rules will win out, and whether data sovereignty will become a central and complex aspect of such obligations. (The proposed Trans-Pacific Partnership treaty has reputedly, in secret drafts shared with industry but kept from the public, promoted an alternative "digital protectionism" characterisation of jurisdiction-aware cloud contracts and may if implemented complicate the implementation of choices in this area. (Allgeier 2013, 4)

Cloud data location and jurisdiction policy

One response to challenges discussed in this paper and related material is a Cloud data location and jurisdiction policy, which can help guide the entire life cycle of all networked data within an organisation from creation to destruction. Such a policy would be founded on a survey of the specific requirements affecting each aspect of a business or agency. It could help answer questions about whether any data must be, or should be, held in a particular location, or under the control of entities regulated by a particular jurisdiction; and if so, how to respond to this need.

Features of the organisation's regulatory environment such as the following can affect Cloud location and jurisdiction choices:

- What statutes and case law directly affect the company?
- What codes, standards and/or rules of professional practice are the company obliged to follow?

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

- With what codes, standards and/or rules of practices could the company choose to further comply?
- What jurisdictions can specifically affect the data, either through its location or the entities that control it?

Factors affecting a Cloud Data Location and Jurisdiction Policy can include:

- The nature and security profile of the data (or sub-categories of it), and whether particular legal, regulatory or similar obligations favour certain locations or jurisdictions (Peterson et al 2011)
- The characteristics of customers, staff or partners: are there particular expectations or vulnerabilities to take into account?
- Risks associated with exposure to various jurisdictions, especially the attitudes and practices of entities who may be seeking access to the data (Maxwell & Wolf 2012)

Legal obligations: statutory, case law and code compliance in Australia

There are a number of reasons one may *wish* to store data in certain jurisdictions, or with entities regulated or controlled under certain jurisdictions:

- Practical technical reasons relating to current uses (increasingly less likely as cloud services mature)
- Contractual obligations (especially with entities including governments which may be subject to stricter statutory obligations)
- Temporary, time limited obligations to retain locally for certain purposes
- Business reasons, including customer or partner expectations
- Security or confidentiality concerns not easily mitigated by contract, or where the hosting partner is unwilling to accept any responsibility for breach and risk assessment suggests such a risk is unacceptable

The second major reason for the local hosting of data is where you are *required by law* to retain the data in the local jurisdiction, or under the control of a entity regulated by that jurisdiction.

Such requirements will tend to fall into one of the following categories:

1. where a statute either:
   - specifically requires the retention of the document in the home country, or by entities under its control; or
   - operates in such a way that the document should be so retained or controlled in

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

order to prove compliance;

2. where there are cloud data location or control obligations related to compliance with industry codes, or to satisfy industry regulators; or
3. where local hosting of, control of, or access to the document is required because there is a reasonable anticipation of litigation to which the document in question is likely to be relevant.

Note that in Australia there are relatively few specific statutory requirements that data be stored on Australian territory. These include:

- Certain documents must be accessible at the registered office of a company.
- A workplace safety rule in NSW says a workplace safety policy must be held locally.
- A provision in the new *Personally Controlled Health Records Act 2012* (Cth) requires the health records be stored locally by a locally registered entity.
- There are conditions on trans-border data flow of personal information in the new *Privacy Act 1988* (Cth); these are updated in the 2014 version (from the 2012 amendments).
- Obligations to ensure security, say under the *Privacy Act*, may not specify a country or jurisdiction, but there may be some practical effect if appropriate security cannot be delivered under a certain arrangement.

An analysis of the obligations on a specific organisation is beyond the scope of this paper, requiring detailed consideration of many facets of the operation of the entity, and its characterisation by various laws.

It is important to note that, of course, many sorts of data are *not* however subject to any location-based statutory requirements, and can be stored off shore if this is consistent with other obligations and judgements.

Promises, promises: what you tell data subjects or providers at the point of collection

However, it is also important to also consider the disclosures required in Australia at the point of collection, whether from expectations under the *Privacy Act* or other laws, or promises made for business purposes. An organisation's representations to its customers and public as to its data storage processes and practices can in effect create obligations.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

These may form a contractual basis for obligations that are not directly specified in statute, but which later come under the *Australian Consumer Law* s18 (the old s52 *Trade Practices Act*) and so cannot be 'misleading or deceptive'.

This issue of what promises are made to clients or customers when the data was collected is quite an important one: it may be more important overall than laws requiring data to be stored in the jurisdiction.

An organisation needs to have a clear view as to whether it is acting within the scope of the position it has put to its public (or, of course, to which it is bound in its contracts) when it decides to store data in the cloud in or under the influence of a certain jurisdiction. Assurances or promises made to end users or customers must be taken into account in assessing the overall pattern of obligations regarding data storage and control.

What data is regulated as "personal information"?

In contemplating criteria for assessing the security profile and hosting requirements of Cloud data (and hence the suitability of various jurisdictions), it is as we note above, important to consider detailed analysis of the application of particular provisions of applicable laws in relevant jurisdictions to certain classes of data, in addition to those relating to 'third party access' discussed elsewhere in this paper.

As noted above, a central concern is the nature of information considered to be "personal", and hence subject to privacy rules and other measures of sensitivity.

For instance "Personal information" (under Australian privacy law), "Personal Data" (EU) or "Personally Identifying Information" (US) refer to similar but not identical regulatory concepts for important data sets, ones that cover a relatively limited class of business information but often drive decision making.

It may be possible to ensure that information held by a service provider is de-identified and not easily re-identifiable. In such cases there are effectively no privacy rules applying to the data, since it is outside the scope of "personal information". (The ease or difficulty of possible re-identification may affect its characterisation under Australian or EU law; less so under US law.)

There are also longstanding wide exceptions to the coverage of the *Privacy Act* (Cth): small businesses, employee records, information related to corporate customers, and many others. The revised *Privacy Act* in force in 2014 doesn't say that foreign providers must comply with Australian privacy law, only that they must not breach the law in holding Australian data. This may limit the scope of the data to be treated in a certain way.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

A paper from the US Department of Commerce (US Dept. of Commerce 2013) looks at a similar concept arising from the "Safe Harbor" arrangements between the US and EU. If the data processor promises to secure the data and hold it strictly at the direction of the data collector, the "will not breach" obligation is satisfied.

However, as noted above, more recently various entities in Europe have, as result of the Snowden revelations, stepped back from the Safe Harbor arrangements, calling them into question. (European Parliament 2014)

7. Competing 'Frames': Digital Protectionism

Concerns raised by the revelations of Edward Snowden are reported to have already had a significant impact on the willingness of non-US business to adopt US based or controlled Cloud services without analysis of risks, with projected impacts running into the tens of billions of dollars over several years. (Hill 2013)

At the same time, there has been a concerted push to re-frame questions of Cloud location and jurisdiction as "digital protectionism", and thus an affront to free trade. (Snabe 2014; Young 2013)

For instance in its 2014 Report, "Powering the Digital Economy: A Trade Agenda to Drive Growth," (BSA 2014) the Business Software Alliance says:

"To spur trade in digital age products and services, BSA outlines a three-part agenda:

- First, modernize trade rules to reflect the realities of digital commerce as it is being conducted today. This requires facilitating trade in innovative services such as cloud computing, keeping borders open to the free flow of data, and preventing mandates on where servers or other computing infrastructure must be located.

- Second, promote the continued progress of technology innovation. For this, a trade agenda must secure modern intellectual property protections and encourage the use of voluntary, market-led technology standards.

- Third, create level playing fields for all competitors. That requires governments to lead by example. They should be fully transparent in how they choose which technologies to buy, basing decisions on whether a product or service best meets their needs and provides good value, not on where the technology was developed."

The controversial secret TransPacific Partnership (TPP) and Transatlantic Trade and Investment Partnership (TTIP, an Atlantic equivalent) also appear to have elements designed to implement this agenda: an industry lobbyist describes a key aim of the TPP as to

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

"Prohibit parties from requiring the establishment or use of local servers or other infrastructure in order to provide digital products and services in a country" (Allgeier 2013, 4). (See also Assange 2013; US Trade Rep 2013)

This framing of the debate seeks to deprecate concerns over data location and sovereignty in the Cloud and other online services, just at the very time when these concerns are brought into dramatic relief by the controversial (and apparently ineffective) mass metadata and data surveillance practices revealed by Snowden. (Hill 2013)

It is perhaps ironic that the means (TPP and TTIP) of pursuing these clearly sectional interests are themselves challenged as being a threat to sovereignty, apparently even of the US, to the extent that they bypass normal democratic scrutiny (on the basis of being "merely about trade") yet purport to bind governments to implement national laws implementing rules negotiated in secret to tilt the playing field against those seeking to make jurisdictional choices about location and control of cloud data.

8. Conclusion

The bulk of the research for this paper occurred before the Snowden era, but the significant effects of Snowden's revelations about actual surveillance practices, and the threats to commercial and government cryptographic (Ball et al 2013) and other online security measures (Schneier 2013) represented by the 'security' agencies of Australia, the US, the UK and the other "5 Eyes" members have only tended to confirm the focus on third party access that forms a major part of this work.

The complex interlinking secret arrangements between the country that is home to much of the commercial Cloud, the US, and this country make legal and regulatory analysis difficult. There are certainly means to enable law enforcement and security cooperation between the two which tend to bypass locational and jurisdictional barriers. But there are also practical, legal and administrative effects of such barriers which are not wholly removed by such cooperation. On balance, for data which is significant and sensitive, there may still be benefits to considering location and jurisdiction issues.

In addition, the pressure for reform, not least from the two substantial reports by President Obama's hand-picked review team in December 2013 and the Congressional Oversight Board in February 2014, and court cases in the US (Judge Richard Leon, *Klayman and Strange v NSA*, US District Court for the District of Columbia in 16 December 2013) drawing out concerns over lawfulness, proportionality and constitutionality, may over time rein in the excesses apparently revealed. The most disturbing of these relate to exceptional measures

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

introduced to fight the exceptional perceived hazard of terrorism now being used for traditional international commercial trade espionage purposes (Jabour & Pengelly 2014).

If so, national sovereignty and jurisdiction over online data and metadata may regain something of its former significance.

It also remains to be seen if the agenda of US cloud and online business to deprecate data sovereignty concerns as unfair "protectionism", in spite of the apparently indiscriminate threats to online security and confidentiality revealed as sourced in their home jurisdiction, and to require national measures to restrict them is successfully implemented in the TPP and TTIP. If this were the case, exercising choices for consumers and business based on the perceived best location for security and privacy in the Cloud may be prevented or obstructed by law.

This would potentially reduce a significant incentive for all governments and businesses to respond to the Australian consumer preference for security and privacy of their data to be protected by location and jurisdiction measures, as identified by the survey which opened this paper. Personal information in particular, but government and business information as well, should probably be recognised as having critical risk characteristics beyond a status of mere trade commodities, such that their hosting in the Cloud may need to be open to whatever precautions and choices those liable for or subject to those risks may seek to make, including choices about location and jurisdiction. If these choices can be freely made, presumably the market will respond in creative ways, as indeed appears to be happening; were they to be constrained by law, the incentive for effectively addressing the concerns may be weakened, and the ultimate levels of trust and confidence in the cloud, the aim of good regulation, may be reduced.

Acknowledgements

This paper arises from a collaborative project (http://cyberlawcentre.org/data_sovereignty/) supported by NEXTDC (http://www.nextdc.com.au), Baker & McKenzie (http://www.bakernet.com) and AON (http://www.aon.com). Thanks to the following for their major contributions to earlier related works and this paper: Kevin Kalinich (AON), Patrick Fair and Adrian Lawrence (Baker and McKenzie); thanks also to Bruce Baer Arnold, University of Canberra, Alison Cook, postgraduate researcher, UNSW Law Faculty, Prof Graham Greenleaf, Professor of Law and Information Systems, UNSW Law Faculty, and interns including Tim Chiang, Annette Haddad, Natasha Hammond-Marks, Sasha Kolodkina, David Lee, Felix Lim, Lauren Loz, Peter Matuszak, Ryan Ruslim, Tia Singh, and Alice Yang (all of UNSW Law), and Cassandra Switaj (Bond University) and Bonnie Yiu

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

(UTS). Responsibility is of course solely that of the author; project supporters and contributors to earlier related works may not necessarily endorse everything in this paper.

References

ACMA. 2013. 'AAPT warned about privacy', media release 26/2013, 24 April 2013. Available at: http://www.acma.gov.au/ theACMA/Newsroom/Newsroom/Media-releases/acma-issues-formal-warning-to-aapt

AGIMO. 2011. "Cloud Computing Strategic Direction Paper: Opportunities and for use by the Australian Government". April 2011. Available at: http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

AGIMO. 2012. Better Practice Guide. (July 2012). 'Negotiating the cloud – legal issues in cloud computing agreements'. Available at: http://www.finance.gov.au/e-government/strategy-and-governance/ docs/negotiating_the_cloud_-_legal_issues_in_cloud_computing_agreements.pdf

AGIMO. 2013. "Australian Government Cloud Computing Policy: Maximising the Value of Cloud [for Australian Government Agencies]", Department of Finance and Deregulation, 29 May 2013. At: http://agimo.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf

Allgeier, P (President, Coalition of Services Industries (CSI)). 2013. "Services Business Objectives for TPP", U.S. Business Coalition for TPP, December 18, 2013, Available at: https://servicescoalition.org/images/TPP_Business_Coalition_Hill_Briefing_Dec_18_2013.pdf

APRA. 2010. Australian Prudential Regulation Authority (APRA) guidelines "Outsourcing and Offshoring: Specific considerations when using cloud computing services," 15 Nov. 2010, Available at: http://www.apra.gov.au/CrossIndustry/ Documents/Letter-on-outsourcing-and-offshoring-ADI-GI-LI-FINAL.pdf

Assange, J. 2013. US, Australia isolated in TPP negotiations, Wikileaks (editorial), 15th November 2013, Available at: http://wikileaks.org/US-Australia-isolated-in-TPP.html. Includes links to the IP chapter of the text.

Attorney Generals Department. 2013. *Telecommunications (Interception and Access) Act 1979 Annual Report*, 2012-2013, Available at: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf

Ball, J; Borger J; Greenwald G. 2013. Revealed: how US and UK spy agencies defeat internet privacy and security, *Guardian Weekly*, 6 September 2013

Bamiah, MA; Brohi, SN. 2011. "Exploring the Cloud Deployment and Service Delivery Models", *International Journal of Research and Reviews in Information Sciences* (IJRRIS) Vol. 1, No. 3, September 2011, 77.

Barwick, Hamish. 2012a. 'The cloud security minefield', *CIO*, 5 September 2012.

Barwick, Hamish. 2012b. Data sovereignty still misunderstood in Australia: Microsoft,' *Computerworld*, 18 September 2012.

Baty, Craig. 2011. CTO, Fujitsu Australia and New Zealand, transcript of Korea-Australia-New Zealand (KANZ) Broadband Summit 2011. Available at:http://www.archive.dbcde.gov.au/__data/assets/pdf_file/0005/138299/Craig_BatyCloud_Computing.pdf

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.31

BeVier, L. 1999. 'The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break up of AT&T', *Stanford Law Review*, Vol. 51, No. 5 (May, 1999), pp. 1049-1125. http://dx.doi.org/10.2307/1229406. Available at: http://www.askcalea.net/

Bleich, Jeffrey (US ambassador). 2012. 'Cloud agreement can bring blue skies', The Age (Melbourne), 11 December 2012, Available at: http://www.theage.com.au/it-pro/government-it/cloud-agreement-can-bring-blue-skies-20121211-2b77f.html

Burr, J. Beckwith. 2010. *The Electronic Communications Privacy Act of 1986: Principles of Reform*, Available at <http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf>.

Business Software Alliance. 2014. BSA Proposes Forward-Looking Trade Agenda to Stop the Spread of Digital Protectionism, 30 January 2014 Available at: http://www.bsa.org/news-and-events/news/2014/january/01302014digitaltradeagenda

Capgemini. 2012. "Business Cloud: The State of Play Shifts Rapidly: Fresh Insights into Cloud Adoption Trends," 29 November 2012, p.19, Available at: http://www.capgemini.com/business-cloud-the-state-of-play-shifts-rapidly/ or http://www.youtube.com/ watch?v=v_ga9orIzFI (worldwide survey of 460 IT and business leaders at companies with over 10,000 employees).

Cate, Fred H. 2007. 'The Vanishing Fourth Amendment', *Privacy and Security Law Report*, BNA, 6 *PVLR* 1875 (Dec. 10, 2007).

Cate, Fred H; Eisenhauer, Margaret P. 2007. Between a Rock and Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements, 6 PVLR 229 (Feb. 5, 2007).

Chapman, Chris (Chair and CEO, ACMA). 2013. Opening remarks, Launch of 'Data Sovereignty and the Cloud—a Board and Executive Officers' Guide', 2 July 2013, Sydney. At: http://www.acma.gov.au/theACMA/Newsroom/Newsroom/Speeches/launch-of-data-sovereignty-and-the-cloud

Chawki, Dr Mohamed, Judge from the Egyptian Council of State. 2011. 'Egypt's Cyber Revolution: Tweeting from Tahrir Square', Cyberspace Law and Policy Centre, UNSW, 18 May 2011, at: http://cyberlawcentre.org/2011/talks/ltt_chawki.htm

Citi Research. 2012. *Cloud Computing – a two part series*, Part 2: Market Sizing, Barriers, Value Network and Outlook, December 2012, page 4.

Connolly, Chris. 2008. 'US safe harbor - fact or fiction?' *Privacy Laws and Business International* 96 December 2008.

Connolly, Chris; Vaile, D. 2012. Drowning in Codes of Conduct: An analysis of codes of conduct applying to online activity in Australia, UNSW Cyberspace Law and Policy Centre, March 2012, Available at: http://cyberlawcentre.org/onlinecodes/report.pdf

DBCDE. 2013. National_Cloud_Computing_Strategy 2013. Available at: http://www.dbcde.gov.au/__data/assets/pdf_file/0008/163844/2013-292_National_Cloud_Computing_Strategy_Accessible_FA.pdf

Dekker, M. 2012. *Critical Cloud Computing: A CIIP perspective on cloud computing services*, ENISA, December 2012. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

Department of Communications (DoC). 2014. Cloud Computing Regulatory Stock Take, forthcoming, 2014 [after consultation in December].

Dobbie, Phil. 2013. 'Forget PRISM: Who's watching on your doorstep?', *SMH*, 18 June 2013, Available at: http://www.zdnet.com/au/forget-prism-whos-watching-on-your-doorstep-7000016935/.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

DSD. 2012. Australian Signals Directorate. Cloud Computing Security Considerations. Available at: http://www.asd.gov.au/publications/csocprotect/cloud_computing_security_considerations.htm p1.

EC Directorate-General for Justice. 2012a. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM/2012/09 final, 25 January 2012, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT

EC Directorate-General for Justice. 2012b. 'Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses,' media release, 25 February 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm

European Parliament. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Article 25, OJ L 281, 23.11.1995, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

European Parliament. 2006. Resolution on the interception of bank transfer data from the SWIFT system by the US secret services, P6_TA (2006) 0317, 6 July 2006, Available at: http://www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2006-0317&language=EN

European Parliament. 2014. Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI) 21 February 2014, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN

Fleming, Jeremy 'US makes first public comment over draft EU data privacy law', *EurActiv*, 29 April 2013, at: http://www.euractiv.com/infosociety/us-airs-views-eu-privacy-rules-news-519279

Forsheit, Tanya L. 2010. "E-Discovery Involving Cloud Facilities." *Computer & Internet Lawyer* 27, no. 12 (December 2010): 1-7. *Business Source Premier*, EBSCOhost (accessed May 9, 2013).

Frost and Sullivan. 2012. *Australian Contact Centre Market* 2012, Available at: http://www.prnewswire.com/news-releases/frost--sullivan-cloud-based-contact-centre-solutions-poised-to-challenge-traditional-on-premise-model---growing-awareness-of-cloud-based-contact-centre-solutions-177556851.html; and http://www.mcafee.com/us/solutions/cloud-security/news/20120809-01.aspx

FTC. 2014. Federal Trade Commission. 'FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework', Media Release, January 21, 2014, Available at: http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply

Gellman, B; Poitris, M. 2013. 'Documents: U.S. mining data from 9 leading Internet firms; companies deny knowledge', *Washington Post*, 7 June 2013, Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. See Slides at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Gilbert, Francoise. 2010. 'Cloud Service Contracts May Be Fluffy: Selected Legal Issues to Consider Before Taking Off', *J Internet Law* 14 No. 6, December 2010, p 17

Gold, Joshua. 2012. 'Protection in the Cloud: Risk management and insurance for cloud computing' (2012) 15(3) *J Internet Law* 23

Greenwald, G. 2013. 'NSA collecting phone records of millions of Verizon customers daily', *The Guardian*, 6 June 2013, Available at: http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

Hill, K. 2013. 'How the NSA Revelations are Hurting Businesses', *Forbes*, 10 September 2013, Available at: http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/

Hunton & Williams LLP. 2014. 'European Parliament Adopts Draft General Data Protection Regulation; Calls for Suspension of Safe Harbor', 12 March 2014, Available at: https://www.huntonprivacyblog.com/2014/03/articles/european-parliament-adopts-draft-general-data-protection-regulation-calls-suspension-safe-harbor/#more-5892

Irion, Kristina. 2012. 'Government Cloud Computing and the Policies of Data Sovereignty' (2012) 4 *Policy & Internet* 3, 40

Jabour, B; Pengelly, M. 2014. 'Australia spied on Indonesia talks with US law firm in 2013', theguardian.com, Sunday 16 February 2014, Available at: http://www.theguardian.com/world/2014/feb/16/australia-spied-indonesia-talks-us-firm

JPCIS. 2013. Joint Parliamentary Committee on Intelligence and Security (JPCIS). *Report of the Inquiry into Potential Reforms of National Security Legislation*, Parliament of Australia, 24 June 2013. At: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm

Keane, B. 2012. 'Protectionism, free trade and security up in the cloud', *Crikey*, 12 December 2012, at: http://www.crikey.com.au/2012/12/12/protectionism-free-trade-and-security-up-in-the-cloud/

Kessler, David J; Coval, Christopher P; Blenkinsop, Peter. 2008. Is Personal Data Located Outside the United States 'Not Reasonably Discoverable'?, 7 *PVLR* 1356 (Sept. 15, 2008).

Kisswani, Nazzal. 2012."Telecommunications interception and access regulation framework in the US and the UK." *International Journal of Technology Policy and Law* 1, no. 1 (2012): 25-47. http://dx.doi.org/10.1504/IJTPL.2012.045944

Kuner, C. 2010. *Transborder Data Flow Regulation and Data Privacy Law* (Oxford: Oxford University Press, 2010)

Lee, Jane. 2012. 'Million-dollar fines set for privacy breaches', Sydney Morning Herald, 30 November 2012, Available at: http://www.smh.com.au/it-pro/security-it/milliondollar-fines-set-for-privacy-breaches-20121130-2al1e.html

LeMay, Renai. 2013. 'Interpol filter scope creep: ASIC ordering unilateral website blocks,' *Delimiter*, 15 May 2013, Available at: http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/

Ludwig, Sean. 2011. 'Cloud 101: What the heck do IaaS, PaaS and SaaS companies do?', *VentureBeat* blog, 14 November 2011, Available at: http://venturebeat.com/2011/11/14/cloud-iaas-paas-saas/

Lynch A; Williams, G. 2006. *What Price security? Taking Stock of Australia's Anti-Terrorism Laws* (2006) UNSW Press

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Maurushat, Alana. 2009. 'Data Breach Notification Law Across the World from California to Australia,' *Privacy Law and Business International*, February 2009. Available as [2009] UNSWLRS 11 at: http://www.austlii.edu.au /au/journals/UNSWLRS/2009/11.html

Maxwell, Winston; Wolf, Christopher. 2012. 'A Global Reality: Governmental Access to Data in the Cloud – A comparative analysis of ten international jurisdictions (Governmental access to data stored in the Cloud, including cross-border access, exists in every jurisdiction)', Hogan Lovells, July 2012

McNicholas, Edward R. 2009.' National Security Letters: Practical Advice for Understanding and Handling Exceptional Requests' 8 *PVLR* 13 (Mar. 30, 2009). Available at http://www.sidley.com/publications/detail.aspx?pub=2047

Mayer-Schonberger, Viktor; Cukier, Keith. 2013. *Big Data, A revolution that will transform how we live, work and think* (John Murray/Hachette, London, 2013)

Michaelsen, Christopher. 2010. "Reforming Australia's National Security Laws: The Case for a Proportionality-Based Approach" (2010) 29(1) *University of Tasmania Law Review* 31

Morris, Chris/IDC. 2012. *Asia/Pacific (Excluding Japan) Cloud Services and Technologies End-User Survey, 2011*, IDC, November 2012.

