COMMUNICATIONS
ALLIANCE LTD

PUBLIC WI-FI NETWORKS
INDUSTRY INFORMATION PAPER

MAY 2012

Public Wi-Fi Networks Information Paper

First published in 2012

Communications Alliance Ltd (formerly Australian Communications Industry Forum Ltd) was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1) Notwithstanding anything contained in this Information Paper :

   a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

      i) reliance on or compliance with this Information Paper ;

      ii) inaccuracy or inappropriateness of this Information Paper ; or

      iii) inconsistency of this Information Paper with any law; and

   b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Information Paper .

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

INTRODUCTORY STATEMENT

The proliferation of 'smart' mobile handsets, tablet computers and always-connected applications has contributed to what is being billed the "Mobile Data Explosion"; a phenomenon seen throughout the developed world and front of mind for most telecommunications carriers as they prepare their networks and growth strategies to meet the challenge and best harness this transformation of the mobile environment.

Public Wi-Fi networks have long been available throughout office environments and public areas such as airports and shopping centres for use as either a free or commercial service for mobile workers, travellers and shoppers, and appear likely to play a larger role in the national 'connectivity matrix' in years to come. The technical, regulatory and planning guidelines for Public Wi-Fi networks are, however, not as well defined in Australia as they are for mobile networks.

Hence the purpose of this document is to provide:

- an overview of the current state of the Public Wi-Fi industry in Australia;
- its current working methods/context, future development direction; and
- the technology and regulatory aspects that need to be considered when planning a Public Wi-Fi deployment in Australia.

Communications Alliance is also interested in feedback and guidance from broader industry and community stakeholders as to what additional issues, deployment options and industry coordination might be required in the future for the successful and coordinated operation of Public Wi-Fi networks throughout Australia.

Rob Haylock
Chair
Public Wi-Fi Networks Group

MAY 2012

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

1.1.1 The development of the information paper has been facilitated by Communications Alliance through a working group comprised of representatives from the telecommunications industry.

1.1.2 This document has been prepared as part of discussion among Communications Alliance members about aspects of public Wi-Fi networks.

1.1.3 The information paper should be read in the context of other relevant Telecommunications industry codes, standards guidelines and other documents.

1.1.4 The information paper should be read in conjunction with related legislation, including:

(a) the *Telecommunications Act 1997 (Cth)* (the Act);

(b) the *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)*;

(c) the *Competition and Consumer Act 2010 (Cth);*

(d) the *Privacy Act 1988 (Cth)*.

(e) *Telecommunications (Interception and Access) Act 1979 (Cth); and*

(f) *the Radiocommunications Act 1992 (Cth)*

1.1.5 This is an information paper and as such does not establish any compliance requirements for existing or new Wi-Fi network operators. The paper does provide a high level overview on a number of issues including regulatory and legal settings. If there is a conflict between the requirements outlined in this information paper and any requirements imposed on a Wi-Fi network operator or CSP by statute, the requirements of those statute documents will take precedence.

1.1.6 Compliance with this information paper does not guarantee compliance with any legislation. The information paper is not a substitute for legal advice.

1.1.7 Statements in boxed text are a guide to interpretation only.

1.2 Scope

1.2.1 The information paper is relevant to:

(a) Carriers;

(b) Carriage Service Providers; and

(c) other entities considering establishing or operating a public Wi-Fi network in Australia.

1.2.2 The information paper deals with the following telecommunications activities:

(a) carrying on business as a Carrier; or

(b) carrying on business activities as a Carriage Service Provider; or

(c) supplying Goods or Service(s) for use in connection with the supply of a Listed Carriage Service.

1.2.3 This information paper does not address in detail matters for bilateral commercial agreement.

NOTE: By their nature bilateral matters are specific to the two parties involved in such an agreement.

1.3 Objectives

1.3.1 The objectives of the information paper are to provide a high level overview of the following aspects of public Wi-Fi networks in Australia:

(a) Legal and regulatory obligations;

(b) Technical requirements;

(c) Commercial models; and

(d) End user issues.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the information paper:

ACMA

means the Australian Communications and Media Authority.

AP

means Access Point.

CSP

means Carriage Service Provider.

EAP-AKA

means Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement

EAP-FAST

means Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling

EAP-SIM

means Extensible Authentication Protocol Method for GSM Subscriber Identity Module

EAP-TLS

means Extensible Authentication Protocol Transport Layer Security

GAS

means Generic Advertisement Service

IEEE

means the Institute of Electrical and Electronic Engineers.