Nicholls, R; Rowland, Michelle. 2007. "Message in a bottle: Stored communications interception as practised in Australia." In The Second Workshop on the Social Implications of National Security, p. 83. 2007

Nielsen, N. 2013. 'The man behind the EU Parliament's data regulation,' *EU Observer,* 6 May 2013, at: http://euobserver.com/justice/119951

OAIC. 2014. Office of the Australian Information Commissioner. *Guide to Handling Personal Information Security Breaches*. Available at: http://www.oaic.gov.au/ publications/guidelines/privacy_guidance/Data_breach_notification_guide_April2012FINAL.pdf

Office of the Inspector General. 2007. *Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act*, Mar. 2007. Available at <http://www.justice.gov/oig/special/s0703b/final.pdf

Office of the US Trade Representative, Trans-Pacific Partnership (TPP), 10 December 2013, http://www.ustr.gov/tppTR: 2013)

Pavolotsky, John. 2012. 'Cloud Services and Information Security: The Public vs. Private Service Provider Debate' (2012) 37 New Matter 1, 32, Available at: http://ssrn.com/abstract=2022519;

Peterson, Zachary N.J; Gondree, Mark; Beverly, Robert. 2011. 'A position paper on data sovereignty: The importance of geolocating data in the cloud', paper presented at Hotcloud 11, Portland, Oregon, USA, 14 June 2011. Available at: http://static.usenix.org/event/hotcloud11/tech/final_files/Peterson.pdf

Pryce, Jeffrey F. 2006. 'The Globalization of Electronic Evidence Gathering: U.S. Joins Council of Europe Convention on Cybercrime', 5 *PVLR* 1450 (Oct. 16, 2006).

QMUL Cloud Computing Project. 2010. 'What is Cloud Computing?', Queen Mary University London, 2010, Available at: http://www.cloudlegal.ccls.qmul.ac.uk/what/index.html

Roach K. 2010. 'The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations', in Andrew Lynch, Nicola McGarrity, George Williams, eds., *Counter-Terrorism and Beyond - The Culture of Law and Justice After 9/11*, Routledge, Sydney, May 2010.

Robinson, Frances. 2013. 'U.S. to EU: U.S. Data Law Is Brill,' *Wall Street Journal*, 19 April 2013, Available at: http://blogs.wsj.com/brussels/2013/04/19/u-s-to-eu-u-s-data-law-is-brill/.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Rodrigues, R; Barnard-Wills, D; Wright, D. 2013. 'EU privacy seals project: Inventory and analysis of privacy certification schemes', European Commission, Joint Research Centre, 2013.

Salgado, Richard. 2010. Written Testimony of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google Inc., House Judiciary Subcommittee on the Constitution, Civil Rights and Civil Liberties, Hearing on *Electronic Communications Privacy Act* Reform (May 5, 2010).

Schneier, B. 2013. 'The US government has betrayed the internet. We need to take it back', *The Guardian*, Friday 6 September 2013

Snabe, Jim Hagemann. 2014. 'Don't let data protection turn into protectionism' Reuters US - Opinion: The Great Debate, 9 January 2014, Available at <http://blogs.reuters.com/great-debate/2014/01/09/dont-let-data-protection-turn-into-protectionism/>.

Srinivasan, Madhan Kumar; Sarukesi, K; Rodrigues, Paul; Sai Manoj, M; Revathy P. 2012. 'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment', International Conference on Advances in Computing, Communications and Informatics, Chenai, India, 5 August 2012

Svantesson, D J. 2013. *Extraterritoriality in Data Protection Law* (Copenhagen: Ex Tuto, 2013)

US Dept. of Commerce. 2013. 'Clarifications Regarding the US EU Safe Harbor Framework and Cloud computing', April 2013. Available at: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

Verizon. 2013. 2013 *Data Breach Investigations Report*. Available at: http://www.verizonenterprise.com/DBIR/2013/

Walden, Ian; Luciano, Laise Da Correggio. 2011. 'Ensuring Competition in the Clouds: The Role of Competition Law?' (April 7, 2011), Available at http://ssrn.com/abstract=1840547

Young, Michael. 2013. 'Global Protectionism on the Rise - But who's being protected? Citizens or local competitors?' *Tech Page One*, 23 December 2013 Available at <http://techpageone.dell.com/business/global-protectionism-rise/#.UvxKAL9WjHg>.

Zimmerman, M. 2013. 'In Depth: The District Court's Remarkable Order Striking Down the NSL Statute', EFF, 18 March 2013, Available at: https://www.eff.org/deeplinks/2013/03/depth-judge-illstons-remarkable-order-striking-down-nsl-statute

Endnotes

[1] Co-convenor, Cyberspace Law and Policy Community, UNSW Faculty of Law, d.vaile@unsw.edu.au.

[2] See for instance the government and corporate strategy documents listed in our extensive bibliography published last year in this journal.

[3] Based on material from Microsoft, 'Windows Azure Platform: Cloud Development Jump Start' via podcast at http://itunes.apple.com/si/podcast/windows-azure-platform-cloud/id415763483, in Ludwig 2011

[4] Private cloud users do not raise loss of control and security as much: see Morris/IDC 2012.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[5] Image from Sam Johnston at: http://en.wikipedia.org/wiki/File:Cloud_computing_types.svg.

[6] Australian Privacy Principles in force from 14 March 2014 encourage greater disclosure of countries to which personal information may be sent. The proposals from ALRC and Prime Minister and Cabinet leading to the 2013 breach notification "privacy alerts" bill lapsed with the 2013 election.

[7] The Privacy Amendment (Privacy Alerts) Bill, introduced to Federal Parliament on May 29, 2013, would have amended the *Privacy Act* 1988 (Cth) (*Privacy Act*) to require data breach reporting obligations for a "Serious Breach" for entities regulated by the Privacy Act, making it less likely an Australian cloud provider could avoid revealing personal info data breaches for personal info under their control -- wherever it is held. A serious data breach is where an Australian entity holds personal information relating to one or more individuals, and the information is either: (a) accessed or disclosed without authority, and the access or disclosure will result in a "real risk" of serious harm (including financial or economic harm and harm to reputation); or (b) lost in circumstances where (a) may occur. A serious data breach also occurs where an overseas entity holds personal information that has been disclosed to it by an Australian entity in accordance with Australian Privacy Principle 8.1, and (a) or (b) occurs in respect of that foreign entity. Where a breach reporting obligation arises, the entity must prepare a disclosure notice setting out the nature of the data breach, information at risk, and any steps that affected individuals can take to mitigate the effects of the breach. Failure to notify the Commissioner or affected individuals when required to would be an "interference of the privacy of an individual". This would have triggered enforcement rights under the *Privacy Act*, including the possibility of a determination by the Commissioner that the entity is required to pay compensation to affected individuals and can also attract a civil penalty of up to $1.7million for corporations. Exemptions would have reduced the impact. Given pressure from jurisdictions in US and EU with such laws already in place, a revised version of these requirements may eventually return to Parliament.

[8] See http://www.dbcde.gov.au/__data/assets/pdf_file/0008/163844/2013-292_National_Cloud_Computing_Strategy_Accessible_FA.pdf

[9] For an extreme example, the then Egyptian government suspended internet services in the Arab spring of 2011 by the simple but [technically if not politically!] effective expedient of blocking access to the key packet routing infrastructure, both internally and out of the country, for a short period, for all but a tiny group of government networks. See Dr Mohamed Chawki 2011

[10] OAIC At: http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/

[11] Though note observations by Nigel Waters, Australian Privacy Foundation policy committee chair and former deputy Privacy Commissioner, who suggests the new law weakens, rather than strengthens privacy protections because it does not give people the right to have a complaint determination made, noting the Privacy Commissioner's office has made only nine determinations in 23 years. "This approach assumes the Australian government is in a position to do something about breaches that occur in another country. At the end of the day the only redress is if the company decides to bring a civil proceeding against [a party in] the country, which is nowhere near as effective as an individual being able to complain directly about the breach." Lee 2012

[12] For an analysis of Code complexity, see Chris Connolly and D Vaile 2012

[13] The *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth) becomes effective in March 2014, with penalties of up to $1.1 million. Before then, different rules applied for private businesses and the public sector; there is still no state or federal statutory tort or similar cause of action for invasion of privacy; and in many other ways Australia's

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

information security laws fall short of international best practice standards. In particular, Australia has lagged behind foreign counterparts in enacting laws holding businesses responsible for losing sensitive information about their customers, employees, and others. Organisations may voluntarily report security breaches, but very few do. Australian does not impose any binding general obligation to do so except in limited circumstances, such as the *Personally Controlled Electronic Health Records Act* 2012 provisions requiring notification if unauthorized disclosure of patient health information has occurred; see Part 4, at: http://www.comlaw.gov.au/Details/C2012A00063/ Html/ Text#_Toc327957207. For the most part though, breach notification is voluntary, and businesses are encouraged to use the Office of the Australian Information Commissioner's *Guide to Handling Personal Information Security Breaches*, at: http://www.oaic.gov.au/publications/guidelines/privacy_guidance/Data_breach_notification_guide_April2012FINAL.pdf. A voluntary scheme with unenforced compliance may offer perverse incentives to avoid compliance, especially where voluntary notifiers have no protection and fear being singled out for publicity. (The 2013 Privacy Alerts bill, which may strengthen reporting obligations, is covered below.)

[14] See also s 16C *Privacy Act*, which holds the disclosing entity accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.

[15] APRA, the Australian regulatory authority overseeing Australian banks, determines whether they may use public cloud computing that hosts data offshore on a case-by-case basis. Although there are no laws explicitly prohibiting a bank from using an offshore cloud provider, APRA's outsourcing risk management guidelines make it difficult for banks to enter in to such arrangements as a practical matter. APRA requires banks to obtain preapproval to use offshore data centres by showing the existence of adequate risk management procedures. Banks must also elicit from the vendor a contractual commitment to allow APRA access to the data centre. Some banks have aggressively pursued cloud solutions, even public offshore clouds, but with a measure of trepidation due to regulatory uncertainty. Like banks, insurance companies must also obtain APRA approval to use cloud environments hosted outside Australia's borders or jurisdiction.

[16] See also "Negotiating the cloud – legal issues in cloud computing agreements: Better Practice Guide" (July 2012), http://www.finance.gov.au/e-government/strategy-and-governance/ docs/negotiating_the_cloud_-_legal_issues_in_cloud_computing_agreements.pdf

[17] "From a security perspective, the concentration of data is a 'double-edged sword'; large providers can offer state-of-the-art security, and business continuity, spreading the costs across many customers. But if an outage or security breach occurs, the impact is bigger, affecting many organisations and citizens at once." See Dekker 2012

[18] For the proposal, see EC Directorate-General for Justice, 25 January 2012. See section 4., 'Data protection in a globalised world', for impact on hosting EU data outside EU. For a summary, see EC Directorate-General for Justice, 25 February 2012

[19] See section 4, "*Third party access by legal means: Does it matter where your data is stored?*" For instance, health information may not be transferred to a service provider unless that provider agrees to comply with the *Health Insurance Portability and Accountability Act* (HIPAA). The *Violence Against Women Act* prohibits domestic violence service providers from disclosing information to third parties without consent. (Public Law 109-162 as amended by Public Law 109-271). Income tax return information may not be disclosed without the taxpayer's consent. (*Internal Revenue Service Rules* - 26 U.S.C. § 6713 and § 7216; 26 C.F.R. §301.7216) A financial institution may not disclose personal financial information about a consumer without his or her consent: The *Gramm-Leach-Bliley Act* (15 U.S.C. § 6802); Video and cable television records may not be disclosed. *Video Privacy Protection Act* (18 U.S.C. § 2710) and *Cable Communications Policy Act* (47 U.S.C. § 551).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[20] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (*USA PATRIOT Act*) of 2001, at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

[21] The *PATRIOT Act* permits the US government to obtain personal information held in any country in the world that is being held by US companies, or those with sufficient connections to the US. The US Federal Bureau of Investigation (FBI) may obtain a court order requiring US Internet service providers to disclose records stored on their servers, without the data subject even being notified. Thus, if cloud data is transmitted to the US or merely hosted by a US-based company anywhere in the world, it is potentially subject to the *PATRIOT Act*. See section 4 below.

[22] US-EU Safe Harbor, 2000, at: http://export.gov/safeharbor/eu/eg_main_018365.asp

[23] US-Swiss Safe Harbor, 2008, at: http://export.gov/safeharbor/swiss/index.asp

[24] Canada's national "Personal Information Protection and Electronic Documents Act" (PIPEDA) regulates personal data gathered and maintained in the course of commercial activities. PIPEDA requires advance consent for disclosure of personal information and must allow individuals to correct inaccurate information. Provincial laws in Alberta, British Columbia, and Quebec offer additional privacy protection similar to PIPEDA, but each has its own definition of "personal data."

[25] *Lawson v. Accusearch Inc.*, (F.C.), 2007 FC 125, [2007] 4 F.C.R. 314, February 5, 2007, Docket:T-2228-05, at: http://reports.fja.gc.ca/eng/2007/2007fc125/2007fc125.html

[26] *See* Digital Due Process, at: http://www.digitaldueprocess.com/

[27] While Australian Law Reform Commission recommended (see Chapter 31 of *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008) that privacy laws should provide that an agency or organisation that transfers personal information about an individual outside Australia will remain responsible for the protection of that information, in the hope of ensuring that an individual has the ability to approach a local privacy regulator and seek redress from someone in Australia if the overseas recipient breaches the individual's privacy, this responsibility was excluded if the entity was 'required or authorised by law' to transfer it. Recent amendments to the *Privacy Act*, discussed above, partly strengthen this exclusion by basing the new test on compliance with Australian law. Similar exceptions would be expected in the event of disclosure to third parties where this is 'required or authorised by law'. ALRC suggested merely that the Privacy Commissioner should offer 'guidance' to transferors, recommending 'a warning that foreign laws might require the disclosure of the information to foreign government agencies'. <http://www.austlii.edu.au/au/other/alrc/publications/reports/108/31.html#Heading748 >

[28] Tenth Circuit Finds no Expectation of Privacy in Data Given Freely to ISP, 7 *PVLR* 418 (Mar. 24, 2008).

[29] *Worldwide Film Entm't LLC v. Does 1-749*, D.D.C., No. 10-38 (May 13, 2010); Web User Lacked Privacy Interest in Account Data, 9 *PVLR* 768 (May 24, 2010).

[30] See *U.S. v. Perrine*, 518 F.3d 1196 (10th Cir. March 11 2008) No. 06-3336; < http://ca10.washburnlaw.edu/cases/2008/03/06-3336.pdf >, Tenth Circuit Finds no Expectation of Privacy in Data Given Freely to ISP, 7 *PVLR* 418 (Mar. 24, 2008).

[31] See *U.S. v. Bynum*, No. 08-4207, 4th Cir. (May 5, 2010); Yahoo! User Lacked Privacy Expectation in Account Data Shared with Yahoo!, Others, 9 *PVLR* 707 (May 17, 2010).

[32] *U.S. v. Li*, S.D. Cal., No. 07 CR 2915 (Mar. 20, 2008); No SCA Reasonable Privacy Expectation for ISP Customer IP Address, Log-In Data, 7 *PVLR* 501 (Apr. 7, 2008).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[33] *U.S. v. Ahrndt*, D. Ore., No. 08-468, 2010 U.S. Dist. LEXIS 7821 (Jan. 28, 2010); No Fourth Amendment, ECPA Privacy Claims in Documents Shared on Unsecured Network, 9 *PVLR* 257 (Feb. 15, 2010).

[34] *Lukowski v. County of Seneca*, W.D.N.Y., No. 08-CV-6098 (Feb. 24, 2009); Privacy Interest in ISP-Stored Identifying Data Held to Depend on Terms of Service, 8 *PVLR* 397 (Mar. 9, 2009).

[35] Detailed statistics are provided in Attorney Generals Department, *Telecommunications (Interception and Access) Act 1979 Annual Report*, 2012-2013, at: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf

[36] Exceptions 10.1(d) and 11.1(e) were part of the Information Privacy Principles which bind federal agencies prior to the December 2012 amendments coming into force in 2014; there were similar provisions in the National Privacy Principles which apply more broadly, and in the new Australian Privacy Principles. They prevent use beyond that for which it was collected or consented to [unless] 'use of the information for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.'

[37] Pub. L. 95-511

[38] ACLU Challenges FBI National Security Letter; First Use of Power to Demand Library Data, 4 *PVLR* 1105 (Sept. 5, 2005).

[39] *See* http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/85A16ADB86A23AD1CA256FC600072E6B? OpenDocument, revised 2005.

[40] 50 U.S.C. § 1861(a)(1); Section 215 of the *USA Patriot Act* of 2001 amended *Foreign Intelligence Surveillance Act*. Code section references in footnotes below are to the relevant sections of *FISA* as amended by Section 215 of *USA Patriot Act*.

[41] 50 U.S.C. § 1861(c) <http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001861----000-.html>

[42] 50 U.S.C. § 1822(a)(1) & (4) <http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001822----000-.html>

[43] 18 U.S.C. § 3103a(c) <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00003103---a000-.html>

[44] 50 U.S.C. § 1805(c)(3) <http://www.law.cornell.edu/uscode/50/usc_sec_50_00001805----000-.html>

[45] 50 U.S.C. § 1805(a)(2); as above.

[46] 50 U.S.C. § 1805(c)(2)(B) ; as above.

[47] 50 U.S.C. § 1802 <http://www.law.cornell.edu/uscode/50/usc_sec_50_00001802----000-.html>

[48] 50 U.S.C. § 1802(a)(4) ; as above.

[49] 50 U.S.C. § 1842 <http://www.law.cornell.edu/uscode/50/usc_sec_50_00001842----000-.html>

[50] 50 U.S.C. § 1842 (c)(B)(i)-(ii) ; as above.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[51] 'High Court Pick Sotomayor Ruled for ISP in National Security Letter Free Speech Case', 8 *PVLR* 808 (June 1, 2009).

[52] *High Court Pick Sotomayor Ruled for ISP in National Security Letter Free Speech Case*, 8 PVLR 808, June 1, 2009

[53] See *National Security Letter Statute* (18 U.S.C. § 2709) at: <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002709----000-.html>

[54] *John Doe Inc., et al. v. Mukasey, et al.,* US CA 2nd Circuit NY, Docket 07-4943-cv, December 15, 2008, at: http://www.aclu.org/pdfs/safefree/doevmukasey_decision.pdf

[55] *In re National Security Letter,* Docket C 11-02173 SI, US DC Northern District California, Order Granting Petition to Set Aside NSL, 15 March 2013, at https://www.eff.org/node/73523. See also Zimmerman M, 18 March 2013

[56] See < http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm>

[57] Personal communication to co-author from senior SWIFT officers visiting UNSW in 2008.

[58] EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281, 23.11.1995, p. 31–50).

[59] <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/266>

[60] Recent Lawsuit Shows Challenges in Applying Warrant Rule, SCA to Remotely Stored E-Mail, 9 *PVLR* 618 (Apr. 26, 2010).

[61] *Id*.

[62] *Rehberg v. Paulk*, No. 09-1187, 11th Cir. (Mar. 11, 2010).

[63] *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008).

[64] *Warshak v U.S.*, 490 F.3d 455 (6th Cir. 2007).

[65] CrimTrac is a Commonwealth government organization designed to assist law enforcement by creating databases and coordinating national information sharing solutions; it has no direct law enforcement role.

[66] At: http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s313.html

[67] At: http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/

[68] Privacy Groups Urge Democrats to Review Bush Anti-Terror Programs, 6 *PVLR* 132 (Jan. 22, 2007).

[69] House Approves FISA Reauthorization bill with Retroactive Telecom Immunity Provision, 7 *PVLR* 931 (June 23, 2008); Bush Signs Wiretap Law, which Lacks Retroactive Liability Protection for Companies, 6 *PVLR* 1279 (Aug. 13, 2007).

[70] Anti-Terror Issues Could Drive New Surveillance Privacy Rules, 8 *PVLR* 59 (Jan. 12, 2009).

[71] *Gonzales v. Google, Inc*., 234 F.R.D. 674 (N.D.Cal, 2006), < http://www.google.com/press/images/ruling_20060317.pdf>; Judge Orders Google to Surrender to DOJ 50,000 Random Internet Addresses, 5 *PVLR* 437 (Mar. 27, 2006).

[72] *In re Uranium Antitrust Litigation*, 480 F. Supp. 1138, 1144 (N.D. Ill. 1979) (distinguishing from the situation where a US court orders someone in the US to produce documents located abroad).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[73] Subject to reservations retaining the operation of existing bilateral mutual assistance treaties and US law in some respects. *See* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[74] *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, and Exchange of Notes,* [1999] ATS 19, <http://www.austlii.edu.au/au/other/dfat/treaties/1999/19.html>

[75] *See* <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>

[76] Legislation implementing the *Convention* passed in 2012 and it came into force in Australia in March 2013.

[77] While pre-dating emerging protectionism debates, Walden &Luciano suggest that alternative legal mechanisms, specifically measures to promote open standards and interoperability in the context of public procurement, as well as a data portability right as a demand-side measure, are likely to have a more significant impact on competition in the cloud computing sector than intervention using traditional competition measures. More recently, see Swedish Data Inspection Board's decision of 10 June 2013 against the use of certain cloud apps by public sector body due to contractual uncertainty, at: http://www.datainspektionen.se/press/nyheter/2013/fortsatt-nej-for-kommun-att-anvanda-molntjanst/; see also http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/.

[78] DSD DSD: 2012/Dept. of Defence, Canberra, September 2012. At: http://www.dsd.gov.au/infosec/cloudsecurity.htm

[79] See also section 3 above

[80] Others see bibliography; Department of Communications (DoC), Cloud Computing Regulatory Stock Take, forthcoming, 2014

Cite this article as: Vaile, David. 2014. 'The Cloud and data sovereignty after Snowden'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 31.1-31.58. DOI: http://doi.org/10.7790/ajtde.v2n1.31. Available from: http://telsoc.org/journal

Geographic Internet domains
Challenges for the developing DNS

Heather Ann Forrest
Australian Catholic University

Geographic names have posed challenges for Internet domain name policy makers since the earliest days of the Domain Name System (or 'DNS', as it is most commonly known). As the DNS develops with the addition of hundreds of new top-level domains and the challenges posed by geographic domains are addressed only on an ad hoc basis, DNS policy on these names reduces coherency, thus reducing confidence in the DNS and its controlling authority, the Internet Corporation for Assigned Names and Numbers (ICANN). The broad range of issues currently and foreseeably raised by the use of geographic names in the DNS means that all Internet stakeholders are affected, not simply those claiming rights or interests in such names. This article offers insight into why geographic domain names remain problematic more than two decades after these issues first arose, identifies trends in DNS policy respecting geographic names and highlights the impact on various Internet stakeholders of current policy and decisions.

Introduction

Geographic names have posed challenges for Internet domain name policy makers since the earliest days of the Domain Name System (or 'DNS', as it is most commonly known). As the DNS develops with the addition of hundreds of new top-level domains and the challenges posed by geographic domains are addressed only on an ad-hoc basis, DNS policy on these names reduces coherency, thus reducing confidence in the DNS and its controlling authority, the Internet Corporation for Assigned Names and Numbers (ICANN). The broad range of issues currently and foreseeably raised by the use of geographic names in the DNS means that all Internet stakeholders are affected, not simply those claiming rights or interests in such names. All domain name registrants must understand the implications of registering domain names incorporating geographic terms (for example, 'fordaustralia' or 'paris.cafe'). All new generic top-level domain operators ('gTLD operators') must ensure that their domain name registration policies satisfy ICANN requirements, which are increasingly influenced by government interests. Brand owners must be aware of the exemptions that new geographic gTLD operators seek from rights protection requirements. Governments

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

challenging geographic names' use must be aware of the legal basis, or lack thereof, for their claims to priority rights or interests in geographic names. This article offers insights into why geographic domain names remain problematic more than two decades after these issues first arose, identifies trends in DNS policy respecting geographic names and highlights the impact on various Internet stakeholders of current policy and decisions.

Why are geographic domain names problematic in the DNS?

In the early 1990s the DNS, which had been operational since 1984, experienced a major shift in focus with the transition of funding from the United States Department of Defense to the United States government's National Science Foundation. (NTIA 1998) Far from simply being a change in the United States government's financial ledger, with this shift the Internet transitioned from military project to public communications resource. The commercialisation of the Internet took another great leap as the twentieth century wound to a close with the incorporation of the Internet Corporation for Assigned Names and Numbers (ICANN), a California non-profit public benefit corporation, and its assumption of responsibility for the DNS by contract with the United States Department of Commerce. At that point, the total number of domain name registrations worldwide in the then only three publicly available gTLDs (.com, .net and .org) barely surpassed ten million. (ZookNIC 2008) Yet even in that relatively small Internet community, conflicts arose over geographic domain names.

One of the first items of business for the newly formed ICANN was developing a dispute resolution policy to resolve the increasing incidence of 'cybersquatting', the practice of registering a domain name that comprises or incorporates a term in which another party has legal rights. In leading ICANN's efforts to develop the dispute resolution policy that would become the Uniform Domain Name Dispute Resolution Policy (or 'UDRP', as it is now universally known), the World Intellectual Property Organization (WIPO) recommended that the policy apply to 'any dispute concerning the domain name arising out of the alleged violation of an intellectual property right.' (WIPO 1998) This recommendation came to life in the first ground that all UDRP claimants must demonstrate, namely, 'the registrant's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights'. (ICANN 1999)

This requirement operates to restrict government challenges where the geographic name in question is not protected by trade mark rights - a significant hurdle due to trade mark law's reluctance to protect a term that consumers may interpret as having multiple associations or meanings. (Forrest 2013a) As a result, complaints against geographic domain names registrations have notably succeeded 'in only a few exceptional cases'. (Bettinger 2005)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

Government influence on DNS policy-making, meanwhile, has increased with greater awareness of and participation in the ICANN policy development process through Governmental Advisory Committee (GAC) representatives. The GAC has progressively increased its demands in relation to geographic names, from 'interim ad hoc' measures to restrict 'the use of names of countries and distinct economies as recognised in international fora as second level domains in the .info TLD' in 2004 (GAC 2001) to preventing in 2012 applications for new gTLDs constituting country or territory names and requiring applicants of new gTLDs comprising other forms of geographic name to demonstrate the consent or non-objection of relevant governments or public authorities. (ICANN 2012a) The purportedly 'interim ad hoc' restriction on registering names of countries and territories now applies to all new gTLDs. (ICANN 2013a)

Geographic names remain problematic in the DNS as a result of this decidedly ad hoc approach to policy-making. While governments' interests in geographic names are not actionable under the UDRP (unless recognised through trade mark law), ICANN policy on top-level (.turkey) and second-level (nyc.restaurant) naming increasingly favours government interests over even third party legal rights. This creates significant uncertainty for the market, to the detriment of the DNS as a whole. Brand owners, commercial and non-commercial domain name registrants, new gTLD applicants and governments are particularly affected.

What is a 'geographic name' for DNS purposes?

One explanation for the ad hoc approach to policy-making with respect to geographic names is the difficulty of defining the term with any precision. Geographic names take many forms: just at the national level there are long-form ('United States of America'), short-form or common usage ('United States'), shorter colloquial names ('America'), acronyms ('US' and 'USA'), and others, along with their translations in other languages. At the sub-national or supra-national levels, further questions arise as to not only the form of the name but the proof of its existence. The gTLD Applicant Guidebook, the principal policy instrument to which all new gTLD applicants in 2012 were bound, incorporated a wide variety of concepts within 'country or territory names', which were excluded from the application program and defined as:

(i) An alpha-3 code listed in the ISO 3166-1 standard;

(ii) A long-form name listed in the ISO 3166-1 standard, or a translation of the long-form name in any language;

(iii) A short-form name listed in the ISO 3166-1 standard, or a translation of the short-form name in any language;

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

(iv) The short- or long-form name association with a code that has been designated as 'exceptionally reserved' by the ISO 3166 Maintenance Agency;

(v) A separable component of a country name designated on the 'Separable Country Names List,' (a list developed by ICANN and included as an Annex to the *gTLD Applicant Guidebook*) or a translation of a name appearing on the list, in any language;

(vi) A permutation or transposition of any of the names included in items (i) through (v)/ Permutations include removal of spaces, insertion of punctuation, and addition or removal of grammatical articles like 'the'. A transposition is considered a change in the sequence of the long or short-form name, for example, 'RepublicCzech' or 'IslandsCayman'.

(vii) A name by which a country is commonly known, as demonstrated by evidence that the country is recognized by that name by an intergovernmental or treaty organization.

Other 'geographic names' that required the demonstration of government support or non-objection were defined as follows:

> 1. An application for any string that is a representation, in any language, of the capital city name of any country or territory listed in the ISO 3166-1 standard.
>
> 2. An application for a city name, where the applicant declares that it intends to use the gTLD for purposes associated with the city name.
>
> 3. An application for any string that is an exact match of a sub-national place name, such as a county, province, or state, listed in the ISO 3166-2 standard.
>
> 4. An application for a string listed as a UNESCO region or appearing on the 'Composition of macro geographical (continental) regions, geographical sub-regions, and selected economic and other groupings' list.

In late 2013, a Study Group was formed within ICANN (specifically, the ccNSO, which deals with country code top-level domain administration) to identify current uses of country and territory names within the DNS. This group reported on various efforts in the Internet community prior to and including the current new top-level expansion policy set out in the gTLD Applicant Guidebook to develop a definitive list or definition of 'geographic name'. The volume and complexity of issues raised by such a task led to the recommendation of the establishment of a Working Group to investigate 'the feasibility of developing a consistent and uniform definitional framework' that would apply across ICANN DNS policy-making efforts. (ccNSO 2013) The definitions, agreed upon for current expansion purposes through the gTLD Applicant Guidebook, set an exceptionally broad precedent upon which to build future policy, capturing names of businesses (Virgin, Iceland), names of products, in particular food and beverage products associated with and protected by a geographical indication (Champagne, Parma), and terms with other, non-geographic meanings (Turkey/turkey). These definitions expand significantly upon the level of protection afforded country and territory names established with the launch of the .info TLD; the issues

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

discussed below suggest that further expansion is inevitable but puts ICANN policy in conflict with international law.

Issues for brand owners

ICANN's new gTLD policy framework is significant in many ways, not least its heightened mandatory mechanisms to protect trademark rights. In addition to implementing the UDRP and a new rapid-relief procedure, 'Uniform Rapid Suspension', all new gTLDs are required to launch with two targeted mechanisms in place: a 'sunrise' registration period, during which trademark holders have priority, and a 'Trademark Claims' period, during which notice of existing trade mark rights is provided to registrants and notice of matching registrations provided to rights holders. (Forrest 2013b) The ICANN-developed technical and operational requirements for implementing these mechanisms make explicit that '[r]egistration of domain names in the TLD during the Sunrise Period MUST be restricted to' verified trade marks; Registry Operators intending to deviate must 'apply to IANN for approval to conduct a registration program not otherwise permitted'. (ICANN 2013b) Reflecting the trend towards heightened recognition of government interests in geographic names, special consideration is given in these requirements to geographic new gTLDs, the applicants of which are encouraged to cooperate with intellectual property interests within ICANN (as represented through the Intellectual Property Constituency) to develop a list of names that may be prioritised over trademark rights during or before the sunrise period.

A wide range of exceptions are envisaged by the launch plans set out in geographic gTLD applications, such as reserving names related to government departments and initiatives, reserving geographically significant place and street names, prioritising registrants involved in the promotion of the new gTLD, and granting priority on the basis of an existing registration in an existing gTLD. Each of these proposals has a significant impact upon brand owners' rights to the extent that these overlap with or could be construed as a geographic name.

Two geographic brand owners' rights, and thus their future business models, in particular have become entangled in the convoluted ICANN geographic name policy web: Amazon and Patagonia. Each of these companies applied for a new gTLD comprised of their trading name, which each had registered and used as a trade mark in various jurisdictions around the world. Governmental Advisory Committee 'Early Warnings' were issued to each applicant articulating an expectation of peoples inhabiting geographic regions associated with these names to identify themselves by these names (GAC 2012a; GAC2012b). Patagonia Inc. withdrew its application soon after issuance of the 'Early Warning', (Patagonia) while Amazon, Inc. opted to defend its application, the progression of which depends upon a

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

decision by ICANN's Board of Directors to accept or reject GAC Advice recommending rejection. (GAC 2013a) The Board of Directors is not obliged to follow GAC advice, however, ICANN's Bylaws require at Article XI that this 'be duly taken into account', and further, 'it shall so inform the Committee and state the reasons why it decided not to follow that advice.' The GAC and Board are then obliged as a next step to 'find a mutually acceptable solution'. (ICANN 2012b)

The decision of the Board of Directors will be a watershed moment for the DNS and the worldwide Internet community. Rejection puts ICANN at odds with international law, as discussed further under the heading 'Issues for governments', below, in that it prioritises government interests in geographic names - which are not protected under international law - over trade mark rights - which are protected under international law. Such a decision will have the effect of preventing future non-government initiatives for any geographically associated top-level domain name; companies such as Patagonia and Amazon, whose names do not even fall within ICANN's carefully crafted, Internet community-agreed definition of 'geographic name', need not apply in future rounds. Approval, by contrast, puts ICANN at odds with the GAC and the now decade-long policy trend commenced with the launch of .info to restrict non-government use of geographic names.

Issues for domain name registrants

All new gTLD Registry Operators are required to restrict registration of country and territory names as domain names. This may significantly hinder new .brand TLDs, many of which plan to use the domain for internal purposes only, from creating a logical structure that follows the company's geographic footprint. For example, despite the fact that it would not be available to the general public and would be entirely unlikely to cause confusion, the domains canada.yahoo and china.toyota cannot be registered. User confusion is equally unlikely in the case of a generically termed TLD, for example australia.cars or japan.wedding, yet these registrations are likewise prohibited by the Registry Agreement into which all new gTLD Registry Operators must enter with ICANN. (ICANN 2013a)

GAC Advice to the ICANN Board extends beyond these express requirements to other categories of geographic name, recalling the breadth of the definitions set out in the gTLD Applicant Guidebook. In its most recent Communiqué following the 48th public ICANN meeting in Buenos Aires, Argentina, for example, the GAC advised that 'appropriate safeguards against possible abuse' are needed in the .wine and .vin proposed new gTLDs. (GAC 2013b) Such safeguards would presumably restrict registration of many, if not most, of the most desirable domain names in these TLDs, but agreement as to the scope and nature of

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

such safeguards is difficult if not impossible to reach. As the Communiqué appropriately notes:

> The current protections for geographical indications are the outcome of carefully balanced negotiations. Any changes to those protections are more appropriately negotiated among intellectual property experts in the World Intellectual Property Organization and the World Trade Organization. (GAC 2013b)

The clearly non-committal wording of the Communiqué exposes the lack of agreement on this matter amongst GAC members, but their willingness to observe international law is remarkable, particularly in the face of attacks which lack of support in international law against such strings as .amazon and .patagonia, as discussed in the next section.

Issues for governments and their citizens

Government motivation in restricting access to geographic names in the DNS is frequently stated as being the protection of Internet users against confusion; users are likely, it is argued, to wrongfully associate any geographic name with the named territory and therefore assume that a related government is responsible for, affiliated with or otherwise endorses the domain and any information accessible through it. Formal studies of this have yet to be mentioned in ICANN policy development processes to support such concerns.

Challenge processes were put into place in the gTLD Applicant Guidebook, including a mechanism whereby members of a community could object to a new gTLD application on the basis of a string's impact on community identity. Identity was key to standing on this objection ground, which was available only to '[e]stablished institutions associated with clearly delineated communities' with a strong association to the applied-for string. (ICANN 2012a) Further, objectors were required by the gTLD Applicant Guidebook to demonstrate 'substantial opposition' within the affected community. The evidentiary burden proved too great for this objection to be of significant use to communities that identify along geographic lines.

The second basis upon which governments call for restrictions on geographic names is claims to rights in such names, yet in 2001, the World Intellectual Property Organization ('WIPO') reported that the principal international treaty on the protection of intellectual property, the Agreement on Trade Related Aspects of Intellectual Property Rights (the 'TRIPS Agreement'), did not expressly recognize governments' rights in geographic names. (WIPO 1999) UDRP decisions involving government names reached over the years since are consistent with this position and indeed the requirements of UDRP itself offer no support for per se prioritisation of government interests. The experience of the registrant of andalucia.com, discussed in detail in '*andalucia.com Revisited*' in this issue, is instructive

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

for private parties facing government challenges. In more than a decade of UDRP decisions, panels have repeatedly rejected governments' claims, as advanced in a well-known case by the government of Puerto Rico in a dispute with a company called Virtual Countries, to "better rights or more legitimate interests" than private parties. (Puerto Rico Tourism Company v. Virtual Countries, Inc.) Such prioritisation is equally unsupported by the Uniform Rapid Suspension procedure and the sunrise registration period, both rights protection mechanisms that must be implemented in new gTLDs.

Governments' claims to rights in geographic names have subsequently been demonstrated to lack recognition under other bases of international law, including trade law, unfair competition, principles of sovereignty and human rights law. (Forrest 2013a) Challenges such as the GAC's Early Warning against Patagonia, Inc.'s application for .patagonia lack legal basis and can only diminish applicants' confidence in the TLD expansion process when existing legal rights are usurped by such legally immaterial facts as:

> PATAGONIA is the name of the south part of Argentina, comprising six provinces of the country. The region is globally known by its name, as a major tourist destination, it is an important region of Argentina because of the importance of mining, oil and agriculture industries and several other activities. It is the home of a vibrant community. (GAC 2012a)

Significant resources have now been expended by ICANN (thus depleting resources that would otherwise benefit the system as a whole), new gTLD applicants (who have agreed to participate on the basis of express requirements and guidelines as agreed by the Internet community) on challenges to new gTLD applications that do not fall within the definition of 'geographic name' set out in the community agreed policy framework to which all new gTLD applicants agreed to submit. While it may be politically convenient to the GAC to resort to the complexities of international legal treaty negotiation in relation to geographical indications' use in the DNS, reference to international law is not a convenience but a necessity.

Conclusion

Geographic naming issues in the DNS are no longer merely the concern of registrants of domain names such as andalucia.com. The expanding definition of 'geographic name' affects businesses, trade mark holders and Internet users.

References

Bettinger, Torsten (ed). 2005. Domain Name Law and Practice: An International Handbook. Oxford: Oxford University Press.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

ccNSO. 2013. 'ccNSO Study Group on the Use of Country and Territory Names: Final Report'. [Internet] Published 2 July 2013. Accessed 7 February 2014. Available from http://ccnso.icann.org/workinggroups/unct-final-02jul13-en.pdf.

Forrest, Heather. 2013a. Protection of Geographic Names in International Law and Domain Name System Policy. Alphen aan den Rijn, The Netherlands: Kluwer Law International.

Forrest, Heather. 2013b. 'Rights Protection Mechanisms in New gTLDs: The multi-stakeholder Internet governance model at work'. 63(2) Telecommunications Journal of Australia. http://doi.org/10.7790/tja.v63i3.427

Governmental Advisory Committee ('GAC'). 2001. 'Meeting 10 Communique: Montevideo 7-8 September 2001'. [Internet]. Accessed 7 February 2014. Available from https://gacweb.icann.org/display/gacweb/GAC+10+Meeting+Montevideo%2C+Uruguay+-+7-8+September+2001.

GAC. 2012a. 'GAC Early Warning: Submittal Patagonia-AR-78254'. Issued 20 November 2012. [Internet] Accessed 7 February 2014. Available from https://gacweb.icann.org/download/attachments/27131927/Patagonia-AR-78254.pdf?version=1&modificationDate=1353465809000&api=v2.

GAC. 2012b. 'GAC Early Warning: Submittal Amazon-BR-PE-58086. Issued 20 November 2012. [Internet] Accessed 7 February 2014. Available from https://gacweb.icann.org/download/attachments/27131927/Amazon-BR-PE-58086.pdf?version=1&modificationDate=1353452622000&api=v2.

GAC. 2013a. 'GAC Communiqué - Durban, South Africa'. [Internet]. Published 18 July 2013. Accessed 7 February 2014. Available from https://gacweb.icann.org/display/GACADV/2013-07-18-Obj-Amazon.

GAC. 2013b. 'GAC Communiqué - Buenos Aires, Argentina'. [Internet]. Published 20 November 2013. Accessed 7 February 2014. Available from: https://gacweb.icann.org/display/gacweb/Meeting+48%3A+Buenos+Aires%2C+Argentina.

NTIA. 1998. National Telecommunications and Information Administration of the United States Department of Commerce. 1998. 'Management of Internet Names and Addresses'. 63 Federal Register 31,741, 31,745 (10 June 1998) (White Paper). ('NTIA').

ICANN. 1999. Uniform Domain Name Dispute Resolution Policy. [Internet] As approved by ICANN on October 24, 1999. Accessed 7 February 2014. Available from http://www.icann.org/en/help/dndr/udrp/policy.

ICANN. 2012a. 'New gTLD Applicant Guidebook'. [Internet]. Released online 4 June 2012. Accessed 19 March 2013. Available from: http://newgtlds.icann.org/en/applicants/agb.

ICANN. 2012b. 'Bylaws for the Internet Corporation of Assigned Names and Numbers, a California Non-Profit Public Benefit Corporation, as last amended 20 December 2012'. [Internet]. Accessed 19 March 2013. Available from: http://www.icann.org/en/about/governance/bylaws#AnnexA.

ICANN. 2013a. 'Base Registry Agreement'. Updated 20 November 2013. Accessed 7 February 2014. Available from http://newgtlds.icann.org/en/applicants/agb/agreement-approved-20nov13-en.pdf.

ICANN. 2013b. 'Trademark Clearinghouse Rights Protection Mechanism Requirements'. [Internet]. Published 30 September 2013. Accessed 7 February 2014. Available from

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.22

http://newgtlds.icann.org/en/about/trademark-clearinghouse/rpm-requirements-30sep13-en.pdf.

Puerto Rico Tourism Company v. Virtual Countries, Inc., WIPO Case No. D2002-1129. Apr. 14, 2003. Available from http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-1129.html.

World Intellectual Property Organization (WIPO). 1998. 'Interim Report of the WIPO Internet Domain Name Process, The Management of Internet Names and Addresses: Intellectual Property Issues'. [Internet]. Published 23 December 1998. Accessed 7 February 2014. Available from http://www.wipo.int/amc/en/processes/process1/rfc/3/index.html.

WIPO. 1999. 'Final Report of the WIPO Internet Domain Name Process: The Management of Internet Names and Addresses: Intellectual Property Issues'. [Internet]. Published 30 April 1999. Accessed 19 March 2013. Available from http://www.wipo.int/amc/en/processes/process1/report/index.html.

ZookNIC. 2008. 'History of gTLD domain name growth'. Available from: http://www.zooknic.com/Domains/counts.html

Cite this article as: Forrest, Heather Ann. 2014. 'Geographic Internet domains: Challenges for the developing DNS'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 22.1-22.10. DOI: http://doi.org/10.7790/ajtde.v2n1.22. Available from: http://telsoc.org/journal

andalucia.com revisited:

Geographic names policy in the Domain Name System up to the mid-2000s

Chris Chaplow

The history of the landmark UDRP (Uniform Domain Name Dispute Resolution Policy) decision in 2006 on <andalucia.com>, related as a memoir by the key protagonist who developed and operated the <andalucia.com> website, shines light on an important legal precedent for the acceptance of non-governmental use of significant geographical names in the Internet Domain Name System.

The narrative is supplemented by an overview of the development of geographical names policy in the domain name system from its inception through the development of ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP), and how Panelists applied it to geographical name disputes including references to the first and second WIPO reports.

Andalucia.com: the beginning

On 17 April 1996 I telephoned U-Net to place an order for web hosting space and to register the domain name <andalucia.com>. The following day the domain was live and I uploaded pages to a new website that I simply called 'Information about Andalucia'. Andalucia is the name of the large region of southern Spain, extending from the Portuguese border in the west to the province of Almería in the east, where I had resided since 1991. It became the second largest of Spain's 17 Autonomous Regions in 1980, following the death of General Franco and the return to democracy with a constitutional monarchy in 1978. My interest was in documenting Andalucia in photographs, and providing information for tourists, since there was almost nothing available on the Internet at that time.

At this time the only generic top level domains (gTLDs) available for general registration were .com, .net and .org. The second level registration of a new domain name was achieved by emailing a template form to Internic. Payment was made several weeks later, on receipt by post of an invoice for US$100 covering two years' registration. There was no web registration nor any web 'whois' interfaces. Domain name allocation was on a first-come first-served basis. This was a simple IANA policy based on entitlement to register, created in

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

an earlier era when there were no registration fees and a technical community who only registered what they needed, no more. At this time there was no mindset to register for resale and profit. There were only a handful of reserved names, a first group reserved for technical reasons and a second group which US authorities judged to be obscene[1] (Forrest 2013: chapter 3).

The project continued to grow. I worked on website design work for clients during the week, while at weekends I travelled extensively around Andalucia collecting information and taking photographs. In January 1997 a man called Lou Dinella, of Bravo Tours in New Jersey, contacted me to ask the price for linking from <andalucia.com> to his website. The concept of selling advertising on the <andalucia.com> website was created.

In early 1997 I visited the offices of the 'Instituto de Formento de Andalucia', a part of the Department of Transport and Industry of the Junta de Andalucía (Regional Government). I formally applied for a grant to help build my tourist information website on the domain <andalucia.com>. I recall the gentleman showed very little interest in the project, saying it would never take off, and the grant was not approved.

The website became popular because we provided detailed, well-researched information written by professional magazine and guidebook journalists. We understood what tourists wanted to read. Numerous other websites began to link to <andalucia.com> for the useful information it provided. We took on our first employee, Mike Cartwright, in July 1998.

ICANN and WIPO

In June 1998 the US Government published its White Paper (NTIA 1998) which led to the creation of ICANN to manage the Internet's naming and addressing. It included in section 8:

> **The Trademark Dilemma.** When a trademark is used as a domain name without the trademark owner's consent, consumers may be misled about the source of the product or service offered on the Internet, and trademark owners may not be able to protect their rights without very expensive litigation.
>
> **Response:** The U.S. Government will seek international support to call upon the World Intellectual Property Organization (WIPO) to initiate a balanced and transparent process, which includes the participation of trademark holders and members of the Internet community who are not trademark holders, to (1) develop recommendations for a uniform approach to resolving trademark/domain name disputes involving cyberpiracy (as opposed to conflicts between trademark holders with legitimate competing rights).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

The following year WIPO published its "Final Report on the First WIPO Internet Domain Name Process" (WIPO 1999). Whilst it recognised the existence of the Domain Name Dispute Policy used by Network Solutions Inc. (NSI) (the sole registrar and registry of the .com, .net and .org gTLDs), this was overly mechanical and the immediate solution was to put a domain name on hold. A subsequent court order was required to make a transfer of ownership of the domain. WIPO recommended that 'ICANN should adopt a dispute-resolution policy under which a uniform administrative dispute-resolution procedure is made available for domain name disputes in all gTLDs.'