ISP

means Internet Service Provider.

LEA

means Law Enforcement Agency

MAC

means Media Access Control.

QoS

means Quality of Service

SIM

means Subscriber Identity Module

SSID

means Service Set Identifier

WBA

means the Wireless Broadband Alliance.

WPA2

means Wi-Fi Protected Access II

2.2 Definitions

For the purposes of the information paper:

Act

means the *Telecommunications Act 1997 (Cth)*.

Carriage Service Provider

has the meaning given by section 87 of the Act.

Carrier

has the meaning given by section 7 of the Act.

Intercell Hand-Over Functions

has the meaning given by section 33 of the Act.

Public Mobile Telecommunications Service

has the meaning given by section 32 of the Act.

Subscriber Identity Module (SIM)

means a physically removable module which is used in the authentication procedures and contains the subscriber identity as well as other subscriber data.

2.3 Interpretations

In the information paper, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(c) words in the singular includes the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included;

(g) words and expressions which are not defined have the meanings given to them in the Act; and

(h) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees.

3 REGULATORY ENVIRONMENT

Public Wi-Fi networks in Australia generally facilitate access between a carrier network and end-user devices, providing a small boundary network of coverage and convenience either within a building, or a limited public area (e.g. park, stadium, shopping mall). This means that regulatory aspects affecting Public Wi-Fi are sometimes unclear or misunderstood. The following provides a summary of the current situation regarding the regulation of Public Wi-Fi networks in Australia.

3.1 Existing legislation provides structure

3.1.1 The *Telecommunications Act 1997* (the Act) requires a carrier license for network carriage to the public. Since a Wi-Fi access link will be a 'network unit' under the (broad) definition in the Act then anyone operating a Wi-Fi network needs to assess their potential for incurring legal obligations as a carrier.

3.1.2 If someone is offering a service to the public over a Wi-Fi link then that service would be a 'carriage service' as defined in the Act and would mean the person providing the service would be captured by the definition of a 'Carriage Service Provider' (CSP) making that person subject to the requirements on a CSP in the Act.

3.1.3 While obligations on CSPs tend to be less onerous than on carriers, they are another potential area of regulatory obligation to be assessed if one offers Wi-Fi services.

3.2 Technical regulation complements the legislation

3.2.1 The Australian Communications and Media Authority (ACMA) regulates the use of radiocommunications spectrum in Australia. Information on regulatory arrangements for public spectrum is available from the ACMA website.

3.2.2 For example, the ACMA webpage *Wireless LANs – design and security fact sheet* points to information including the regulation of spectrum for Wi-Fi networks by the *Radiocommunications (Low Interference Potential Devices) Class Licence 2000*.

3.2.3 The ACMA website also has a number of other pieces of information on the regulation and use of Wi-Fi networks, including the:

(a) ACMA information paper on *Low interference potential devices;*

(b) Webpage *Wireless LANs in the 2.4 GHz band FAQs* including "*How do I know if I need a carrier licence?*"; and

(c) *Wireless LANs – what and how fact sheet*.

3.2.4 Refer to the References section at the end of this document for URLs of these ACMA publications.

3.3 However there is some flexibility for the operation of Wi-Fi services

3.3.1 When Wi-Fi emerged as an alternative wireless access technology to mobile telephony networks the Minister for Communications, Information Technology and the Arts determined (in September 2002) under section 51 of the Act to exempt wireless networks from the need to be licensed in certain circumstances where a fixed line network providing the same service would not require a carrier licence.

3.3.2 In line with this determination[1], wireless equipment used to supply communication services to the public on a single premises (such as an internet cafe, an area of a shopping centre, an airport lounge, hotel or conference centre) does not require a carrier licence where the service is not to be re-transmitted by radiocommunications to another property.[2]

3.3.3 So the ministerial determination allows for some exemptions but apart from these exemptions the operation of Wi-Fi equipment would require a carrier license.

3.3.4 The Act allows up to 500m of cabling for a 'network unit' before one requires a carrier license. So if the range of a Wi-Fi network does not exceed the equivalent of 500m of fixed network cabling then there may be an argument the network does not require a carrier license. A final position would need to be determined having regard to the different circumstances applying in each case.

3.3.5 Another potential allowance arises from legislation of a fixed wireless and 'terrestrial radio customer access network' which has allowance for use on a non-commercial service without a carrier license e.g. on a single factory floor.