Geographical names were considered to be outside the scope of the report. "Other issues remain outstanding and require further reflection and consultation. Amongst these other issues are: the problem of bad faith, abusive domain name registrations that violate intellectual property rights other than trademarks or service marks, for example, geographical indications and personality rights" (WIPO 1999)

The ICANN Board accepted the WIPO report and requested that their Names Council produce a policy to deal with the issue. In October 1999 the ICANN Board approved the Uniform Domain Name Dispute Resolution Policy (UDRP), still hailed as one of ICANN's most successful policies (ICANN 1999). One month later WIPO was approved by ICANN as the first dispute provider and within days the first complaint, re <worldwrestlingfederation.com>[2], was received.

After five months WIPO had received about 550 complaints under the policy. Many included well known brands, such as <f1.com>, <easyjet.net>, <Telstra.org>, <banesto.net>, <dior.org>, <jpmorgan.org>, <tata.org>, <Microsoft.org>, <abta.net> and <niketown.com>. There were a few complaints that included a geographical element where the complainant held trademarks for products such as <timesofindia.com> and <raimat.com>[3] or real estate developments such as <ashburnvillage.com>[4]. There had been a handful of cases in French courts <santropez.com> and <laplagne.com> and German and Swiss courts respectively <Heidelberg.de>, <berner-oberland.ch> and <luzern.ch>, all resulting in transfer of ownership to the city authority or agency. There had been no complaints relating to geographical names brought under the UDRP thus far.

On June 28 2000, WIPO received a letter (Alston 2000) from the Government of Australia and 19 of WIPO's other member governments, seeking to initiate a Second WIPO Process to address certain intellectual property issues including geographical indications, geographical terms and geographical indications of source (e.g. for the Champagne region).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

Andalucia.com gains distinctiveness

In early 2000 a distinctive <andalucia.com> logo was designed by Joaquin Dominguez. The logo is reproduced here:

Figure 1. The logo for andalucia.com

By now the company had several employees, including a dedicated sales team, web designers and administration staff. In May 2000 we reached 20,000 unique visitors a week, reading 100,000 pages a week. This was the highest for any website about Spain.

Clearly our brand was gaining distinctiveness. We decided to register a trademark in Spain. On the 27 July 2000 we approached Ungria, the trademark agents in Madrid, about a Spanish trademark for the company.

On 1 August 2000 they gave us important advice that I still believe to be relevant today: *"Andalucia can never be monopolised by anybody as an exclusive title. Furthermore Spanish trade mark law actually expressly prohibits this"* but *"as a graphic Andalucia with the .com and the three @ inside a circle forms a distinctive unit and can be registered"*.

We instructed Ungria to proceed with registration. On 16 April 2001 came the news that our application had been 'suspended' because the Junta de Andalucia had objected on the grounds of similarity to the "JUNTA DE ANDALUCIA" trade mark (1,124,069 & 2,105,103) and the 'A ANDALUCIA' trade mark (1,641,600). Ungria presented our case to the Spanish Trademark Agency OPEM but it was rejected. On 18 April 2001 Ungria wrote to us suggesting we appeal as a different examiner might take a more reasonable view. However we decided not to pursue the matter due to additional costs.

The barcelona.com case

<Barcelona.com>[5] was registered in February 1996 and on 26 May 2000 WIPO received a complaint under the UDRP: the first UDRP geographical name dispute. The Barcelona city council did not have a descriptive trademark for the term 'Barcelona' in Spain (Spanish trademark law[6] prohibited registration of marks consisting exclusively of 'geographical origin') or elsewhere. However it did have various trademark registrations which included "one main element, namely the expression 'BARCELONA"".

Under Section 4(a) of the UDRP, a domain name registration is abusive on proof of the following three elements:

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

(i) the Registrant's domain name is identical or confusingly similar to a trademark or service mark in which the Complainant has rights;

(ii) the Registrant has no rights or legitimate interests in respect of the domain name; and

(iii) the Registrant's domain name has been registered and is being used in bad faith.

The Panel found that the Complainant did have trademark rights under UDRP section 4(a)(i) on the basis that the 'distinctive character' of the Complainant's mark was the name 'Barcelona'.

There was no website at the Barcelona.com address when the complaint was filed and the Panel did not accept the Respondent's evidence of planned website business activity as a legitimate interest under UDRP section 4(a)(ii).

In the third test in 4(a)(iii), the Panel's finding on bad faith usually follows the line of the first two and does not change the outcome itself. In this case the Panel concluded on a negative note, 'to put in doubt the existence of good faith at the time the Respondent obtained the registration of the domain name'.

All three elements being proved, the domain was transferred to the Complainant. (It was later returned through use of the different criteria of the United States Federal trade mark law, the Lanham Act,[7] which protected, the registrant, a USA company in the Fourth Circuit Court of Appeals.[8])

The second UDRP case was <stmoritz.com>[9] where the city did have 'St. Moritz' as a registered trademark in 27 countries and the panel did 'find that the Domain Name is identical to the trademark "St. Moritz" of the Complainant giving rights under UDRP section 4(a)(i)'

In this case the website owner did not submit a response to WIPO. The Panel looked at the website on the domain and reported that "Respondent provides informational services about the city of St. Moritz and about Switzerland." So they found it "does qualify as a bona fide activity" and that the "Respondent may have legitimate rights" under UDRP section 4(a)(i)'

Of the third UDRP element the Panel found that "the circumstances present do not indicate that the Respondent would have registered and is using the Domain Name in bad faith."

Only the first of the three elements being proved, the Complaint was denied.

During the 15 months following publication of the <Barcelona.com> and <stmoritz.com> case decisions, governments or their agencies brought 28 geographical term WIPO UDRP cases[10]. This number tailed off over the subsequent four years (9, 7, 7 and 1 from 2002 to 2005) as clear patterns emerged.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

In 2005 WIPO also published an overview which clarified the consensus view that "Some geographical terms however, can be protected under the UDRP, if the Complainant has shown that it has rights in the term and that the term is being used as a trademark. Normally this would require the registration of the geographical term as a trademark." and added "It is very difficult for the legal authority of a geographical area to show unregistered trademark rights in that geographical term on the basis of secondary meaning" (WIPO 2005).

In short, to be successful the Complainant needed an identical or very similar registered trademark, whereas the Respondent only needed a website with some information about the place.

The second WIPO report

Meanwhile the Second WIPO Internet Domain Name Process addressed the outstanding issues through a process of consultations and the result was a final report published on 3 September 2001. Section 6 covers the subject of geographical names; half of the section covers protection for geographical terms per se, as opposed to geographical indications in the source of goods and services.

The report acknowledged evidence of the misuse of geographical domain names, citing case examples where the website content "bears no relationship with the geographical indication" and where the registration was "with a view to preventing others from registering the same name". This report observed, after less than two years of UDRP cases, that they "do not necessarily stand for the proposition that the registration of a city name or the name of a region, as such, is to be deemed abusive" (WIPO 2001).

It presented an analysis of country names, and city names using a UNESCO World Heritage list, underlining two points that governments were fundamentally uncomfortable with:

i. The overall majority of country names . . . have been registered by persons or entities that are residing or located in a country that is different from the country whose name is the subject of registration.

ii. In almost all cases . . . the registrant is a private person or entity. Only rarely is it a public body or an entity officially recognised by the government of the country whose name has been registered.

The WIPO second report highlighted that there were "fundamental problems in endeavoring to apply the existing international legal framework to prevent the bad faith misuse of geographical indications in the Domain Name System (DNS)..... in respect of applicable law because of the different systems that are used, at the national level, to protect geographical

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

indications." It was suggested that "These problems of applicable law could be avoided if a multilaterally agreed list of geographical indications were to be established."

> *244. It is recommended that no modification be made to the UDRP, at this stage, to permit complaints to be made concerning the registration and use of domain names in violation of the prohibition against false indications of source or the rules relating to the protection of geographical indications.*

As Governments did not support this recommendation, picking up on WIPO's need for a new law to enable progress to be made, and the uncomfortable analysis that the Paris Convention[11] did not expressly prohibit country names as trademarks, the Member States subjected WIPO's second report to WIPO's Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indicators. Special sessions were held in December 2001 and May 2002 and its recommendations were transmitted by letter to ICANN (Gurry 2003):

> *Country Names* It was recommended that this protection should be implemented through an amendment of the UDRP and should apply to all future registrations of domain names in the gTLDs.[12]

On 13 March 2006, ICANN informed governments that it had not been possible to achieve consensus among ICANN's constituencies concerning the recommendations of the Second WIPO Internet Domain Name Process (ICANN 2006). The UDRP remained unmodified in its original and basic form – as discussed in detail in (Forrest 2013: chapter 3).

The andalucia.com case

Meanwhile, back in Andalucia, completely unaware of what had been happening at WIPO and ICANN, I continued to build the andalucia.com website business, and in April 2006 we celebrated our 10th anniversary. By this time the website was receiving approximately 300,000 unique visitors a month viewing around 1.6 million pages. The company behind it had also grown to employ 12 full time and two part-time members of staff and was supported by five journalists. We had moved into new offices in Estepona in the province of Málaga.

Thus it was with great surprise that on the evening of Wednesday 14 June 2006 I received an email about a WIPO complaint, on behalf of the Tourist Board of the regional government, the Junta de Andalucia.

After some intensive study of the ICANN and WIPO websites, we started to compile a shortlist of possible lawyers to act on our behalf. We sent out emails on the following Sunday and were impressed to receive a few replies the same day. We set up a call with Matthew Harris of Norton Rose in London (now with Waterfront Solicitors) on the Monday and engaged him later that day. Matthew requested support from Spanish lawyers. Since it

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

proved to be difficult to find an Intellectual Property lawyer in Andalucia willing to take on the case, I travelled to Madrid to meet and engage a leading firm who insisted that their name not be associated with the case.

Trademark Rights

The UDRP Panel reported that[13] the Complainant (Tourist Board of Andalucia) owned many registered trademarks which included the word "Andalucía" as part of a number of words. The case focused on a trademark consisting of the stylised word ANDALUCIA below a badge-shaped logo comprising a stylised letter "A" in white on a part blue, yellow and green background, registered on 10 June 1991 as follows.

Figure 2. The Andalucia trademark

The Complainant clearly had rights in the trademark as registered. But does such a "'word and design' registration give the Complainant rights over the geographical indication ANDALUCIA?

We, as the Respondent, argued[14] that the mark and the word were not identical; "even if one discards the graphical elements of the mark, what is left is not the word "Andalucia" but the phrase "A Andalucia" which translates roughly in English as "To Andalucia". (Indeed, the intent of the trademark designer appears to be a moderately clever play upon the fact that the word for "to" in Spanish is also the first letter of the word "Andalucia".)

The Panel reviewed a number of cases that the Complainant referred to as supportive but found that none of these cases were determinative.

The Panel found that the Complainant did have trademark rights under UDRP section 4(a)(i) and explained the rationale.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

> "Although the Panel believes it is a close call, the Panel concludes that at least as to the A ANDALUCIA word and design mark, ANDALUCIA is the dominant feature in the mark. Therefore, the Panel finds that the domain name at issue is confusingly similar to a mark in which Complainant has rights."

Legitimate interests

There had been a website about Andalucia on the domain for the entire time since it had been registered. In view of all previous case decisions I still wonder how the Complainant could possibly have made a valid case for lack of legitimate interests.

Here the Complainant focused on its trademark, again stating that we had no rights or legitimate interests because the "Respondent knew or should have known of Complainant's registered marks."

The Respondent also highlighted its own trademark, but the fundamental right and legitimate interests were that it has expended resources over the years in the development of the informational website about Andalucia. Additionally the Complainant, knowing of Respondent's website, failed to object for at least five years to Respondent's use of the domain name.

Predictably the panel found legitimate interest under UDRP section 4(a)(ii).

> "Respondent is using a geographical indication to describe his product/business or to profit from the geographical sense of the word without intending to take advantage of Complainant's rights in that word, then the Respondent has a legitimate interest in respect of the domain name."

Bad faith

The Complaint contended that the "Respondent has registered and is using the domain name at issue in bad faith since it has no licence or other permission of the mark owner to use the mark in a domain name. "

The Respondent contended that it "did not register the domain name at issue in bad faith, since at the time it registered the domain name it did not know of Complainant's mark" and it did not "use the domain name in bad faith, since it had no idea that Complainant objected to its use of the domain name at issue until it received a copy of the complaint in this matter."

The Complainant also made some startling claims for a Destination Marketing Organization (DMO) about the alleged concentration of information on the website about the upmarket resort town of Marbella whilst "virtually ignoring all other provinces or regions of Andalucia

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

and only mentioning for sales purposes some of the distinctive items of this internationally famous region such as olive oil and serrano ham, and basically treating the most symbolic aspects of Spanish culture such as flamenco and mozarabic art with little respect." In the response we had a duty to prove these allegations to be false by detailing relevant website pages.

The Panel found that Complainant had failed to establish any of the bad faith circumstances that the domain name was registered or being used in bad faith.

Accordingly, the Panel found that the Complainant had failed to satisfy its burden of proof and the complaint was denied.

Reverse Domain Hijacking

The Respondent requested a finding of Reverse Domain Name Hijacking, alleging that the complaint in this matter was filed in bad faith. Despite the Respondent filing ten detailed points to support this claim the Panel did not find against the Complainant, nor give any detailed rationale to explain their decision.

Conclusion: the legacy

> "Landmark decisions such as <newzealand.com> and <andalucia.com> set a precedent of recognising non-governmental interests in geographical names' use in the Domain Name System. Decisions such as <brisbane.com> and <rouen.net> and <rouen.com> have unequivocally elucidated that government use of a geographical name is not equivalent to trademark rights, the only form of right protected by DNS rights protection policy." (Forrest 2014).

Andalucia.com was also an unusual case. It was about control of a domain name over a leading website that had built up substantial traffic and influence over ten years. The timeline for this case is shown in Figure 3.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

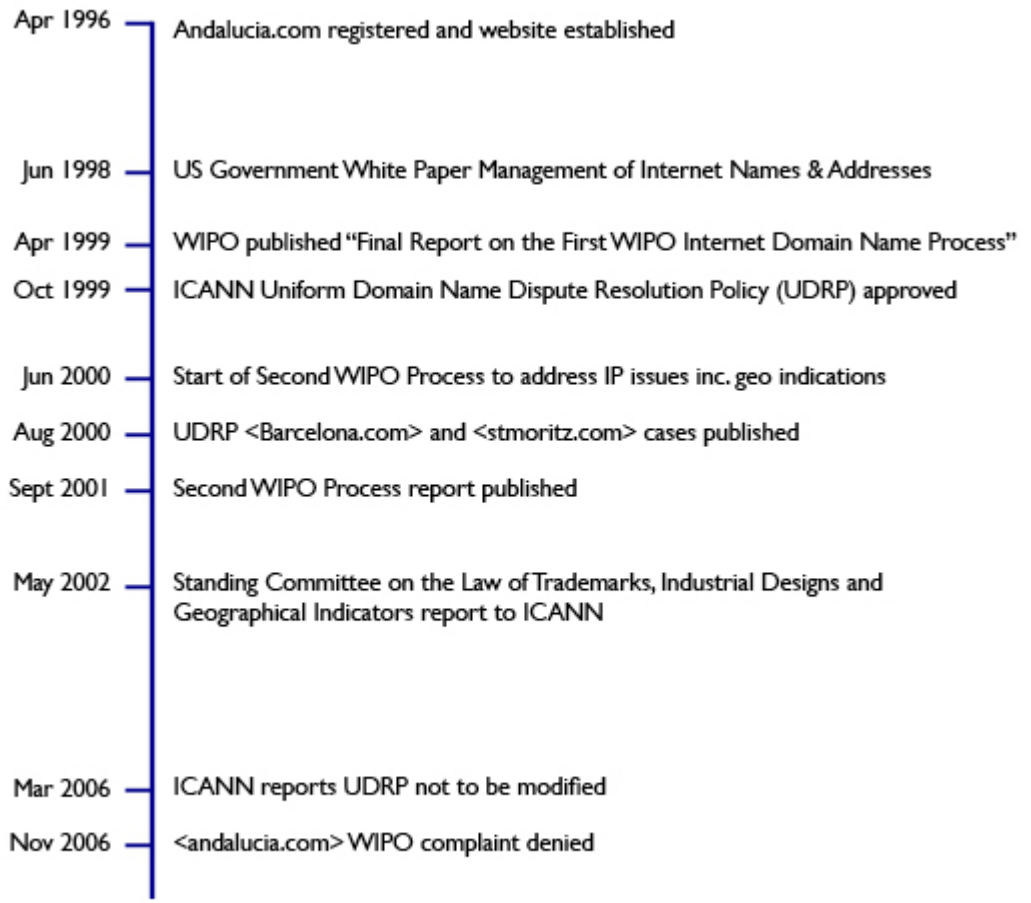

Figure 3. Timeline for the andalucia.com WIPO/UDRP case.

The UDRP panel comprised three panelists who were very experienced in the field, and whose landmark decision finally defined the UDRP landscape in respect to geographical names. In the eight years since there have only been three cases brought to WIPO.

At this time the applicable law has not been changed as requested by the second WIPO report, nor has the UDRP been revised. Governments still do not find this a very satisfactory situation and have channeled their concerns through ICANN's Government Advisory Committee (GAC) (Forrest 2014).

Looking ahead: 900 gTLDs

Shortly after the <andalucia.com> case the new generic Top Level Domain (gTLD) program was given approved by ICANN board and in early 2014 the first of the 900 new open domains (for example: .guru, .bike .photography, .estate) are accepting general registrations at the second level. Will this lead to another wave of UDRP cases in geographical names?

On one hand the Governments' Destination Marketing Organisations (DMOs), who brought most of the past UDRP complaints, have had six years to ensure their trademarks are in

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

place. On the other hand, the website owners have also had this time to understand the need to feature information about the destination on their domains. Happily, publishing this information is also perfectly in line with the mission of the DMOs.

The distinctive green <andalucia.com> brand website continues to grow at an ever increasing rate, and we remain guardians of a nine character string in the .com zone of the DNS of the Internet.

References

Alston, Senator Richard. 2000. Letter from Richard Alston, Minister for Communications, Information Technology and the Arts, Government of Australia to Dr Kamil Idris, Director General, World Intellectual Property Organization.

http://www.wipo.int/amc/en/processes/process2/rfc/letter2.html

Forrest, Heather. 2013. *Protection of Geographic Names in International Law and Domain Name System Policy*. Alphen aan den Rijn, The Netherlands: Kluwer Law International.

Forrest, Heather. 2014.'Geographic Internet domains -- Issues in the developing DNS'. *Australian Journal of Telecommunication and the Digital Economy*, 2(1), March 2014.

Gurry, Francis. 2003. Letter from Francis Gurry, Assistant Director General, Legal Counsel, WIPO to Dr. Vinton G. Cerf, Chairman, ICANN (February 21, 2003). At http://www.wipo.int/export/sites/www/amc/en/docs/wipo.doc

ICANN. 1999. *Uniform Domain Name Dispute Resolution Policy*. [Internet] As approved by ICANN on October 24, 1999. Accessed 7 February 2014. Available from http://www.icann.org/en/help/dndr/udrp/policy.

ICANN. 2006. Letter from Dr Paul Twomey, President and CEO, ICANN to Mohamed Sharil Tarmizi, Senior Advisor, Office of the Chair, Government Advisory Committee of ICANN, 13th March 2006. Available from http://www.icann.org/en/news/correspondence/twomey-to-tarmizi-13mar06-en.pd

NTIA 1998. Management of Internet Names and Addresses. National Telecommunications and Information Administration, UNITED STATES DEPARTMENT OF COMMERCE. Available from: http://www.icann.org/en/about/agreements/white-paper

WIPO (World Intellectual Property Organization). 1998. 'Interim Report of the WIPO Internet Domain Name Process, 'The Management of Internet Names and Addresses:

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.23

Intellectual Property Issues'. [Internet]. Published 23 December 1998. Accessed 7 February 2014. Available from: http://www.wipo.int/amc/en/processes/process1/rfc/3/index.html

WIPO (World Intellectual Property Organization). 1999 The Management of Internet Names and Addresses: Intellectual Property Issues. Final Report of the WIPO Internet Domain Name Process April 30, 1999. Available from: http://www.wipo.int/export/sites/www/amc/en/docs/report-final1.pdf

WIPO. 2001. Second WIPO Internet Domain Name Process: The Recognition of Rights and the use of Names in the Internet Domain Name System. WIPO September 3, 2001. Available at: http://www.wipo.int/amc/en/processes/process2/report/html/report.html

WIPO. 2005. Overview of WIPO Panel Views on Selected UDRP Questions, Original Edition (2005) Available from: http://www.wipo.int/amc/en/domains/search/oldoverview/

Notes

[1] These were the thirteen words forbidden on US television.

[2] World Wrestling Federation Entertainment, Inc. v. Michael Bosman <worldwrestlingfederation.com> WIPO Case No. D1999-0001 (18-01-2000) http://www.wipo.int/amc/en/domains/decisions/html/1999/d1999-0001.html

[3] Raimat, S.A. v. Antonio Casals <raimat.com> WIPO Case No. D2000-0143 (02-05-2000) http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0143.html

[4] Ashburn Village Development Corporation & Bondy Way Development Corporation v. Re/Max Premier WIPO Case No. D2000-0322 20-06-2000 http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0322.html

[5] *Excelentísimo Ayuntamiento de Barcelona v. Barcelona.com Inc.* WIPO Case No. D2000-0505 (Aug. 4, 2000), http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0505.html (last visited Jan. 10, 2014).

[6] Spanish Trademark Law of 1988, Art. 11(1)(c)

[7] Lanham Act §§ 32, 45, as amended, 15 U.S.C.A. §§ 1114, 1127.

[8] *Barcelona.com, Inc. v Excelentísimo Ayuntamiento de Barcelona*, 330 F.3d 617 (4th Cir, 2003).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.23

[9] Kur- und Verkehrsverein St. Moritz v. StMoritz.com WIPO Case No. D2000-00617 August 17, 2000 http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0617.html

[10] Index of WIPO UDRP Panel decisions" Category II.A.1.k.(ii) Geographical Terms http://www.wipo.int/amc/en/domains/search/legalindex.jsp?id=11250.11280

[11] Paris Convention for the Protection of Industrial Property. March 20, 1883 and revised and amended to September 28, 1979 http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

[12] The decision on the protection of country names was supported by all Member States of WIPO, with the exception of Australia, Canada and the United States of America, which dissociated themselves from the decision. Japan also expressed certain reservations, which are recorded in the text of the decision

[13] Junta de Andalucia Consejería de Turismo, Comercio y Deporte, Turismo Andaluz, S.A. v. Andalucia.Com Limited, WIPO Case No. D2006-0749 (Oct. 13, 2006) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0749.html

[14] Response in WIPO Case number D2006-0749. (Unpublished)

Cite this article as: Chaplow, Chris. 2014. 'andalucia.com revisited: Geographic names policy in the Domain Name System up to the mid-2000s'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 23.1-23.14. DOI: http://doi.org/10.7790/ajtde.v2n1.23. Available from: http://telsoc.org/journal

Geographic names and domain names

David Lindsay
Monash University

Review of Heather Ann Forrest, *Protection of Geographic Names in International Law and Domain Name System Policy* (2013, Wolters Kluwer) 339 pages including bibliography, tables and diagrams.