3.4 'Handover' under the Telecommunications Act

3.4.1 Complexities arise from referring to 'handover' between wireless networks, as defined for a Public Mobile Telecommunications Service. For example, a Wi-Fi network is fixed wireless network.

3.4.2 However the term 'handover', or "Intercell Hand-Over Functions" in the Act, has its origins in the handing over of a voice telephony call between cells of the same mobile network, which was an assumption in the legislative drafting process at the time.

3.4.3 Note that 'handover' is defined for handover between cells on 'a network' (i.e. singular) and not 'between networks'.

3.4.4 This contrasts with a device changing network connectivity from one network to another (for example 'roaming' between mobile

[1] http://www.comlaw.gov.au/Series/F2004B00444

[2] Source: http://www.acma.gov.au/WEB/STANDARD/313429/pc=PC_1778

networks) which is quite different to handover from one 'cell' to another.

3.5 Emergency Calling

3.5.1 A number of regulatory arrangements exist around the provision of an emergency calling capability.

3.5.2 For example, a carrier has a responsibility for users of the network to be able to make emergency calls.

3.5.3 A service provider obligation to support emergency calling arises with the supply of a standard telephone service.

NOTE: There is an argument that the supply of a 'data only' service over a private network (e.g. by a system integrator) would not have an obligation to support emergency calling.

3.5.4 Issues arise under the *Telecommunications (Emergency Call Service) Determination 2009* as to whether or not a service provider supporting telephony and using Wi-Fi is obliged to offer an emergency voice calling capability.

NOTE: The Telecommunications (Emergency Call Service) Determination has a number of obligations depending on the type of service e.g. for a 'standard telephone service', a 'location independent carriage service' or a 'public mobile telecommunications service'.

3.5.5 If a CSP is obliged to offer an 'always on' functionality for emergency calling and the power supply is interrupted, it is unclear what power back up arrangements the CSP would need to have in place.

3.5.6 As Wi-Fi networks become ubiquitous, they may become seen as complementary to traditional networks. As a result there is some potential for the associated regulatory arrangements for emergency voice calling to change over time.

3.5.7 As the usage of Wi-Fi networks grows, it is feasible that emergency voice calling will become partly a policy issue, and partly an issue of public expectations e.g. if I can make a voice call readily using Wi-Fi, should I be able to make an emergency voice call just as easily?

3.5.8 This expectation may lead to a mismatch between the technology and end user expectations e.g. Hotspot 2.0 consciously omits emergency services.

NOTE: Refer to Section 5.3 and Appendix B for more information on Hotspot 2.0, a specification for operators of Wi-Fi networks.

3.6 Location Information

3.6.1 Wi-Fi networks typically have a smaller cell size than on mobile networks that use licensed spectrum. There is usually an exchange of "venue information" between the end user device and a wireless Access Point (AP) so the granularity of location information can be better than for base station triangulation on a mobile phone network.

3.6.2 A question could then arise about the nature of location information that might be made available to emergency service organisations (ESOs) in emergency communications, its reliability (e.g. verification by a trusted network operator vs. end user assertion of location).

NOTES:

1. For example an arrangement for roaming between a Wi-Fi network and a mobile network is likely to need to address obligation such as s52A of the Telecommunications (Emergency Call Service Determination (2009). This has an obligation for "a network … used to supply a public mobile telecommunications service" to supply the "most precise mobile location information available" to parties such as emergency service organisations.

2. Refer to section 5.5 for more information on roaming arrangements between mobile and Wi-Fi networks.

3.7 Government policy

3.7.1 At the time of publication the role that Wi-Fi networks might have in the government's digital economy strategy[3] is unclear – the strategy generally does not address specific technology types.

[3] http://www.nbn.gov.au/the-vision/digitaleconomystrategy/

4 LEGAL ISSUES

NB: The information contained in this section should not be relied as legal advice. Providers and/or potential providers should obtain their own advice.

Public Wi-Fi networks in Australia share many characteristics of licensed mobile phone networks such as the ability to go online (e.g. to access websites), and then download, store and share content and the ability to record or log usage. With these characteristics come many of the questions that relate to content and interception.

4.1 Downloading of copyright material

4.1.1 Recent activity on online copyright issues has had some discussion on the use of public Wi-Fi networks however the focus of attention has been on delivery via other (e.g. licensed) networks and (e.g. ISP) services.