At the heart of many of the legal problems raised by the Internet is the fundamental tension between law (and legal rights), which are for the most part local, and the Internet, which transgresses legal borders. In many respects, the Domain Name System (DNS), which uses words (in which there may be legal rights) as part of a global addressing system, has been a laboratory for working through conflicts between local laws and global technologies. The conflicts are nowhere more apparent than in issues relating to the protection of geographic names – which are quintessentially connected to locations in the physical world – in the DNS. The rights of public authorities, including governments, over geographical names, including country names, was an important issue in ICANN's fraught New gTLD Program, which has opened up the DNS to a massive number of gTLDs. This book, which is the first major academic study of the legal protection of geographic names in the DNS, admirably fills a glaring gap in the scholarly literature, and provides a significant legal and historical knowledge base for the development and application of policy in this area.

ICANN's New gTLD Program, which may see the addition of over 1,400 TLDs (Top-Level Domains) to the DNS, provides the current focus for policy debates regarding geographical names, especially given that there were 66 applications for what are known as GeoTLDs as part of the program. These applications include applications for .tokyo and .berlin, which have already been delegated, as well as applications for .sydney, .melbourne and .nyc. As the author of the book, Heather Forrest, explains in the Introduction, the New gTLD Program was an opportunity for ICANN to clarify policy on a range of persistent issues, including the treatment of geographic names. After a comprehensive analysis of the relevant legal principles, however, by the end of the book the author concludes that ICANN's policy on the protection of geographic names has been based on inadequate assumptions about the law, and especially about the rights of States over geographic names under international law. Sadly, a lack of precise and accurate analysis of legal issues, including issues relating to legal

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.29

process, sometimes seems to characterise developments led by technologists, including gTLD policy-making. The publication of this highly-accessible book, based on the author's Ph.D. thesis, means that ignorance of the law in this area should no longer be an excuse.

The book has three parts.

Part I, consisting of chapters 1 and 2, provides the building blocks for the subsequent parts by introducing the problems relating to rights in geographical names in the DNS, and explaining the DNS and its development. In chapter 1, Forrest sets out the context of the research problems addressed by the book by explaining why DNS disputes, to date, have focused on trademark rights in second and lower level domain names, but that the New gTLD Program has seen a shift in focus to rights in names in gTLDs. In the final version of the *gTLD Applicant Guidebook* (Version 2012-06-04), which sets out the rules for the New gTLD Program, there are two approaches to dealing with geographical names:

- Country or territory names are completely reserved from registration as new gTLDs; and
- Other geographic names – specifically including capital cities, cities, sub-national place names (county, province or state) and geographical indications (which are names that identify a product as originating from a geographic location) – can only be registered with the support or non-objection of relevant governments or public authorities.

As Forrest explains, the *Guidebook* simply assumed that governments (or other public authorities) have exclusive or superior rights in these geographic names, without any analysis of the position under international law. In chapter 2, the book explains the evolution of the DNS, including the expansion of gTLDs, leading up to the decision to open up gTLDs with the New gTLD Program.

Part II of the book, which consists of chapters 3 and 4, explains the policy and legal frameworks for protecting rights in geographical names in the DNS (chapter 3) and under international law (chapter 4). Chapter 3 first sets the scene by explaining the development of systems for recognising trademark rights in domain names, including the Uniform Domain Name Dispute Resolution Policy (UDRP). As Forrest explains, rights in names may be protected either *ex ante* (such as by reserving names from use in the DNS) or *ex post* (by systems, such as the UDRP, which provide mechanisms for challenging registered domain names). The chapter includes an explanation of the controversy involving whether or not geographical names should be reserved from registration, which applies to second and lower level domain name registrations in new gTLDs pursuant to Specification 5 of ICANN's Registry Agreement. The problem with geographic names, as opposed to trademark law

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.29

more generally, is that there is an absence of consistency between legal regimes in the protection accorded geographical names, including a lack of consistency in how geographical names are treated under national trademark laws. This explains why *ex post* dispute resolution mechanisms, such as the UDRP, have been confined to trademark rights, where they have been generally effective, but not extended to protect other rights, such as rights in geographical names.

Chapter 4 is an exposition of the legal framework for protecting rights in names under international law. It explains the sources of international law, the general principles of international law, and the growing role of non-state actors, including ICANN, in the developing international legal framework. As Forrest points out, an understanding of international law is essential to understanding the protection of rights in new gTLDs as the ICANN board adopted a recommendation that rights in strings must not infringe existing rights recognised under international law.

Part III of the book, consisting of chapters 5 to 9, explains and analyses the protection of geographic names under international law, with a view to evaluating the policies on the protection of geographic names in the DNS adopted and applied by ICANN. Chapter 5 explains the protection of geographic names under intellectual property law, especially trademark law. As the chapter explains, there are considerable difficulties in protecting geographic names as trademarks as such terms are generic or descriptive, not distinctive of a particular trader or business. With the exception of the special category of geographical indications, there are significant limits on the extent to which geographical names can be protected under intellectual property laws.

Chapter 6 is an exposition of rights in geographic names under international law, including whether States can prevent the registration of geographic names as trademarks and whether governments have inherent rights over country names as an incident of sovereignty. First, while Article 6*ter* of the Paris Convention on industrial property prohibits registration as a trademark of emblems of national significance, such as national flags, as Forrest explains, the prevailing view is that this does not prevent the registration of country names as trademarks. Second, the chapter examines the rights of States over country names as an incident of the principle of sovereignty, including analysis of a right to select a country name, a right to prevent the use of the same or similar name by other States, and a right to be referred to by a chosen name. As Forrest effectively points out, the position is extraordinarily complex, with considerable legal uncertainty. While sovereignty does not require a State to select and use a name, States have authority to do so if they so choose, and to control the use of that name within their sovereign territory. As a matter of international law, however, rights over country names are clearly not absolute. As is apparent from the complex dispute

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.29

between Greece and the Former Yugoslav Republic of Macedonia (FYROM), a State's rights over a country name are not absolute but may be limited by obligations not to encroach on another State's sovereignty. There are, however, no clear legal rules for resolving one State's objections to the use of a country name by another State. Finally, although there is obviously a uniform international practice of referring to States by name, this is not based on clearly identifiable legal principles but rather on good international relations. Accordingly, there are no clear bases under international law for States to claim exclusive rights over geographic names, including over country names.

Chapter 7 deals with the protection of geographical indications, which are names used to denote the geographic origins of products, such as wines and spirits. The chapter examines the multiple legal frameworks applying to geographical indications, includng the TRIPS Agreement, which includes an obligation on member states to prevent the importation of goods that directly or indirectly use false geographic indications. The chapter concludes that the international protection of geographic indications, in the absence of trademark protection, has limited scope to prevent the use of a geographic name as a gTLD, as the protection relates to the use of names in association with goods, whereas TLDs are a service (for the registration of domain names under the TLD) with no direct connection to goods.

Chapter 8 considers the protection of geographic names under unfair competition laws, which essentially protects commercial names against misleading or deceptive business practices. This can include false representations of the source of a good or service. The chapter points out that there are serious difficulties in applying unfair competition law to gTLDs, including problems with categorising a potential registrant of a gTLD as a 'competitor' of a government or public authority associated with a geographic name. The analysis leads to the conclusion that the relevant articles of the Paris Convention (Arts. 10 and 10*bis)* do not require member States to prohibit the unauthorised registration of geographic names or geographical indications as gTLDs.

The final substantive chapter, Chapter 9, examines international human rights law, including rights to national identity, freedom of expression or cultural rights, as a potential basis for rights in geographic names. Acknowledging that there are links between human rights and geographic self-identification, the chapter concludes that the human rights to freedom of expression and to culture require recognition of a person's right to use a geographic name. This leads Forrest to the conclusion that the assertion by governments of exclusive rights over geographic names, including country names, in the DNS may be in breach of the fundamental human rights to freedom of expression and to culture.

As Forrest points out in her concluding chapter, which summarises the arguments set out in the book, DNS policy-making should be based on an accurate analysis of the legal protection

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.29

of rights in names, and not merely assumptions. On the basis of the analysis of international law presented in the book, Forrest concludes that there is no compelling foundation, as a matter of international law, for States to assert exclusive rights over geographic names, including country names. In fact, insofar as it is possible to reach conclusions on the application of international law to the DNS, international human rights law (which protects individuals and not States) suggest that assertions of exclusivity by governments may be in breach of human rights. The uncertain legal basis for ICANN's policies of restricting the registration of geographic names as gTLDs lead Forrest to predict that there may be greater attempts to protect geographic names as trademarks under domestic intellectual property laws, such as has been pioneered in Switzerland.

The lack of academic attention given to the complex legal issues relating to domain name law and policy is an ongoing source of surprise, especially given the potential for the DNS to raise novel and highly significant legal issues. One possible explanation for the relative scarcity of authoritative research in the area is the high barriers to entry, arising from the dense thickets of technical and bureaucratic jargon that characterises DNS policy-making. Despite the unavoidable use of acronyms, this book is very clearly written, providing accessible introductions to complex legal issues. The author, who is a lecturer at the Australian Catholic University, displays a rare combination of skill and rigour in collecting and synthesising a wealth of source material, both technical and legal.

The central arguments, some of which are substantially original, are clearly presented, with helpful summaries at the end of each substantive chapter. This is an admirable achievement in an area that is as replete with inconsistencies and ambiguities, and subject to such diverse legal regimes, as the protection of geographic names under international law. By clearly elucidating legal issues that have apparently been overlooked by ICANN in developing its New gTLD Program, including the suggestive analysis of the implications of international human rights law for rights in geographic names, the book performs an important public service. The book, moreover, advances legal understanding of both private and public legal rights in names by means of a detailed case study of the regimes that apply to the protection of geographic names in the DNS.

Finally, the book highlights the importance of independent scrutiny of claims that are made by governments – in this case, the claims to exclusivity over geographic names by ICANN's Governmental Advisory Committee (GAC) – which all too often fail to withstand sustained critical analysis. Although it is understandable that there will be some lapses in an endeavour as complex and demanding as ICANN's New gTLD Program, the fragility of the international DNS governance arrangements require continual vigilance, especially in scutinising the claims made by powerful stakeholders, including those represented in the GAC. If

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.29

appropriate internal safeguards are not applied, the ICANN multi-stakeholder model will continue to be threatened, including by competing models that may potentially be more centralised and less consultative.

Cite this article as: Lindsay, David. 2014. 'Geographic Names and Domain Names'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 29.1-29.6. DOI: http://doi.org/10.7790/ajtde.v2n1.29. Available from: http://telsoc.org/journal

Building a digital society:
Questions for communication researchers

Catherine Middleton
Ryerson University

This paper outlines three areas in which communication researchers can offer insights on the ongoing development of a digital society: infrastructure development, the role of mobile connectivity, and the need for better data through which to understand access to, and engagement in, digital society. The paper offers a discussion of digital society, then outlines a variety of research questions that can be explored to help shape digital society in citizen-centric ways. It concludes by noting the value of research as a means of introducing alternative perspectives to discourses about digital society.

Some Context

More than 130 countries are now recognised as having a digital strategy (Cisco and International Telecommunication Union 2013). The scope of such strategies varies widely, ranging from specific short-term programs for investing in broadband infrastructure, like Canada's 2009-2012 Broadband Canada program (Industry Canada 2009), to long-term comprehensive visions for economic transformation through widespread adoption of information and communication infrastructure, as in Singapore where the iN2015 vision (Infocomm Development Authority of Singapore 2010) is supported with government investment in a next generation broadband network (Infocomm Development Authority of Singapore 2013) and initiatives to develop information and communication technology (ICT) skills across the economy.i What is common across strategies is a commitment to advance availability and uptake of digital technologies to enable participation in a digital society.

Governments are also undertaking specific initiatives to transform service delivery. In the United Kingdom, the 'digital by default' approach will deliver "digital services which are so straightforward and convenient that all those who can use digital services will choose to do so, while those who can't are not excluded" (Cabinet Office 2012, p. 5). In the United States, the digital government strategy aims to enable Americans "to access high-quality digital government information and services anywhere, anytime, on any device" (US Department of State 2012, p. 2).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

Australia's National Digital Economy Strategy notes "In 2013, the use of online services by Australians covers almost every aspect of daily life, from checking tomorrow's weather forecast to preparing a meal, paying bills, arranging a holiday or accessing education or health services from remote locations. Almost every aspect of life can be enhanced through some form of online service delivery. New ideas that apply digital technology to everyday situations emerge almost daily" (Australian Government 2013, p. viii). While the future of this specific digital economy strategy is uncertain following a change of government, there is no doubt that throughout the developed world[ii] online services will be central to the ways that people interact and engage with community, business and government in the future.

This move to the online economy offers many potential benefits, including development of more innovative services, more efficient and cost effective service provision, and improved convenience. A shift online is not limited to economic activities – increasingly social engagement and community interaction also take place online, for example through email, social networking platforms (to share messages, exchange photos) and online chats (video and text). However, as moving to a digital environment requires use of access technology (typically an Internet connection, accessible through a computer, tablet or mobile phone) and sufficient literacy and confidence to negotiate the online world, there are concerns that this digital transformation may disenfranchise citizens who do not have the capacity for online access.

While governments often frame their efforts in facilitating and encouraging the development of the digital ecosystem as digital *economy* initiatives, from a citizen perspective, it is a digital *society* that is of concern. Digital society is being shaped by governments, industry, civil society organisations and individuals, each with somewhat different (and sometimes conflicting) interests and priorities. As the contours of digital society are negotiated among stakeholders, there is a role for communication researchers to investigate and articulate citizens' technological and literacy needs, and to bring these needs to the attention of policy makers, regulators, and infrastructure and service providers.[iii] The sections below discuss some challenges in connecting to digital networks, identify opportunities for researchers to advance understandings of the infrastructure needs of citizens, and make the case for ongoing research to assess citizens' capacities to engage with society through digital means.

Access to Fixed Line Communications Infrastructure

As digital platforms become the default for service delivery and communication, there is a need to re-examine the characteristics of broadband networks that provide connectivity to digital services, in order to determine what is required for full participation in the digital society and consider how these requirements can be met. Similar to the emergence of other

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

large scale infrastructures (Jackson et al. 2007), broadband networks that provide Internet access have been developed by multiple players, using a variety of technologies, resulting in inconsistent user experiences. When commercial broadband services first became available to households in the late 1990s, Internet access was not essential to daily life, and Internet services were deployed on a 'best effort' basis. This best effort model still applies to much Internet traffic, meaning that mechanisms are not deployed to guarantee the quality of service of particular transmissions across the Internet, thereby compromising reliability for certain applications and services. Further, as different types of networks have different capacities, there is a need to either design digital services to the lowest common denominator (for instance recognising that many Internet connections have very low capacity to upload data) or accept that those with limited capacity connections will be disadvantaged when services are designed to make effective use of the most advanced connections.

Governments often view the provision of digital connectivity as an exercise in improving the availability of high speed Internet services, and it is common for national broadband plans to define broadband in terms of download speeds only. In failing to recognise broadband connectivity as an enabler of services beyond Internet access and by not establishing requirements for upload capacity, quality of service, and reliability that allow for delivery of a broader range of services, the power of broadband networks as enabling infrastructure is constrained. It is certainly possible to deliver good quality services over the Internet, but models that develop broadband networks to provide uniform, universal connectivity across a population, support a multitude of service providers and allow for service quality guarantees offer a much stronger platform for innovation. However, as evidenced by the many challenges in building such a national broadband infrastructure in Australia, there is much to be learned about how to develop a compelling business case for such an approach, to convince the public of its value, and to manage the complexities of building broadband infrastructure on a national scale.

Much broadband infrastructure has been developed and is controlled by the private sector. While private ownership of infrastructure is not inherently bad, there are times when Internet service providers' commercial practices may constrain individuals' abilities to use their Internet services in ways that they want. As the Internet becomes more essential to everyday life, constraints in its use become more problematic, especially as individuals often have limited choice in service providers. It is important to understand the impacts of these constraints (examples of which are noted below), for those developing digital services, and for everyone using the Internet in their daily activities.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

If the Internet is indeed an essential infrastructure, should principles of neutrality and non-discrimination apply to services and content available over the Internet? The principle of network neutrality is important in ensuring that Internet subscribers can access content from any source without the need for content providers to negotiate preferential treatment to ensure their content is available. In other words, network neutrality requires that Internet service providers (ISPs) allow traffic to flow over their networks without unreasonable discrimination as to its source, making it possible for anyone to communicate with or deliver services to anyone else. At the time of writing, network neutrality rules are under review in the US,[iv] and the CRTC (Canada's telecommunications and broadcasting regulator) is investigating a complaint that Canadian mobile ISPs are offering preferential access to their own mobile TV offerings, and disadvantaging their customers when they access competing video services.[v]

Another concern for Internet users arises when a service provider attempts to influence the information content provided to its customers, and to use customer information in ways that violate their privacy rights. A recent case is that of Bell Canada's "Relevant Ads" program, implemented in late 2013 for its mobile Internet subscribers and to be extended to fixed broadband customers at a later date. The program was implemented on an opt-out basis, and allows Bell to use data about customers' online browsing, location, television viewing and phone calling patterns to provide 'more relevant' advertising to its customers. However, as an Internet service provider, there is an expectation that customers have simply signed up for an Internet service, allowing them to select the content and services they choose, without any additional content (relevant or not) being imposed upon them by the service provider.

A formal complaint to the CRTC by the Public Interest Advocacy Centre and the Consumers' Association of Canada[vi] argues that changing this relationship violates the Canadian Telecommunications Act. The program has also sparked an investigation by Canada's Privacy Commissioner as data on users' online behaviours are being tracked by the Internet service provider without user consent (opting out only impacts the advertisements served to users, it does not exclude customers from behaviour tracking). As society becomes increasingly reliant upon Internet service providers to provide connectivity to the services essential to daily life, it is important to raise awareness of instances where service providers exploit their customers for commercial gain, or violate customers' reasonable expectations of privacy in transacting their lives online.

Getting services fixed when something goes wrong often proves challenging. Years ago, going without Internet service for a couple of days would not cause great difficulty for most, but now, in an increasingly 'digital by default' world, a problem with service means that people are disconnected from the infrastructure required to access essential services. The onus of

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

resolving the problem is firmly on the consumer, and often great resilience is needed to fully resolve complaints to the consumers' satisfaction. Research by the UK Communications Consumer Panel found "some consumers are suffering in silence while for others, the negative experience of contacting their provider – the time taken to resolve a complaint, the number of contacts required and the sheer level of persistence demanded to reach a solution – made the whole situation worse," concluding that "this is simply unacceptable."[vii]

In an ideal world, individuals would have an extensive choice of Internet service and broadband network providers, allowing them to avoid those with unfavourable terms of service. Some countries have been more successful than others in establishing strong competition among Internet service providers. There are also instances where communities or governments have decided to build their own infrastructure, providing an opportunity for alternative approaches to Internet service provision, often on more favourable terms. For most individuals however, a do-it-yourself approach to infrastructure is highly impractical, and in some locations in the United States, local initiatives to develop infrastructure that would compete with private sector providers are banned or constrained.[viii]

The discussion above notes a number of issues that impact individuals' access to Internet services. As Internet access is essential in a digital society, there is a role for researchers to articulate these access challenges, and to identify approaches to improving access. Efforts to define what adequate Internet service consists of when it is the platform underpinning service delivery and communication are necessary. Researchers can explore the deficiencies in service availability and identify policy actions that can help to ensure that adequate Internet infrastructure is available to all citizens at an affordable price. There are opportunities to explore alternative models of network provision, focusing on identifying various stakeholders' needs and finding ways to satisfy them. Particular challenges persist in providing service to rural and remote areas where existing coverage and choice of providers is poor. There are questions about the role of regulation, for instance to ensure network neutrality principles are applied. Is more oversight needed to ensure that citizens get the services they pay for, and that problems in service delivery are resolved in a way that recognises the essential nature of connectivity in a digital society? If so, what form(s) might such oversight take?

Putting Mobile Connectivity on the Policy Agenda

In 2011, the Australian Communications and Media Authority observed: "There is widespread recognition that mobile broadband services are an economic enabler within society and the provision of these services, technologies and applications in the wider community is in the public interest" (Australian Communications and Media Authority

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

2011). The International Telecommunication Union estimates there are now more than 2 billion mobile broadband subscriptions worldwide (International Telecommunication Union 2013b), and Cisco forecasts increasing demand for additional services over the next few years (Cisco 2014). Although demand is strong for mobile services, mobile broadband access is much more expensive than fixed line access at present. Despite the convenience of anytime, anywhere access to the Internet when connecting with mobile broadband, individuals often limit their use when away from a home base, as evidenced by data showing that the vast majority of data is downloaded over a fixed line connection rather than a wireless one (Australian Bureau of Statistics 2013). This behaviour may suggest that although individuals find value in mobile broadband services, the current models for service provision do not fully meet their needs for connectivity while away from their fixed line services.

Provision of mobile broadband services is somewhat fragmented. In addition to the services from commercial providers, represented by the 2 billion subscribers, mobile broadband connectivity is available in many locations through Wi-Fi. There are no comprehensive statistics that track Wi-Fi users, and data downloads on Wi-Fi devices are recorded as fixed line downloads, making it difficult to determine the demand for, and use of this form of mobile broadband connectivity. Service is available on a patchwork basis, with many different providers offering Wi-Fi coverage in specific geographic locations, sometimes for free, sometimes not. Public Wi-Fi connections are often unreliable – some simply do not work at all, and others offer very slow speeds or allow only limited access to particular online sites and services.

At present, mobile broadband is often viewed primarily as a complement to fixed line services. Policies tend to focus on shaping the environment for commercial mobile broadband provision (e.g. licensing and allocating spectrum). To better reflect user experience, it is suggested that mobile broadband should be defined broadly as a service offering wireless broadband connectivity, accessible over licensed or license-exempt spectrum (i.e. from commercial or non-commercial providers, through Wi-Fi or through commercial providers' networks) and available in multiple locations.[ix] Existing business models offer mobile broadband connectivity in silos, with commercial services not integrated with Wi-Fi offerings. This approach can be frustrating for consumers who want reliable, affordable coverage without constantly having to negotiate the terms of access to available services.

There are policy questions as to whether mobile access to the Internet is necessary to enable full engagement in a digital society. Should efforts to develop robust broadband infrastructures expand to include mobile connectivity? Is it reasonable for citizens to expect access to the Internet from everywhere, and if so, should making broadband coverage

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

ubiquitous be an objective for governments? What are the characteristics of good mobile broadband connectivity, in an era of digital by default services? What do consumer-centric business models for mobile broadband connectivity look like, and how do they differ from existing offerings? What policy options are there to encourage extension of mobile broadband services, and how can government intervention avoid interference in existing competitive markets? To date, national government efforts have focused on defining the type of fixed broadband infrastructure required to enable a digital society, with accompanying actions to foster fixed line infrastructure development where needed. But as the OECD asks, "Why shouldn't every fixed network node support a mobile wireless connection?" (OECD 2012). This is as much a political question as a technical one, but raises further questions about the role of policy to extend mobile broadband coverage through Wi-Fi as well as commercial services. These are some of the many questions to be investigated regarding the ongoing role for mobile broadband in a digital society.

Data for a digital society

Ensuring good access to the Internet and other broadband services is essential in a digital society. It is important to be able to monitor the provision of broadband services, to assess coverage, as well as quality, reliability, and affordability, so as to understand whether this essential digital infrastructure is meeting citizens' connectivity needs. Connectivity provides a platform for engagement but to actually make use of online services, and to interact with others in a digital environment, individuals need to know how things work. The concept of digital literacy is used to describe an individual's ability to use the Internet and online tools and services effectively. Initiatives to improve digital literacy across populations are central to many national digital strategies, and it is essential to be able to understand literacy levels when designing new services and encouraging a shift to digital by default engagement with governments and others.

There is extensive research on the digital divide, identifying and describing those who, by choice, economic circumstance or because of a lack of skills, do not make use of digital tools and services, but much more insight is needed to understand the consequences of not engaging in a digital society. The idea of engagement itself is nuanced, and has not been captured effectively in quantitative data compiled by the International Telecommunication Union on the characteristics of an information society (International Telecommunication Union 2013a; Middleton 2013b). Even basic statistics, like Internet adoption rates, are not very informative, because they are based on binary measures, meaning that a highly competent, frequent user is counted in the same way as a tentative, infrequent user. National level surveys offer some additional information, including lists of things that Internet users do online, but still provide limited insights into whether Internet users have the necessary

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

skills to negotiate online information and services,[x] and to use online tools as a central means of communication. In an increasingly 'always-on' culture, measures like hours spent online are poor indicators of engagement.

Data on connection speeds and costs of fixed and mobile broadband services can be quite contentious. The OECD has been tracking these for years,[xi] providing relative rankings of service quality and pricing across countries, and demonstrating changes over time. These data are used by policy makers to demonstrate the success of their policies, or as a call for action when performance is not internationally competitive. Researchers often point to these data to note failures in policy environments, but can be subject to aggressive attempts by service providers to argue that the data are inaccurate, and produced using flawed methodologies.[xii] Researchers and service providers may choose to be selective in the data they present, focusing on figures that support their particular viewpoints while ignoring others that offer contradictory perspectives. Part of the challenge of making sense of OECD data is that the metrics offered do not always accurately capture the ways that services are used or marketed (e.g. the bundles of services included in price calculations are not reflective of bundles users are offered or would choose to consume, and speed data tracks advertised speeds rather than comparing the speeds tiers users are paying for with what is actually being delivered).

There are opportunities for researchers to engage in policy making processes, for instance by participating in consultations with assessments of the nature of existing infrastructure, or providing data on literacy and engagement in digital society. However, as researchers and policy makers often frame issues in different ways there is work to be done by researchers to better understand how to intervene effectively.[xiii] But because researchers may frame issues differently, they can offer new perspectives on existing data, and help to identify the sorts of data that, if collected by regulators and government agencies, could allow for better decision making around infrastructure and access in a digital society.

There is a long tradition of research as to how people make use of digital communication technologies, and how networks are provisioned. What is important now is to revisit previous research with a view to understanding what changes when digital technologies are no longer just an additional way of engaging, but are the primary means of interaction for every day activities. What changes when digital technologies are not optional, but essential, and what metrics are needed to assess the changes? Who has the necessary data to understand engagement in a digital society, how could these data be improved, and what partnerships could be developed to foster more informed data analysis? How is essential infrastructure assessed? What does digital engagement really mean, and how can it be recognised? There are many questions that can be better understood with more

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

comprehensive, nuanced data, and researchers can partner with policy makers and industry to develop stronger evidence bases for assessment and decision making.

Closing Comments

In closing, it is noted that researchers can play an important role in informing the development of digital society. This paper has focused on issues related to access to fixed and mobile broadband services, and discussed the need for better data to inform decision making, but it is noted these are not the only avenues for engagement. Regulators and policy makers are influenced by dominant discourses. In matters related to shaping digital society, the viewpoints of industry are well-articulated, but perspectives of civil society stakeholder groups and individual citizens are not always so clear. Alternative perspectives should be articulated, and researchers can use their analytical skills to interpret data and surface perspectives that might otherwise be overlooked.

Acknowledgement

This paper is based on a keynote address given to the *Emerging Issues in Communication Research & Policy Conference*, hosted by the News & Media Research Centre at the University of Canberra in November 2013.

References

Australian Bureau of Statistics. 2013. 'Internet Activity, Australia, June 2013 – Volume of Data Downloaded by Access Connection, for ISPs with More Than 1,000 Subscribers'. Accessed 5 November 2013. Available from: http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0.

Australian Communications and Media Authority. 2011. 'Towards 2020—Future Spectrum Requirements for Mobile Broadband'.

Australian Government. 2013. 'Advancing Australia as a Digital Economy: An Update to the National Digital Economy Strategy'. Canberra: Department of Broadband, Communications and the Digital Economy.

Cabinet Office. 2012. 'Government Digital Strategy'. United Kingdom.

Cisco. 2014. 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018'.

Cisco; International Telecommunication Union. 2013. 'Planning for Progress: Why National Broadband Plans Matter'. Geneva: International Telecommunication Union.

Industry Canada. 2009. 'Broadband Canada: Connecting Rural Canadians'. Accessed 18 February 2014. Available from: http://www.ic.gc.ca/eic/site/719.nsf/eng/home.

Infocomm Development Authority of Singapore. 2010. 'Realising The iN2015 Vision. Singapore: An Intelligent Nation, a Global City, Powered by Infocomm'. Singapore: IDA.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

Infocomm Development Authority of Singapore. 2013. 'Fact Sheet: Next Generation Nationwide Broadband Network (July 2013)'. Accessed 11 August 2013. Available from: https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Infrastructure/Wired/NextGenNBNFACTSHEET.pdf.

International Telecommunication Union. 2013a. 'Measuring the Information Society'. Geneva: International Telecommunication Union.

International Telecommunication Union. 2013b. 'The World in 2013: ICT Facts and Figures'. Geneva: International Telecommunication Union.

Jackson, Steven J.; Edwards, Paul N.; Bowker, Geoffrey C.; Knobel, Cory P. 2007. 'Understanding Infrastructure: History, Heuristics and Cyberinfrastructure Policy'. *First Monday* 12 (6-4). http://dx.doi.org/10.5210/fm.v12i6.1904

Middleton, Catherine. 2013a. 'What About Wireless? An Investigation of Mobile Broadband in Fibre to the Home Environments'. Telecommunications Policy Research Conference; Arlington, VA.

Middleton, Catherine. 2013b. Beyond Broadband Access: What Do We Need to Measure, and How Do We Measure It? In *Beyond Broadband: Developing Data-Based Information Policy Strategies*, edited by Taylor, Richard D and Schejter, Amit M. New York: Fordham University Press. 9-22.

OECD. 2012. 'Fixed and Mobile Networks: Substitution, Complementarity and Convergence, OECD Digital Economy Papers, No. 206'. Paris: OECD Publishing.

OECD. 2013. *OECD Skills Outlook 2013: First Results from the Survey of Adult Skills*. OECD Publishing.

Shepherd, Tamara; Taylor, Gregory; Middleton, Catherine. 2014. 'A Tale of Two Regulators: Telecom Policy Participation in Canada'. *Journal of Information Policy* 4: 1-22.

US Department of State. 2012. 'Digital Government: Building a 21st Century Platform to Better Serve the American People'. Washington, DC.

EndNotes

[i] See the Infocomm Talent Portal, at http://www.infocommtalent.sg.

[ii] The Broadband Commission for Digital Development has done extensive work advancing digital society in the developing world (see http://www.broadbandcommission.org) but the scope of this paper is on the developed world.

[iii] There is extensive existing research in these areas. This paper outlines some ways in which these areas can be advanced through ongoing attention and highlights their importance for strengthening citizens' capacity for engagement in digital society.

[iv] The US Federal Communication Commission's *Open Internet Order* was struck down by an appeal court in late 2013. The FCC Chair has indicated that the commission will take action to restore the principles of network neutrality that were set out in the Open Internet rules but at the time of writing no action had been taken.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.27

[v] See CRTC file 8622-B92-201316646. Part 1 Proceeding – Application requesting fair treatment of Internet services by Bell Mobility, extended to consider the fair treatment of mobile TV services offered by Rogers and Videotron.

[vi] CRTC file 8665-P8-201400762. Part 1 Proceeding – Application regarding Bell's use of customer information.

[vii] http://www.communicationsconsumerpanel.org.uk/news-latest/latest/post/304-going-round-in-circles-the-consumer-experience-of-dealing-with-problems-with-communications-services

[viii] See the Institute for Local Self-Reliance's Community Broadband Networks website at http://muninetworks.org/communitymap for information on the 19 US states which have barriers in place to discourage or disallow local broadband initiatives.

[ix] This definition and arguments about the need for a more user-centric view of mobile broadband are developed more fully in Middleton (2013a).

[x] The OECD survey of adult skills (OECD 2013) parses out these differences and reveals that many adults have quite limited capacity to solve problems in technology-rich environments.

[xi] http://www.oecd.org/sti/broadband/oecdbroadbandportal.htm

[xii] See for example the exchanges between Canadian legal scholar Michael Geist, and employees of TELUS, one of Canada's largest wireless service providers, about whether wireless prices in Canada were competitive. http://www.michaelgeist.ca/content/view/6906/125/

[xiii] This challenge is explored by Shepherd, Taylor and Middleton (2014).

Cite this article as: Middleton, Catherine. 2014. 'Building a digital society: Questions for communication researchers'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 27.1-27.11. DOI: http://doi.org/10.7790/ajtde.v2n1.27. Available from: http://telsoc.org/journal

Information Network Villages

A community-focused digital divide reduction policy in rural Korea[i]

Man Chul Jung
Foundation of Agriculture, Technology, Commercialization & Transfer (South Korea)

Sora Park
University of Canberra

Jee Young Lee
University of Canberra

This study examines South Korea's Information Network Village (INVIL) project as an exemplary policy of building sustainable communities through a digital divide policy implemented in small rural areas. INVIL project has three objectives: to close the digital gap between urban and rural areas, to create new sources of revenues from existing industries, and to build sustainable local communities. The conception was that rural digital divide can only be resolved by addressing deep rooted rural issues that influence the provision and adoption of ICT. While the INVIL programs may not remedy the gap in the short term, it provides a future vision to the communities. Due to this multi-layered and long term approach, the villages have been successful in narrowing the digital divide, not only in terms of access but also in effectively utilising broadband to enhance the local economy and building sustainable communities. This paper introduces the INVIL project, the plans and outcomes, as well as a qualitative evaluation of the process across a decade. Following a general description of the project, an in-depth case study of three successful INVILs is provided. The uniqueness of the program is that it emphasises investment in human capital rather than on infrastructure and includes a tailored vision of each local community. This motivates local residents to be active participants, which is the key to the success of the policy.

Introduction

South Korea is one of the most connected nations in the world, with 82.3% of households using broadband, with an average connection speed of 14.7 Mbps and with smart phone users reaching over 60% of the population (Korea Communications Commission 2013; Korea Internet Security Agency 2013). Nevertheless, the rural digital divide issue has not been resolved and there is still a considerable gap between urban and rural areas in terms of access and usage. The digital divide index reported annually by the Korean Government

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

indicates that rural residents still have less access, and more importantly, the gap in skills and utilisation of the Internet is still persistent (Park & Kim 2014).

The Information Network Village (INVIL) project, a government funded initiative to bridge the rural digital divide, was launched in 2001. The government acknowledged that laying the infrastructure in rural areas cannot simply remedy the digital gap and that further intervention would be necessary. This paper examines the framework of the INVIL project, analyses the outcomes and provides an in-depth case study of three exemplary villages that have benefited from the project.

Rural areas are disadvantaged in telecommunications infrastructure due to the distance from major cities and the low population density. Without public intervention, it is not usually economically viable to provide quality services to rural areas. Digital divide policies have always been South Korea's priority with regards to rural and urban areas. This is particularly so because rural areas overlap considerably with agricultural and fishery communities that have been socially excluded groups.

The provision of broadband in rural areas is an initial step towards overcoming the digital divide. However, access itself does not guarantee adoption and usage. In order for broadband connectivity to result in benefits for users, people must use the technology effectively. Effective use captures the notion that beyond connectivity, users must have the capacity to use the services to realise their benefits (Gurstein 2003). Thus, government subsidised programs alone cannot achieve sustainable adoption. Other intervention policies such as public education campaigns must follow (LaRose et al. 2011; Strover 2001).

Empirical research indicates a positive economic impact of infrastructure investment in rural areas (Katz & Suter 2009). This is enabled not only by increasing productivity and creating value for businesses but also by enabling sustainable social networks and communities (Atasoy 2013; Hollifield & Donnermeyer 2003; Steinfeld et al. 2012; Stenberg et al. 2009). However, digital divide policies are difficult to implement in rural areas due to the lack of community participation (Kumar 2012) or other unintended externalities, such as deprivation of human resources in rural communities (LaRose et al. 2008) or benefiting non-agricultural sectors rather than the target area (Flor 1993).

The complexity of enabling sustainable broadband adoption and usage in rural areas is the reason why despite aggressive government policies on the digital divide policies, the rural sector still has the largest gap among digitally excluded groups including the disabled, low income and aged (NIA 2012b). South Korea has been successful in closing the access gap but the second-order effects of skilful use of the technology have not been resolved (Moon et al. 2012).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

Information Network Villages (INVIL)

In 2001, South Korea's Ministry of Security and Public Administration (MOSPA, former Ministry of Public Administration and Security) launched the Information Network Village (INVIL) program starting with 21 INVILs. The program aimed to narrow the digital gap between urban and rural areas by equipping rural citizens with the necessary skills to thrive in the online environment. The ultimate aim was to enable rural citizens to use those skills to increase income levels and improve everyday lives (INVIL Central Agency 2013a). As of 2013, 361 INVILs were operating in various locations across the country in small rural towns.

For the first few years, the project focused mainly on investing in infrastructure, setting up the INVIL Centres, distributing computers to rural households and designing INVIL websites. Korea Telecom (KT), which was a public company at that time, participated in the consortium, enabling large-scale capital investments in the early days of the project. Since 2006, more focus was placed on identifying sustainable income streams from either e-commerce or by selling rural tourism packages.

As of June 2013, among the 394 INVILs funded by the government, 361 were actively operating. The majority of the villages – 247 (68%) - were launched in the first five years of the program. This reflects the policy framework of first laying the infrastructure and then finding ways to sustain the uses. INVILs are classified into revenue generating models and non-revenue models. There are three types of revenue generating models: e-commerce, tourism and mixed. Non-revenue INVILs are mainly urban community models. Except for the four non-revenue villages that are located in urban areas, INVILs are designed to generate additional income (Whang 2012).

The cost of setting up one INVIL is approximately A$300,000. Thus most of the funds are spent on maintaining and managing the centres. In 2013, the central government budget for the INVIL program was A$5 million, of which 30% was allocated to salaries of INVIL managers. The central and provincial governments contribute to the maintenance of the villages. While the proportion varies by area, the provincial governments are increasingly taking up a larger role.

Gangwon Province has the most INVILs with 57 in total, whereas Gyungki Province has 54. Provincial governments of these two provinces contribute approximately 46% and 52%, respectively, to their INVIL programs, which is a higher figure compared to other provinces. Both provinces are relatively close to Seoul metropolitan area, which makes the tourist packages more accessible to urban residents (Table 1).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

	2001	2002	2003	2004/ 2005	2006	2007	2008	2009	2010	2011	2012	2013	Total
Busan	-	1	2	1	-	-	-	-	-	-	-	-	4
Daegu	1	1	-	-	-	-	-	-	-	-	-	-	2
Gwangju	1	1	2	-	-	-	-	-	-	-	-	-	4
Gyungki	3	5	9	19	6	6	6	-	-	-	-	-	54
Gangwon	3	10	9	8	9	6	4	3	2	1	1	1	57
Chungbuk	-	5	3	5	1	4	2	2	1	-	-	-	23
Chungnam	1	10	8	7	2	3	3	-	-	2	1	-	37
Jeonbuk	2	6	8	13	4	2	2	2	-	-	-	-	39
Jeonnam	2	8	13	11	1	4	6	3	-	-	-	-	48
Gyungbuk	5	14	10	10	1	3	1	-	1	1	1	-	47
Gyungnam	2	6	7	5	1	3	3	2	-	-	-	-	29
Jeju	1	3	3	3	1	3	3	-	-	-	-	-	17
Total	21	70	74	82	26	34	30	12	4	4	3	1	361

Table 1- INVIL launch by province and year
Source: INVIL Central Agency (2013a)

Among the 361 active INVILs, 251 were funded initially by the central government's fund and 110 were funded exclusively by the provincial governments. The central government reviews the performance of INVILs every year and if a village fails to fulfil the requirements for two years in a row, then the government can decide to withdraw the funds. To date, there have been 33 villages that have been revoked. According to the INVIL Central Agency (2013b), there are several reasons why a village might be assessed as unsatisfactory. First, some villages have had conflict between residents and the INVIL manager. New sources of revenue became the source of conflict, thus causing disruption of the community. The second reason

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

is due to the lack of quality control of the new products the village are offering and thus not accumulating enough revenues. Finally, some villages were re-assigned to another administrative area by the government because of the declining population and thus became non-existent.

The vision of INVIL was that, in order to overcome the rural digital divide, the provision of infrastructure and services must be followed by participation in the digital economy by rural residents and eventually sustainable communities enabled by the new technologies. The emphasis on community building is the unique feature of the project. From its inception, the INVIL project had four distinct characteristics: first, it was a joint program between the central and provincial governments; second, it was built upon the existing strengths of the rural communities; third, it was based on very small communities, often smaller than 100 households, which made it manageable; fourth, it was designed as a long term project that would continue for several years or decades. Unlike many programs where infrastructure costs are provided upfront but facilities are never updated, INVIL emphasised maintenance and sustainability.

The central government oversees the funded villages nationally and provides the initial funding. The provincial governments select, manage, review and provide support in their areas. This systematic approach allows each village to build upon its own strengths and needs. Once the village is set up with the training centre, a full time employee – the INVIL manager – takes up a crucial role in developing and maintaining the program. The manager helps the villages set up their websites, run training programs and create user demand by examining the local needs. Often an existing community member, the manager is an essential component of the program.

There have been many tangible outcomes of the INVIL program over the past decade. In particular, INVILs have been largely successful in narrowing the digital divide. Before the INVIL program was launched, in villages selected for the INVIL program the average computer penetration was 37.3% and Internet usage 9.1%. After the launch of the INVIL program, the averages increased to 72.1% and 66.5%, a much higher rate compared to the rural average (see Table 2 below). The increase in usage can be ascribed to the training programs offered by the INVIL managers. In the early stages of INVIL, most of the training programs focus on basic computer use; but once the village is established, setting up e-commerce sites, online marketing, system operation and online finance become more popular among village residents. In 2001, there were about 15,000 trainees in the program, but by 2012 this figure had increased to 400,000.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

The central government provides training opportunities to INVIL managers every year, so that they can improve their services to the local community members. In 2012, MOSPA held more than 20 training sessions for INVIL managers in nine locations. The provincial governments also run re-training programs for the managers. Most INVIL managers have at least two professional trainings per year.

	INVILs		**Agricultural/fishery areas** (2011)	**National average** (2011)
	(2000)	(2008)		
Computer penetration	37.3 %	72.1%	60.8 %	81.9 %
Internet usage	9.1 %	66.5%	38.9 %	78.3%

Table 2 - Access and usage gap between INVILs and non-INVILs

Source: National Information Society Agency (NIA) (2012).; National Information Society Agency (NIA) (2012).; INVIL Central Agency (2013b).

The economic outcome of INVIL programs has been confirmed by various statistics and empirical studies. In Gangwon Province, the revenues of INVILs were increased by 827.5 times in 2010 compared to 2001 (Whang 2012). The main factors contributing to revenue increase were the websites and knowledge sharing among community members (Jeong et al. 2010). To systematically enhance economic gains, MOSPA set up two central websites: one for selling local produce and the other for selling travel packages. The central agency provides consultation to rural farmers to help them develop new products, services and marketing tools. Revenues from the two online shopping malls in 2006 were $A3 million, which increased to A$40 million in 2012. During the same period, the average revenue per village increased from $A11,000 to $A114,000. In 2012, there were 1.1 million INVIL online shopping mall visitors and 176,181 purchases were made through the site. INVIL travel package visitors reached 310,000 and 38,443 purchased travel packages from the site (see Figure 1).

The INVIL online shopping mall has sold more than 11,000 different types of products to date. Most of them are locally produced agricultural products. The most popular products in 2012 were green apricot jelly (Jeonnam Gwangyang ‘Maehwa Village’), wild honey and apples (Miryang ‘Ice Valley Apple Village’; Yeongdeok ‘Peach Village’). While selling local produces to consumers in other areas can help local farmers in terms of revenue, the flow is

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

outbound. In contrast, various tourist packages can bring travellers from other areas into the local community that has externalities such as boosting local businesses and building a sense of community among the members. There are 348 different INVIL travel packages such as farm-stay, weekend farming and bed-and-breakfast. Popular packages include 'making cheese' at Imshil Cheese Village, 'trout catching' at Jeongseon Baekdu Village and 'clam digging' at Hwaseong Baekmiri Village.

While e-commerce and online tourism packages are the main components of the INVIL program, there are other promotion events such as 'INVIL Festa', which is held annually to encourage face-to-face interaction (http://festa.invil.org/index.html).

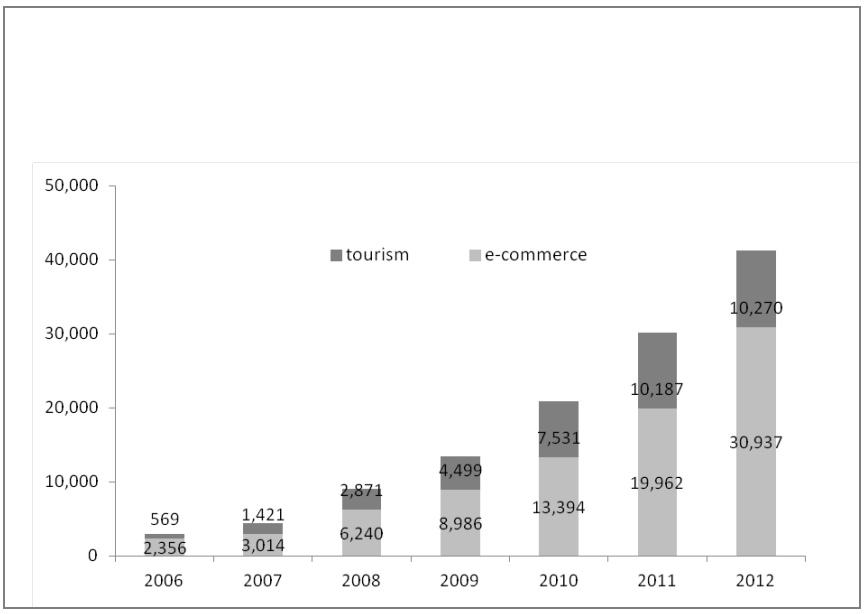

Figure 1 - Revenues from e-commerce and tourism (Unit: A$1000)

Source: INVIL Central Agency. (2013b).

Case study of three villages

The community has always been at the centre of the INVIL program. The commitment of local residents is a major component for the program to be launched. Participation is crucial to the maintenance of the program. Participation could be in the form of online engagement, training or other economic activities generated by the program (Kang 2009).

The essential element of the INVIL project is to build sustainable communities. This is an outcome that cannot be quantified but nonetheless crucial to the performance of the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

program. It is more difficult to ascertain such intangible benefits and a case study approach may be useful in that regards.

We conducted an exploratory case study of three successful villages - Mosan Onion Village, Baekmiri Village, and Gaemideul Village - to evaluate the intangible outcomes as well as the potential for a longer-term policy strategy applicable to all rural areas. In 2012, Mosan was the village with the highest e-commerce revenues while Baekmiri generated the highest tourist package income. Gaemideul adopted a combined approach of having both e-commerce and tourism components in their program, and has been awarded the best village prize for three consecutive years by the Government.