4.1.2 Digital rights owners have been looking to change the behaviour of end users who infringe copyright via online activities including peer-to-peer file sharing. Notwithstanding the recent judgment by the High Court of Australia in the case Roadshow Films Pty Ltd and Others v iiNet Ltd[4], pressure on users of fixed networks in this regard might continue and could be extended to mobile and/or Wi-Fi networks in future.

4.2 Downloading of prohibited content

4.2.1 Prohibited content in Australia is based on the national classification scheme[5].

4.2.2 ACMA has the regulatory power to ensure that prohibited online content is not hosted within or made available within Australia[6].

4.2.3 At present if an end user is identified as accessing prohibited content via a Wi-Fi network then the party with the legal responsibility for identifying the offender has not been tested.

4.2.4 Similarly the nature of the interaction between Wi-Fi network operators and service providers with law enforcement agencies (LEAs) has not been tested. This is in contrast to standing arrangements that exist between LEAs and both licensed carriers and CSPs.

[4] http://www.hcourt.gov.au/cases/case-s288/2011

[5] http://www.classification.gov.au/ClassificationinAustralia/Pages/default.aspx

[6] http://www.acma.gov.au/WEB/STANDARD/191065/pc=PC_90102

4.3 Legal/lawful interception

4.3.1 While legal/lawful interception can be done, the associated processes are not standardised in the way they are for tracing (phone) numbers in a licensed carrier network. Practical challenges on a public Wi-Fi network may include:

(a) Dynamic address allocation, which hampers usage tracking i.e. a different IP address is allocated per session, which can make tracking usage by IP address quite difficult.

(b) The absence of user data on a Public Wi-Fi network i.e. there is typically no user data retained on public Wi-Fi networks, unlike in licensed carrier networks.

(c) Permitting anonymous, temporary use, which can be difficult to trace after the event.

4.3.2 There are recent examples of Wi-Fi network operators assisting LEAs resulting in the relevant LEA matching different information sources to identify a suspect e.g. the use of an IP address combined with CCTV footage at a related site.

4.4 Handover between networks

4.4.1 Apart from being good business practice to protect commercial interests, it is important that parties operating services on Wi-Fi networks have in place clear understandings about the boundaries of responsibility, such as:

(a) arrangements that define handover between Wi-Fi and other wireless networks;

(b) processes for the handover of sessions between networks (e.g. 'hard' or 'soft' handover);

(c) agreements about the notification(s) given to a customer when handing over (e.g. warning that roaming charges may apply); and

(d) agreements about who has the responsibility to provide secure access to the network (e.g. provision of encryption options).

5 TECHNICAL

Public Wi-Fi networks operate on the IEEE 802.11™ family of standards and specifications which defines wireless connectivity protocols with fixed, portable or moving devices in local area. This section has information on both the accepted and emerging standards that support the development of next generation Public Wi-Fi networks.

5.1 Public Wi-Fi Network Architecture

5.1.1 A typical Public Wi-Fi network architecture consists of a single Wireless AP or multiple APs, a Wireless LAN controller, a LAN Switch, a gateway, and a router to connect to the internet.

5.1.2 Some Public Wi-Fi networks may restrict access and only allow authorised users and this will require additional authentication function either through a simple Service Set Identifier (SSID) password entry or through a more sophisticated authentication process requiring dedicated authentication server and captive web portal where users are redirected to a landing page.

5.2 Emerging Wi-Fi Standards – IEEE 802.11u protocol

5.2.1 Current Public Wi-Fi networks suffer from the inconvenience of manually typing the username/password to be authenticated before accessing the internet. This is especially true when typing onto the small smartphones screen. IEEE 802.11u aims to simplify the authentication and authorisation process for Wi-Fi access and will play a critical role to automate the login process for user connecting to Wi-Fi networks.

5.2.2 802.11u enables Public Wi-Fi networks to advertise their capabilities and then allow devices to connect to them automatically rather than requiring the end user to manually select the available wireless network.

5.2.3 For the automated login process to work, both the wireless device and the Wireless AP must support 802.11u standard.

5.3 Emerging Wi-Fi Industry Certification – HotSpot 2.0

5.3.1 In 2010, the Wi-Fi Alliance group formed a certification process of ensuring mobile devices and wireless APs comply with the new Hotspot 2.0 industry certification. The goal of the Hotspot 2.0 was to define a common set of standards that would bring a 3G-like end-user experience to Wi-Fi Authentication.