The purpose of this case study is to assess the program by using both qualitative and quantitative measures. We interviewed three INVIL managers of the villages selected as the sites. We also consulted public government documents, Information Village Network websites and interviewed the INVIL program co-ordinator at MOSPA. Multiple sources of data were used to validate the results and minimise any bias of the qualitative data. We used a case study approach due to the complexity and unpredictability of the policy outcome (Liu 2012). The aim of the case study was to qualitatively assess the program's effectiveness, not only in terms of tangible outcomes but capturing the externalities.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

Name of village	Mosan Onion	Baekmiri	Gaemideul
Business model	E-commerce	Tourism	Combined
INVIL launch year	2003	2008	2009
Number of households(population)	220 (350)	130 (370)	39 (88)
Percentage of households participating	43%	54%	36%
Informatisation			
Computer penetration (%)	50%	More than 90%	90%
Internet usage (%)	50%	More than 90%	70%
Average ICT training frequency per INVIL participant per year	5.5	4.7	68
Economic gains			
Average annual income generated by INVIL per household (2012)	$A4,700	$A54,300	$A39,200
Average increase in income per year since the start of INVIL	66%	176%	103%
Sustaining communities			
Number of website visitors in 2012	34,000	35,000	51,000

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

	Number of tourist program participants in 2012	400	150,000	28,000

Table 3 - Comparison of three villages

Mosan started the INVIL program in 2003 and launched their e-commerce site in 2006. As of 2013, 43% of the households participate in selling their products online. Internet use among INVIL households in Mosan is about 50%, which is higher than the overall village average of 20%. Compared to urban areas or the national average, this is still a low figure but considering its high median age and previous usage statistics, this is a promising outcome. Since 2003, when Mosan was first funded by the INVIL program, there has been very little upgrade in computer facilities in the households mainly due to the aging population.

The main products they sell online are onion extract and peeled garlic, both very popular food products in South Korea. This generated an average of $A4,700 extra revenues a year per household in 2012. Since 2006, the average increase in income was 66% for INVIL households. Each year, approximately 340,000 visit the village website and purchase products online. Around 400~500 online consumers visit the village to participate in harvesting and processing the original produces, which generates additional tourism revenues.

Active participation of the residents was crucial to the success of this INVIL. Participants hold a monthly meeting to discuss INVIL management issues but during those meetings, they naturally talk about ways to improve their community as well. Among INVIL participants 74% are over the age of 60, which is a similar trend in most agricultural regions. Mosan Village was one of the earlier INVILs, launched in 2003. This makes it vulnerable to sustainability issues. Computers at home have not been replaced since then and Internet usage has not improved. Nonetheless, having regular visitors from outside the village has enabled a more vibrant and lively village atmosphere.

Baekmiri focuses more on selling tourist packages to urban residents. It is a fishery village located in Gyungki Province, southwest of Seoul. Program participants have a high computer penetration (over 90%) and internet usage rate (over 90%). Their main products are clam/crab catching packages. The tourist packages are seasonal – popular during May to November. Nevertheless, it has been a solid source of additional income for the village households. Since 2009, the average annual revenue increase has been 176%. In 2012 alone, 150,000 tourists have visited this village, most of them from Seoul metropolitan area. This has become a source of indirect revenues where tourists purchase local produce while they visit the village, amounting to $A7.8 million per year.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

During the non-tourist season – December to April – INVIL participants received an average of 5.7 ICT trainings per year. The new business model of drawing tourists to the village where participants are required to take part, as well as the frequent interaction through training sessions, have heightened the sense of community among INVIL participants.

Gaemideul adopted a mixed model of selling agricultural products and tourist packages online. It is a typical farm village, the main produce being organic chilli peppers and bonnet bellflowers, both popular Korean vegetables. In 2009 they were funded by the INVIL program and 36% of the households currently participate. Computer penetration is 90%, while internet usage is 70%, both relatively high figures compared to other rural areas.

This village is particularly active in getting regular ICT training. On average, INVIL participants attend about 70 training sessions per year. The main products they sell online are organic peppers, wild vegetables and corn. Their tourist packages include trout fishing, making rice cakes and bicycle hiking, which were carefully designed to appeal to urban families.

In 2012, there were 50,000 website visitors and around 28,000 tourists visited the village. While most of them purchase tourist packages online, that was not always the case. Total revenues generated by the INVIL program in 2012 were A$549,000. This was an increase by 103% since the launch of the program in 2009.

The most striking outcomes of the INVIL program are digital engagement and participation in the digital economy. However, there are many other intangible outcomes that make the program sustainable. The INVIL managers of Gaemideul and Baekmiri both suggest the morale of the residents has been boosted by participating in the program, mainly because they now have an extra source of revenue. Another spill-over effect occurs during digital training sessions because these provide opportunities for villagers to meet with other residents. More frequent interaction with members enhanced their sense of community. This was observed in all three villages by the managers.

Participation in the program is purely voluntary, so there were no conflicts between INVIL households and non-INVIL households. However, pollution and noise were suggested as a factor that discourages certain residents to participate in the program. This was especially the case in tourist packages, where urban visitors would create unnecessary noise and increase garbage in the area.

One of the most critical issues in the sustainability of the program is the aging population of the villages. In Baekmiri, 66% of INVIL participants are over the age of 60 and 74% in Mosan

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

Village. This trend cannot be resolved through INVIL programs but, nonetheless, can be a crucial hindrance of the program.

Gaemideul provides some insights into how rural communities can overcome this problem. INVIL participants over the age of 60 comprise only about 33% in this village. Most of the participants are in their 40s. They provide good examples of rural migrants through their tourist packages and useful information about living in rural communities. Some of the INVIL participants are rural migrants who have high levels of digital literacy. They inspire the existing community members, teach them how to use digital devices informally and actively communicate with the senior residents.

The seasonality of agricultural products and tourist packages is another hurdle to overcome; the revenue stream is not consistent throughout the year. Mosan actively addressed this issue and has developed processed agricultural products that can be sold year round. In case of Gaemideul, they have developed a tourist package – straw art – that can be experienced in an indoor environment during the winter months.

Conclusion

The INVIL program is a unique digital divide policy that has been largely successful in narrowing the rural digital gap in South Korea. Its unique approach to the adoption of sustainable broadband is the key to the success. First, the INVIL program can be differentiated from any other government intervention programs in South Korea. Unlike previous programs such as the Ministry of Agriculture, Food and Rural Affairs' (MAFRA) Digital Lounge program or Rural Development Administration's (RDA) e-commerce grant, both of which limited the funding to 1~2 years, systematic support following the initial launch is built into the program. The emphasis on continuity rather than infrastructure is one of the reasons why INVILs are successful and sustainable.

Second, INVIL programs have an inbound strategy that brings people into the villages, if not in person, through their website. Sometimes, it stretches to attracting rural migrants into the area. All INVILs share the ultimate goal of building communities. It is not merely adding a layer of ICT to existing villages but a constant effort to enhance the sense of community by utilising the INVIL centres as a central location within the village where member convene. Typically, INVIL members actively participate in the program management which is facilitated by the INVIL manager. Managers are hired not only to operate the training centre but also to monitor, interact with and educate residents within the community.

Third, INVIL programs are designed to provide seamless switching between offline and online environments for a sustainable digital engagement. The website where participants

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

sell their produce or tourist packages is maintained by the INVIL manager and also overseen by the INVIL Central Agency. This provides standardised, quality access to any consumer who might be interested in purchasing the products and services. It also provides INVIL participants with a sense of a larger online community. More importantly, this space does not exist separately from their offline everyday lives where they convene and learn about the online space in their village centres. The manager serves as the intermediary in both the online and offline spaces, which makes the transition from being non-users of the Internet to active online participants easier.

The digital divide is not simply a binary divide between ICT haves and have-nots. Rather it should be understood as varied degrees of multiple layers of digital disadvantage. The digital exclusion issue is better understood if we adopt a concept of digital continuum that is related to other social exclusion parameters (Servon & Pinkett 2004). While INVIL is largely a successful policy due to its sustainable nature, there are still issues surrounding rural and urban digital divide that must be addressed. First of all, a second level digital divide may be occurring at various levels. Even in INVIL areas, the urban/rural divide has not completely disappeared. While the recipients have benefited greatly from such governmental support, the development of broadband technologies in urban areas is not static, meaning the urban counterpart would have advanced even further. This is why programs need continuous re-evaluation and re-design, in order to fully embrace the changing technologies.

Second, another possible area of the second level digital divide is that there may be a rift within the community between those who participate in the INVIL program and those who do not. Policies implemented to bridge the digital divide usually have an ultimate goal of benefiting all individuals. INVIL programs are effective in enhancing communities as a whole but there may be individuals who are not fully part of the picture. Currently, there are no statistics to support this argument and needs further attention in future research. The third area where the second level digital divide may occur is that there may be a widening gap among rural areas across the nation, creating a new type of hierarchy. There are some areas with largely successful INVILs but there are other areas with not-so-successful INVILs. Furthermore, there are non-INVIL areas where there is no support. This, again, is not supported by empirical evidence and needs further investigation.

Among the 394 awarded villages, 361 are still actively operating. This can regarded as a highly successful program in terms of the retention rate. This is in part due to the small size of each INVIL. In Korea, there were more than 3,400 small towns in rural areas as of 2012, which means only about 10% of the rural towns have benefited from the program to date. Such small sized projects made it manageable at the town level which is a crucial element of

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

the policy but this specificity may be a barrier when applying the policy to cities and larger regional areas where the sense of community may be slightly different.

This study examined the overall outcome of the INVIL program with the emphasis on the policy framework of narrowing the digital divide, increasing economic gains and sustaining communities. Three exemplary cases were examined to provide an in-depth account of how INVILs can help sustain rural communities. The analyses show that efforts to bridge the digital gap can be successful by identifying the needs of local communities and providing continuity in support. Further comparative analysis of villages that have been successful and those that have not may shed light on the common elements of sustainable broadband adoption in rural areas. INVIL managers play a crucial role in implementing and maintaining the program in each village. Their role extends beyond teaching digital literacy or technical support for the residents. The varied degree of participation and the outcomes of the 361 INVILs are largely dependent upon the capacity and enthusiasm of the manager. Further research into the multiple roles of INVIL managers will add knowledge to how digital divide intervention policies can be more sustainable.

Endnote

1. An earlier version of this paper was presented at the News and Media Research Centre 2013 Conference, Emerging Issues in Communication Research and Policy (Dec 2013, Canberra). .

References

INVIL Central Agency. 2013a. 'Information Network Village (INVIL) project guide book'. Seoul, Korea INVIL Central Agency.

INVIL Central Agency. 2013b. Internal Data.

Atasoy, H. 2013. 'The effects of broadband Internet expansion on labor market outcomes'. *Industrial & Labor Relations Review*, 66 (2): 315-345.

Flor, A. G. 1993. 'The informatization of agriculture'. *Asian Journal of Communication*, 3 (2): 94-103. http://dx.doi.org/10.1080/01292989309359584

Gurstein, M. 2003. 'Effective use: A community informatics strategy beyond the digital divide'. *First Monday*, 8 (12). http://dx.doi.org/10.5210/fm.v8i12.1107

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.21

Hollifield, C. A., & Donnermeyer, J. F. 2003. 'Creating demand: Influencing information technology diffusion in rural communities'. *Government Information Quarterly*, 20 (2): 135-150. http://dx.doi.org/10.1016/S0740-624X(03)00035-2

International Telecommunication Union (ITU). 2012. The impact of broadband on the economy: Research to date and policy issues. International Telecommunication Union (ITU).

Jeong, S., Koo, C., & Lee, D. 2010. 'A story of success factors and profitability of e-village shopping mall supported by the Korean government'. *Information Systems Review*, 12 (3): 141-158.

Kang, B. S. 2009. Bridging the digital divide between urban and rural areas: Experience of the Republic of Korea. ESCAP Technical Paper, (IDD/TP-09-07).

Katz, R., & Suter, S. 2009. 'Estimating the economic impact of the broadband stimulus plan'. Columbia Institute for Tele-Information Working Paper.

Korea Communications Commission. 2013. Annual Report 2012. Seoul, Korea: Korea Communications Commission.

Korea Internet Security Agency. 2013. Smartphone Usage Trend Report 2012. Seoul, Korea: Korea Internet Security Agency.

Kumar, R. 2012. 'Rural informatics: Use of information and communication technologies for the rural poor – from digital divide to digital opportunity in rural India'. *Media Asia*, 39 (4): 183-190.

LaRose, R., Gregg. J.L., Strover. S., Straubhaar. J., & Inagaki. N. 2008. Closing the rural broadband gap (Final technical report). Retrieved from https://www.msu.edu/~larose/ruralbb/.

LaRose, R., Strover, S., Gregg, J. L., & Straubhaar, J. 2011. 'The impact of rural broadband development: Lessons from a natural field experiment'. *Government Information Quarterly*, 28 (1): 91-100. http://dx.doi.org/10.1016/j.giq.2009.12.013

Liu, C. 2012. 'The myth of informatization in rural areas: The case of China's Sichuan province'. *Government Information Quarterly*, 29 (1): 85-97. http://dx.doi.org/10.1016/j.giq.2011.06.002

Moon, J., Hossain, M. D., Kang, H. D., & Shin, J. 2012. 'An analysis of agricultural informatization in Korea: The government's role in bridging the digital gap'.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

Information Development, 28 (2): 102-116. http://dx.doi.org/10.1177/0266666911432959

Ministry of Security and Public Administration (MOSPA). 2010. Current trends of Information Network Village (INVIL) project. Seoul, Korea: MOSPA.

National Information Society Agency (NIA). 2012a. 2012 Informatization white paper. Seoul, Korea: NIA. http://eng.nia.or.kr/english/bbs/board_view.asp?BoardID=20111222611162611&id=10365&nowpage=1&Order=301&search_target=&keyword=&Flag=&objpage=0

National Information Society Agency (NIA). 2012b. Digital Divide Index 2011. Seoul, Korea: NIA http://www.nia.or.kr/BBS/board_view.asp?BoardID=20111128132107445 8&id=6615&Order=010200&search_target=&keyword=&Flag=010000&nowpage=4&objpage=0

Park, S. & Kim, G. 2014 forthcoming. 'Lessons from South Korea's Digital Divide Index (DDI)'. *Info: the journal of policy, regulation and strategy for telecommunications, information and media*, 16(3).

Servon, L. J. & Pinkett, R. D. 2004. 'Narrowing the digital divide: the potential and limits of the US community and technology movement' in *The Network Society: A Cross-Cultural Perspective*, ed. M. Castells, Edward Elgar, Cheltenham, UK, 319–38.

Steinfield, C., LaRose, R., Chew, H. E., & Tong, S. T. 2012. 'Small and medium-sized enterprises in rural business clusters: The relation between ICT adoption and benefits derived from cluster membership'. *The Information Society*, 28 (2): 110-120. http://dx.doi.org/10.1080/01972243.2012.651004

Stenberg, P., Morehart, M., Vogel, S., Cromartie, J., Breneman, V., & Brown, D. 2009. Broadband Internet's value for rural America. US Department of Agriculture, Economic Research Service.

Strover, S. 2001. 'Rural internet connectivity'. *Telecommunications Policy,* 25(5): 331-347. http://dx.doi.org/10.1016/S0308-5961(01)00008-8

Whang, B. G. 2012. 'A study on performance evaluation of Information Network Village: Focusing on Information Network Villages in Gangwon-do'. *Journal of Korean Association for Regional Information Society*, 15 (4): 47-70.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.21

Endnote

[i] An earlier version of this paper was presented at the News and Media Research Centre 2013 Conference, Emerging Issues in Communication Research and Policy (Dec 2013, Canberra).

Cite this article as: Jung, Man Chul; Park, Sora; Lee, Jee Young. 2014. 'Information Network Villages: A community-focused digital divide reduction policy in rural Korea'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 21.1-21.17. DOI: http://doi.org/10.7790/ajtde.v2n1.21. Available from: http://telsoc.org/journal

Economics of public WiFi

Jason Potts
RMIT University

Local governments in urban regions continue to find the idea of public or municipal WiFi attractive. This is for multiple reasons, not all of which are based on economic logic (such as city branding, vote-buying, emergency services, commercial lobbying, peak-traffic broadband off-loading). However, the purpose of this paper is to gather together the basic economic arguments for and against public provision of municipal WiFi. First, we consider what type of economic good WiFi is, and the logic for public rather than market provision. Second, we review four main economic arguments against public WiFi (capitalization; no market failure; competitive distortion; inefficiency of supply side response). Finally, we consider what may be the strongest, yet least made, case for publicly funded municipal WiFi, which is local demand discovery as an implicit subsidy for WiFi entrepreneurship and innovation.

Keywords: municipal WiFi, public economics, market failure

Introduction

WiFi (Wireless Fidelity) is the brand name of a radio-frequency-based system (using the 802.11 standard) that allows an enabled device (such as a laptop, tablet or smart phone) to exchange data or connect to the Internet over a wireless local area network (WLAN) through an access point (called hotspots or zones). These access points have a range of about 20 metres, and are therefore ideal in a home or business setting to enable multiple devices to connect to a single access point that can be public (or open) or secure (requiring a password or registration). A wireless mesh network (WMN) involving multiple radio nodes over a mesh topology can enable WiFi to provide a blanket coverage over a much larger area, such as several city blocks.

The basic economics of wireless communication (Shy 2001, Benkler 2002) coupled with rapid growth and popularity of WiFi-enabled devices and the increasing demand to be always connected to the Internet has, since the early 2000s, induced numerous cities around the world, but particularly in the US, to undertake the provision of public or municipal WiFi (Travis 2006, Jassem 2010). By about 2008 this had begun to fail in the US (Wu 2007, Fraser 2009, Economist 2013) because of the technological and regulatory challenges associated with providing seamless coverage, but also for cost and convenience factors owing to competition from next generation (3G and 4G) broadband networks (Lehr and McKnight 2003, Yaiparoj et al 2008) as well as increased coverage by private providers of WiFi.

However, new wireless mesh network technologies, along with appreciation of multiple business models that a local authority might use to own and operate a public WiFi network

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

(Bar and Park 2006) have led to a resurgence of interest in municipal WiFi. This includes proposals in Singapore and Kuala Lumpur to mandate WiFi into all new businesses (such as restaurants) or make it part of new building codes. Thus despite the collapsed business case, the public provision of WiFi appears to remain attractive for city councilors, seemingly in the face of technological, regulatory and cost hurdles. This paper considers the basic economics of that choice.

What sort of economic good and market is WiFi?

Most economic analysis starts by identifying the type of good in question, classifying by properties of rivalrousness and excludability in order to determine whether a good is a private good (rivalrous and excludable), a public good (non-rivalrous, non-excludable), a club good (non-rivalrous but excludable) or a commons (rivalrous but non-excludable). A second step in the approach then considers the market for the good on a scale from competitive (free entry and marginal cost pricing) to monopolistic (entry barriers and average cost pricing). Economic analysis proceeds in this way in order to identify the prospect of market or coordination failure, and the existence and source of rents (whether these are natural consequences of the technology, or artificial consequences of regulation, the form of property rights, or imperfect competition). The purpose of this analysis is to diagnose any potential welfare gains from public provision or public intervention. A good that is essentially private in a market that is essentially competitive has no claim to improvement by public ownership or intervention. However, where market failure can be demonstrated, an economic argument for social welfare improvement through public provision can sometimes be made. But in order to reveal this, we first need to ask what type of good and market is WiFi?

First, is municipal WiFi a natural monopoly? This is the standard argument for public utilities and network goods (Shy 2001) and is based on recognition that wherever there are large fixed costs in establishing the service (say, building the network) and relatively low marginal costs in adding further clients, such that the average cost curve is everywhere downward sloping, then the most efficient number of suppliers is one. Such a natural monopoly is usually licensed to prohibit wasteful competition, but also regulated so that it cannot exploit its monopoly to price at a profit maximizing level. The combination of protection from competition and regulated pricing and service delivery invariably means that natural monopolies are not very innovative businesses, technologically stagnant, often captured by their workforces and stakeholders.

WiFi certainly has fixed-cost network-like properties. But there is no economic basis to claim that the most efficient number of providers is one. Rather, this only makes sense when we

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

speak of seamless roaming and passage from one WiFi zone to another, but that is a matter of interoperability standards (i.e. a coordination and contracting problem, not a supply problem). Yet while such standards can benefit from public imposition, there is no essential reason why they need to be. It is plausible that they more efficiently arise from voluntary associations through commons mechanisms. The Internet exchanges are an example of a highly effective voluntary association in this area (http://www.ausix.net/).

WiFi is clearly not a public good for the simple reason that access can be easily excluded through encryption keys. This is sometimes called a quasi-public good (a public good where exclusion is possible) but really it is a 'club good' instead (Buchanan 1965), the economics of which implies that the most efficient provision solution is through price-discrimination in the market. The relevant question then concerns the optimal size and sorting of WiFi clubs – given technological constraints in supply and business models in payments – and the extent to which that is distorted by regulation.

The language of quasi-public good is sometimes used in relation to WiFi when considering the limits to service obligations of commercial broadband networks. On the one hand, some parts of a market may be unprofitable and underserved by commercial networks, and public WiFi can fill that gap (this will rarely be the most efficient solution, compared to subsidizing extended broadband coverage, either on the demand or supply side). On the other hand, some parts of the broadband network can become congested at peak-load, and private providers may seek to off-load some of that data traffic onto WiFi networks (Qiu et al 2013). This can be efficient because it reduces overinvestment in broadband peak-load capacity. However, this outcome is usually a consequence of competition regulations prohibiting joint contracting of supply (sharing networks) in which different suppliers compete on some traffic and cooperate on others. This problem is widespread in public utilities and network goods such as rail transport and airline routes. The solution here is usually de-regulation to allow firms to organize among themselves, including new entrants, the most efficient mixture of pricing and bundling (as for example airlines now do with codesharing). This is the solution to the problem of discovery of optimal size and sorting of WiFi clubs.

Another claim made about WiFi is that it has properties that add value to existing public assets and utilities. WiFi is thus a 'bundled good' that can be added to existing or new assets such as public transport, and public utilities such as airports and public spaces, or bundled into all new buildings (through the building code). Economic efficiency usually comes from unbundling goods, or from the process of producers experimenting with different bundles to meet particular segments of market demand. Furthermore, the bundling argument applies equally to private providers of WiFi as a public good. For example, Microsoft and Yahoo, US

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

technology companies, have both offered free WiFi in select municipal locations in order to direct traffic to their search engines.

These arguments suggest that public WiFi may be less of an economic good than a political good (as analyzed in public choice theory, Olson 1971), in that it is something that can be offered to a particular group as a transfer from others (ratepayers within the council area) in order to secure the political support of that group.

Four basic economic objections to public WiFi

These initial considerations of what type of good and market WiFi is, despite the various degrees of boosterism from different lobby groups and consultancies (Cohen 2007), suggests that the case for public provision is neither obvious nor strong. This is plainly true of a lot of public sector activities, and is certainly not unique to WiFi. However, it will be useful to set out the main benchmark objections that a standard (neoclassical) line in economic reasoning would level against public provision of municipal WiFi.

#1 Capitalisation of 'free' WiFi in land value

The basic economic objection to public WiFi is that it is a pure rent transfer that will be capitalized in increased property values (Caplan 2001). The argument is simply that to the extent that the 'free WiFi' adds value to a location, that will increase the marginal product of the location, and thus its value to or 'willingness to pay' of existing and potential tenants, which at the margin will bid up land and building prices, which will at the margin flow through to rents. There may be redistribution if the WiFi is funded from a wide pool of ratepayers but the benefit is delivered to a narrow group.

Any benefit to particular consumers, say tourists passing through or local residents who lease (rather than own), that accrues to the free WiFi will be compensated by higher rents (owing to higher debt costs or higher rates from land valuations) and prices for local services (such as cafes and short-stay accommodation). For this reason the target population of the free WiFi policy – which is presumably a coalition of voters on lower incomes, renters, visitors, or those who benefit from a flow of visitors – may yet experience no net benefit once the general equilibrium effects have washed through. The main beneficiary would be landlords in the area serviced by free WiFi. Yet benefiting existing landlords is not usually argued to be the main purpose of public municipal WiFi.

A variation on this is capitalization in private companies that would benefit from increased Internet use, such as for example Google, Yahoo or Microsoft. The economic logic is that 'free' WiFi is a subsidy to Internet use, thus leading to increased consumer demand. In a monopolistically competitive industry, this increases the economic rents that accrue to

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

companies that sell goods that are complementary with increased Internet use (such as search technologies, devices or hardware). We would thus expect that the coalition of lobbyists seeking to promote public municipal WiFi would be composed of at least local property owners and Internet technology companies.

#2 There is no market failure

The theoretical case for public provision of a good or service requires evidence of some form of market failure that is causing an inefficient allocation. This can be due to a pervasive externality, asymmetric information, principal-agent problems, imperfect competition or public goods leading to a systematic under-investment in private provision of WiFi compared to the theoretical welfare maximizing optima.

It is difficult to make this claim. There have been numerous consultancy-driven reports extolling the benefits of public WiFi (Cohen 2007, for instance) but few serious attempts to estimate the costs, in terms of destroyed existing private infrastructure and business models, or the crowding-out effects on private provision. It is probably still too soon to tell. But analysing this from first principles there is no strong basis to suspect market failure in the direction argued by proponents of public municipal WiFi.

The externality argument is actually strongest in private WiFi networks and would suggest some kind of club good (for example eduroam, which is a global academic WiFi network). The existence of wide-spread private WiFi networks in cafes and most private businesses for instance suggests there are few barriers to entry and thus no market power to exclude at work. If there is a profitable opportunity to provide WiFi, we can expect it to be provided. This means that non-provision is probably due to it not being profitable to do so, which in turn gives us an indication of local consumers' willingness to pay at that point. There is no information asymmetry involved here (where buyer and seller have very different or hidden information, which can cause some markets to fail, such as insurance).

The upshot is that none of the standard market failure-based arguments for public provision seem to apply here. In consequence, public provision in such a situation is likely to lead to crowding out and an inefficient allocation through rent and wealth transfers. There will certainly be winners and losers from this, but not necessarily in a way that increases overall social welfare.

#3 Unfair competition to existing providers

This market failure consideration extends outward from an unnecessary distortion (or misallocation) to the risk of harm to two specific classes of agents: existing and potential private providers, and ratepayers.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

It matters whether public provision is a complement to existing providers, or a substitute. If it is a complement, then we can claim that municipal WiFi is a positive externality that benefits private providers. But if it is a substitute, then it is in competition. This is an empirical question, and it depends upon consumer and citizen behaviour but, to the extent that existing consumers' decisions about which café or hotel to choose depends upon their provision of WiFi, then public WiFi is in competition with those that already do provide it, and a subsidy for those that already do not. This will be distortionary, harming those who have already invested in the service, but benefiting those who have not. Furthermore, this will reduce the positive externality from the private provision of that service. Public WiFi could run into problems with competition policy, and indeed has in North America and Europe in particular.

Second, municipal WiFi networks involve substantial upfront and ongoing maintenance costs. Ratepayers are at risk of these cost overruns, and also to a raft of unforeseen consequences stemming from public access to the Internet. The immunity provisions for ISPs through unlawful acts (copyright infringement, objectionable content, and so forth) by third parties do not necessarily extend to WiFi hotspots, placing providers at risk of criminal liability. The economic point here is that there is substantial uncertainty associated with these risks, and without the private protection of limited liability.

#4 Public good doesn't necessarily mean public provision

A fourth stock objection flowing from standard economic theory to the prospect of public WiFi is that even if we can establish a natural monopoly, a positive externality or a market failure argument, and show that there is no crowding out or destruction of private capital, it does not follow that public provision (or intervention on the supply side) is necessarily the best option. We may still have a case for public payment through ratepayer fees, poll-taxes (or some manner of citizen levy), or property taxes, without then arriving at the conclusion that these need to be publicly supplied, operated or contracted. This point seems to have been missed in most of the public analysis, even when an ownership/operation distinction is made (e.g. Bar and Park 2006).

The real choice is not between the different models of public ownership, operation and delivery (public utility, hosted service, public overlay, wholesale, franchise, wholesale open platform, common carrier, organic mesh, etc.) but rather between whether this intervention takes place on the supply side or the demand side of the market. The case advanced by most proponents of municipal WiFi is predicated on a supply-side intervention, but standard economic theory suggests that it would be better done on the demand side. This would be WiFi vouchers, allocated to citizens or denizens or those travelling through. The analogous concept is school vouchers.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

Demand side funding has two major advantages. First, it minimizes distortions to the existing market by enabling consumers to choose themselves what particular bundles and configurations they want. This should also maximize consumer surplus. The second benefit is that it furnishes incentives for producers to provide consumers what they want, thus leading to efficient maintenance and bundling without harming innovation and adoption of new technologies. None of these benefits accrue to the supply side model, which will require significant oversight reporting to ensure accountability and transparency, and will be prone to cost blow-outs (as is common in any model where capital and operations are paid for by a third-party, not the consumer). In short, the supply-side model of provision (whether by operation or third-party contracting) loses all the benefits of a market mechanism.

The economic case for public WiFi: demand uncertainty

So, those are the basic economic reasons to be skeptical of municipal public WiFi. However, there is at least one good reason to support public WiFi, in the sense of a genuine market failure/public good, but it is an argument that so far as I am aware has not been made.

In essence, it is that WiFi is an experimental technology in each municipal location with substantial entrepreneurial uncertainties. This, specifically, is the market failure, and it accrues not to consumers (most consumers know how to use WiFi, or understand how they benefit for specific uses), nor on the technology side (engineers mostly know what to expect, and what capabilities the technology has) but to entrepreneurs in figuring out new applications of WiFi to create new businesses or business models. This is demand uncertainty, and it is a genuine market failure that is not associated with the technology in general but with its application in a particular municipal location in the context of the mix of other businesses, resources and markets.

The market failure is in figuring out entrepreneurial opportunities, market demand, business models, and so forth that are niche and contingent to particular places and times (Rodrik 2004, Bakhshi et al 2011). These are a market failure because, in a competitive market, firms will not have the rents (supernormal profits created by imperfect competition) to explore and discover where these opportunities lie, but worse, what they do discover is easily copied and appropriated by imitators who do not carry the costs associated with that experimentation. There is therefore a legitimate role for public sector support for an experimental test bed in discovering these opportunities.

The implication however is that public provision of municipal WiFi is not about providing an ongoing utility (or something sufficiently permanent that it will impact on rents and property prices, see objection #1) but a temporary underwriting of an experiment to test consumer behaviour and investment in innovative new uses or opportunities that might then be

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.20

subsequently taken up by private businesses. This is also not about adding value to public enterprises (such as airports and public transport, or even city branding) but about underwriting a discovery process that yields market information about entrepreneurial opportunities as a public good.

Conclusion

There are many reasons to support public provision of municipal WiFi, but few of these are found in basic economic analysis. Municipal WiFi is not a natural monopoly, it is not subject to market failure; public provision would likely distort existing markets and devalue existing investments. Furthermore, a better solution to proceed with public WiFi is to intervene on the demand side (through vouchers, for instance).

However, a case can be made for clear market failure resolved through public provision of WiFi in terms of demand uncertainty affecting entrepreneurs. The reason is that this information about opportunities is actually a pure public good, and its provision is likely to be welfare enhancing in maximizing the rate and scope of innovation in relation to the WiFi technology in the particular municipal location. (This includes information about what is unlikely to work, and thus minimizing wasted investments.)

Putting these arguments together, one can discern two main justifications for public WiFi provision, depending on the particular circumstances of the municipality involved:

1. Where there is already, or is likely to be, adequate wireless access available from competitive sources, then an intervention to stimulate WiFi use by a municipality, if justified, should be on the supply side: that is, temporary vouchers to make WiFi affordable. This is likely to be the best practice municipal WiFi intervention in many cases.

2. Where there is a likelihood that the provision of public WiFi would lead to entrepreneurial activity that will identify value-enhancing opportunities in the municipality, then a case can be made for demand-side intervention: that is, the provision of classical public WiFi networks.

References

Bakhshi, Hasan; Freeman, Alan; Potts, Jason. 2011. 'State of uncertainty' Nesta Provocation. Available at: http://www.nesta.org.uk/publications/state-uncertainty

Bar, Francois; Park, Namkee. 2006. 'Municipal WiFi Networks: the goals, practices and policy implications of the US Case' *Communications and Strategy* 61(1): 107–27.

Benkler, Yochai. 2002. 'Some economics of wireless communications' *Harvard Journal of Law & Technology*, 16(1): 25-83.

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n1.20

Buchanan, James. 1965. 'An economic theory of clubs' *Economica*, 32: 1–14. http://dx.doi.org/10.2307/2552442

Caplan, Bryan. 2001 'Standing Tiebout on his head: Tax capitalization and the monopoly power of local governments' *Public Choice*, 108: 101–22. http://dx.doi.org/10.1023/A:1017564623294

Cohen, Sarah. 2007. 'Monetizing municipal wireless networks' Forrester Research. (For purchase at: www.forrester.com/Monetizing+Municipal+Wireless+Networks/fulltext/-/E-RES42418)

Economides, Nicholas. 2005. 'The Economics of the Internet Backbone' *Handbook of Telecommunications*. I. Vogelsang (ed) Amsterdam: Elsevier.

Economist. 2013. Babbage Column (26th July) 'Whatever happened to municipal WiFi?' Available at: http://www.economist.com/blogs/babbage/2013/07/wireless-networks

Fraser, Eric. 2009. 'The Failure of Public WiFi' *Journal of Technology Law & Policy*, 14(2): 161–78.

Jassem, Harvey. 2010. 'Municipal wifi: the coda' *Journal of Urban Technology* 17(2) 3–20. http://dx.doi.org/10.1080/10630732.2010.515090

Lehr, William; McKnight, Lee. 2003. 'Wireless Internet access: 3G vs. Wi-Fi? *Telecommunications Policy* 27: 351–70. http://dx.doi.org/10.1016/S0308-5961(03)00004-1

Olson, Mancur. 1971. *The Logic of Collective Action*. Harvard University Press. Cambridge, MA.

Qiu, Laingfei; Rui, Huaxia; Whinston, Andrew. 2013. 'Hotspot Economics: Procurement of Third-Party WiFi Capacity for Smart Mobile Data Offloading' Available at: http://www.utexas.edu/cola/_files/ms37643/cellular_offloading.pdf

Rodrik, Dani. 2004. 'Industrial policy for the 21st century' Available at: http://www.hks.harvard.edu/fs/drodrik/Research%20papers/UNIDOSep.pdf

Shy, Oz. 2001. *The Economics of Network Industries*. Boston: MIT Press. http://dx.doi.org/10.1017/CBO9780511754401

Travis, Hannibal. 2006. 'Wi-Fi Everywhere: Universal Broadband Access as Antitrust and Telecommunications Policy" *American University Law Review* 55(6): 1697–1800.

Wu, Timothy. 2007. 'Where's my free wifi? Why municipal wireless networks have been such a flop' Slate Magazine, http://www.slate.com/articles/technology/technology/2007/09/wheres_my_free_wifi.html

Yaiparoj, Saravot; Harmantzis, Fotios; Gunasekuran, Vinoth. 2008. 'On the economics of GPRS networks with Wi-Fi integration' *European Journal of Operational Research*, 187(3): 1459–75. http://dx.doi.org/10.1016/j.ejor.2006.09.025

Cite this article as: Potts, Jason. 2014. 'Economics of public WiFi'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 20.1-20.9. DOI: http://doi.org/10.7790/ajtde.v2n1.20. Available from: http://telsoc.org/journal

TransACT's foundation and initial rollout

A memoir

Robin Eckermann
Principal, Robin Eckermann & Associates
Adjunct Professor, University of Canberra

TransACT (2000-) introduced Australia's first VDSL network, offering a 'triple play' of voice, data (e.g. Internet access), broadcast and video-on-demand services in Australia's capital city, Canberra, in competition with the incumbent carrier Telstra. TransACT's founding Chief Architect, Robin Eckermann, reminisces on the founding of TransACT and some of the lessons to be learned from this fore-runner of the National Broadband Network (NBN).

Introduction

TransACT was a pioneering network by many measures. The deployment that began in 2000 after a four-year incubation period was one of the first to implement open access principles with the structural separation of local access and services. It took fibre deep into the access network, within 300m of the end-user, in a fibre-to-the-kerb (FTTK) architecture. It was the first network in the world to deploy VDSL technology (with a raw speed of 51.84 Mbps), enabling support of a triple play suite of services including broadcast-quality video. Fourteen years later, with the network now owned by iiNet (ASX: IIN), the original electronics are being replaced by VDSL2, enabling speeds of 100 Mbps over the original cabling. Many Australians can only hope that the NBN will provide similar capabilities in their areas over the next ten years.

It was one of the highlights of my professional career to lead the creation of TransACT, with hands-on involvement in every aspect - designing the architecture, selecting the technology, developing the business models, defining the products and raising the investment needed to proceed. My role began in 1996 as Project Leader (on a consulting basis to ACTEW, the ACT Electricity and Water Authority) and in 2000 I took up a full-time position with company and served as Chief Architect during the rollout from 2000 to 2003.

The Beginnings of TransACT

For me, the story began when I had my first exposure to broadband in 1994 – long before the advent of ADSL. I had the overwhelming sense that what I was seeing would transform the world. Coupled with a visit to CeBIT where I saw robots for laying fibres in sewers, I came

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.24

back inspired with possibilities and shared my excitement with a long-standing client within ACTEW. That led to an invitation to present to a team of ACTEW executives in November 1995. Unfortunately project "TENPARC" (as we dubbed a plan to run fibre through the sewers) wasn't an instant winner and I thought that would be the end of the idea.

Fortunately, there was another initiative brewing in the background. A small team engaged in a management development program was looking at an electricity reticulation technology called Aerial Bundled Conductors (ABC). Rather than spreading bare conductors on the cross-arm of a power pole, the conductors were insulated and twisted together into a single bundle to improve immunity to interference from vegetation. They found that ABC cabling could include an optical fibre cable – but their project ran to its conclusion in late 1995 before being really able to explore the communications possibilities that this might enable.

A new management development team commenced in early 1996, around the same time that Australia's Pay TV rollouts were running full-steam ahead. Although Telstra and Optus were engaged in a race to establish coverage in the major population centres like Sydney and Melbourne, both approached ACTEW wanting to secure the rights to string their cables on the utility's power poles within the Australian Capital Territory. However, neither was in a rush to actually start building in Canberra due to its smaller market size and the fact that electricity lines ran through back-yards with no access except by foot and ladder. This “rear spine” electricity network architecture was part of Walter Burley Griffin’s design for Canberra to avoid cluttering street-scapes with power poles.

It was around this time that my earlier presentation was remembered, and I was invited to share some perspectives as to where the industry was heading with the three key members of the management development program - Joe Ceccato, Rob Clarke (both electrical engineers) and Jane Taylor (a librarian). A few weeks later, I was engaged by ACTEW and the four of us became fully consumed by the thinking that culminated in TransACT's establishment a few years later.

The initial question centred on whether to allocate pole access rights to Telstra, Optus or both. Each wanted the upper position on the pole - but it was clear that the poles couldn't support *two* additional sets of cabling for reasons of weight and/or clearance (not to mention the public outcry that would have ensued at such unsightliness).

Resolving that there could only be one set of cabling led to a series of questions that ultimately shaped the whole TransACT architecture. If ACTEW was to grant access to one party only, should it insist that they use its workforce to generate employment as well as to maintain tight control over the electricity assets? Or should ACTEW go further and build

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.24

and own the cabling, making it available to both Telstra and Optus on some form of open access basis?

A single set of cabling shared by multiple parties seemed to promise the best outcome economically, aesthetically and for customers (in terms of choice of services). Thus the concept of an open network became a key pillar of the TransACT vision.

The initial leaning was to own the cables only, but it soon became apparent that electronics would be needed to convert passive wires into a network capable of supporting multiple services (including video services) and service providers. We invited proposals, and the choice quickly netted down to either one of several Hybrid Fibre Coaxial (HFC) solutions or a unique FTTK/VDSL solution - in either case, deploying an entirely new cabling regime. Whilst we recognised the proven capabilities of HFC for video delivery, ultimately we saw broadband data as the primary service of the future. Accordingly we opted for the FTTK/VDSL approach in the belief that the dedicated copper "tails" would give superior broadband performance as well as supporting a high-quality conventional POTS service.

Our initial goal was to avoid venturing into the services space, so we embarked on discussions with prospective partners who could provide ISP and telephony services, subscription TV services and video-on-demand services. In the telephony area, we came close to consummating deals with each of two major carriers. However, it became clearer that their view of sharing risk and reward was that we take the risk (with the massive investment involved in a cabling deployment) and they take the rewards (with lucrative telephony revenue). It also would have largely put TransACT's fate in the hands of the partner who owned telephony switch and risked reducing TransACT's asset to little more than a tangle of wires.

From Concept to a Working Pilot

During all of these negotiations, the network solution had progressed from loose concepts (often sketched out on paper napkins at the local coffee shop) to a laboratory-based proof-of-concept configuration. In mid-1998, ACTEW's Board approved a $6m budget to embark on the next stage and test the solution by deploying the network in one of Canberra suburbs. The ACT Chief Minister was booked to launch the initiative at the end of November, and that set a 4 month timer ticking on building a network head-end at a new site, extending optical fibre cable some 7 kms to the pilot area, running a complex cabling architecture past some 850 homes and establishing a credible suite of services.

There was no longer time to pursue a deal with a telephony provider, so we bit the bullet and purchased a Class 5 telephony switch. Several ISPs came on board, and we were able to

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.24

secure partners to provide a range of broadcast video channels as well as some video-on-demand content.

Few people will know just how hard the team pedalled during that four-month period, and there are many entertaining anecdotes from the era. The story of how we came to get planning approval is an example of venturing into territory that was as unknown to us as it was to the planning authorities. We simply joined the queue of builders with garage plans etc under their arms, and when we got to the front of the queue, unrolled a map of the pilot suburb showing all the proposed cabling. There was some nervous shuffling on the other side of the counter, then a consultation with a supervisor – but in the end we secured the necessary approvals for the same $60 fee as applied to housing extensions and other minor building works.

The launch was a great success – and the demonstrations of multi-megabit speeds, at a time when dial-up was the norm, drew an audible gasp from those attending. From a personal viewpoint, one of the great team triumphs was delivering what many others saw as a "mission impossible" on time and a few thousand dollars *under* budget.

From Pilot to Deployment

Following on from the successful pilot, TransACT started its quest to attract the investment needed to progress to a large-scale rollout. With the assistance of a merchant banker, the initial investors signed up, led by Telecommunications Venture Group (TVG) from Hong Kong and ACTEW. Their confidence triggered a scramble to get a stake in the venture, and ultimately it proved necessary to cap the funds it took on board. What a stark contrast to the mood that set in just a few months later, from April 2000, when the technology bubble burst. TransACT was formally established as a company in 2000, and the first CEO – the late Richard Vincent – took up his role in March.

The network rollout proceeded over the subsequent three-and-a-half years, ultimately passing some 65,000 premises and representing an investment of the order of a quarter of a billion dollars. The original FTTK/VDSL network was augmented with ULL/ADSL access to the "other half" of Canberra that fell outside the FTTK footprint. In greenfield areas, TransACT became one of the pioneers of fibre-to-the-premises (FTTP) in Australia and the first to deploy GPON technology (the same technology to be chosen many years later by NBN Co for its FTTP deployment).

The TransACT business was acquired by iiNet in late 2011, and the FTTP areas have since been acquired by NBN Co. In addition to serving tens of thousands of residential customers, TransACT has built a successful business meeting the specialised and high-performance

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.24

needs of major government and corporate users - including offering high quality data-centre space.

Lessons Learned

There were lots of lessons in the TransACT experience. We made our share of mistakes – indeed, they represent some of the most valuable lessons learned, and it always disappoints me when I see others reinventing the same mistakes for themselves! However, we got some important things right:

1. Good people and good teamwork are the keys to great outcomes. If I had been asked to pick my team at the outset of the TransACT adventure, I probably wouldn't have picked all the individuals that I inherited as team leader. However, looking back at the end of the journey, I don't think we could have succeeded with any lesser team. During the course of growth the occasional misfit found their way into the group – but they were quickly ejected by the rest of the team. Individual egos, ambitions and politics get in the way of the collective mission and must be quickly excised if they are not to undermine progress.

2. A clear vision inspires people and enables them to power through the tough times. Being attacked by sceptics ("You're crazy thinking you can do this") is healthy – it tests, refines and strengthens the vision until ultimately it becomes robust enough to withstand the most aggressive pressure. And for some of us, there is no greater motivator than being told that something in which you believe cannot be done!

3. Capturing the order of a third of the fixed line telecommunications market in TransACT's network footprint within a year of turning on services was a measure of tremendous public acceptance. Considering the strengths and resources of the incumbent, this was a real David versus Goliath accomplishment and something that few other telecommunication start-ups anywhere in the world have been able to match.

4. Open access is the right approach in areas where duplication of infrastructure simply doesn't make sense. If a single advanced network is capable of supporting an unlimited array of services and service providers, it makes no more sense to build multiple networks than it would to deploy a second set of power-poles to get competition into the supply of electricity. TransACT's implementation of open access involved the structural separation of local access (retailed directly by TransACT to the end-user) and services (available from a range of retail service providers (RSPs)). This avoided the inherent duplicate charging that occurs – for example, under the wholesale/retail approach that NBN Co has adopted – where each RSP that an end-user engages must pay the network owner/operator for another full access line and

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.24

recover this in their retail charges. TransACT's approach was cost-reflective in that the end-user paid the line rental costs only once, and each additional RSP only paid a marginal fee for access to the customer.

5. Punting on the growth of broadband (rather than prioritorising video services) was a good decision. At the time of TransACT's commencement, Internet access for most homes involved dial-up connections layered on top of the phone service. This is totally inverted today, with broadband data rapidly becoming the "foundation service", and both telephony and video services being increasing layered on top of it.

6. The deep fibre plus high-quality "Cat5" copper cabling regime has proven its long-term worth. Electronics come and go, but cabling is the durable asset in any network. The original FTTK/VDSL network has already been partially upgraded with VDSL2 technology, and speeds of 30-100 Mbps are now available to all customers in the original network footprint. For just a few million dollars (a tiny fraction of the hundreds of millions that would need to be spent in over-building new FTTP infrastructure), the network can be further upgraded with VDSL2 throughout – making speeds of 100 Mbps available to all users. Further, when the time comes, there's enough fibre in the network to migrate to an FTTP architecture simply by upgrading the last 300m – again at a fraction of the cost of a total rebuild.

Conclusions

Unquestionably, it was a unique set of conditions that prevailed back at the time TransACT originated.

Some were largely coincidental – relating to the particular activities in which I and some other folk at ACTEW were engaged at the time and to the personalities of a team of individuals who weren't constrained by traditional thinking.

Others related more to the general environment of Canberra back in the mid-1990s. Canberra's economy is information/knowledge-centric, and its population are amongst the most highly educated in Australia. Households led the country in their uptake of personal computers and their use of the Internet – so there was no better market in Australia to pioneer an advanced broadband network. ACTEW had a sound platform from which to venture into telecommunications – not just its own electricity poles and wires, but a workforce used to operating critical infrastructure, a multi-utility business (electricity, water, sewerage and gas), a 100% customer-base and an entrepreneurial CEO. All it needed was the spark of approaches from the companies engaged in Pay TV rollouts to ignite this melting pot of potential.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.24

The years leading TransACT's establishment were the most demanding in my professional career, with the routine 12-hour days, 6 days a week, taking a toll on other family priorities and a healthy, balanced lifestyle. However, when I look back and ask myself if it was all worthwhile, the answer is a resounding "Absolutely!"

Acknowledgements

Needless to say, projects like TransACT are never the result of any individual person's efforts, and I want to pay tribute to the outstanding team of colleagues with whom I had the privilege of working. It would also be remiss of me not to particularly acknowledge the role that Mike Sargent (CEO of ACTEW, the ACT Electricity and Water authority at the time TransACT commenced) and Neville Smith (Business Development Director) played. Mike "got" the vision and gave TransACT the initial space to take root; Neville "flew cover" for the project – insulating the team from the distractions of corporate politics so that it could get on with the challenge at hand.

Cite this article as: Eckermann, Robin. 2014. 'TransACT's foundation and initial rollout: A memoir'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 24.1-24.7. DOI: http://doi.org/10.7790/ajtde.v2n1.24. Available from: http://telsoc.org/journal