5.3.2 The key driver for introducing HotSpot 2.0 were:

(a) Growing mobile (smartphone) data demand that is leading to congesting of cellular networks.

(b) The economic benefits of offloading mobile data from cellular to Wi-Fi.

(c) Solving the usability problems of today's Public Wi-Fi by handset devices automatically authenticating with Wireless APs though the IEEE 802.11u standard.

(d) Addressing the security threats exposed in the current Public Wi-Fi networks.

5.4 Emerging Wi-Fi Industry Certification – Wi-Fi Certified PassPoint™

5.4.1 As part of the Hotspot 2.0 process, Wi-Fi Alliance recently introduced Wi-Fi Certified PassPoint[7] program ensuring both manufacturers of mobile devices and Wi-Fi network equipment vendors comply with the IEEE 802.11u standard.

5.4.2 The specification of Wi-Fi Certified PassPoint defines the following features:

(a) *Network discovery and selection:* Devices identify and associate with Passpoint networks in the background, without any active intervention from the subscriber.

(b) *Seamless network access*: Authentication no longer requires a browser-based sign-on or the subscriber to enter a password. Devices are authenticated automatically, using Extensible Authentication Protocols (EAP) based on a SIM, a username and password, or certificate credentials.

(c) *Secure authentication and connectivity:* All connections are secured with WPA2™- Enterprise, which provides a level of security comparable to that of cellular networks.

5.5 Security Encryption via WPA2

5.5.1 The Wi-Fi Protected Access II (WPA2) protocol, widely available for IEEE 802.11 implementations, is used for encryption to secure wireless links.

5.5.2 It was based on IEEE 802.11i-2004 which was subsequently incorporated into the IEEE 802.11-2007 standard.

5.5.3 WPA2 is the *de facto* standard for securing Wi-Fi networks, however in order to allow easy connection, most public Wi-Fi networks operate unsecured, instead relying on the end-user or an application to secure any sensitive data (such as through the use of an IPsec, VPN or SSL connection (HTTPS).

5.5.4 IEEE 802.11u may also enable easier use of WPA2 encryption on Public networks.

5.5.5 Note that WPA2 does not provide individual connection encryption, but that all terminals on the same Wi-Fi SSID and WPA2 key can see all information of other users on the same

[7] http://www.wi-fi.org/passpoint

network. This is why the use of VPN or SSL end point encryption is recommended.

5.6 Security – Encryption via other methods

5.6.1 WPA2 encryption is satisfactory for many purposes e.g. in enterprises, for Hotspot 2.0.

5.6.2 WPA2 uses 256 bit encryption, which reduces the potential for sniffing.

5.6.3 However the use of WPA2 involves use of a shared key, which means other users on the same Wi-Fi network key are more able see the network traffic than on a link with a unique key.

5.6.4 Alternatives to WPA2 for authentication and encryption to improve security for Wi-Fi networks include:

(a) IEEE 802.1X, which uses encryption and tunnelling, operating at the Ethernet layer;

(b) The use of higher layer security (e.g. IPsec, which is subject to ongoing debate on whether or not to implement it);

(c) The use of SIM level authentication; and

(d) Technology for 'per device' encryption e.g. the use of a unique key based on the hardware MAC address.

5.7 Authentication methods

5.7.1 The introduction of IEEE 802.11u overcomes the need for a user to enter a password. A profile is stored on the device so that authentication and network selection occurs in the background.

5.7.2 Once a user has the relevant profile established for network access then it becomes easier to manage access to multiple Wi-Fi networks where there might be a number of networks available e.g. for networks deployed in a shopping centre, stadium, etc. by carriers, site owners and retail outlets.

5.7.3 This is facilitated by the Generic Advertisement Service (GAS) which operates on 'layer 2', and keeps communicating in the background to allow seamless authentication.

5.7.4 Four methods for authenticating a device on a Wi-Fi network are:

(a) **on a GSM network using a SIM card**
(using Extensible Authentication Protocol Method for GSM Subscriber Identity Module or EAP-SIM)
EAP-SIM requires support on both a mobile device and an AP in a similar way to IEEE 802.11u requiring support on both sides of the air interface. Similarly this requires support from carriers and device suppliers as well.

(b) **on a UMTS network**
(using Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement or EAP-AKA).

(c) **on a CDMA network**
(username and password, X.509 certification (using Extensible Authentication Protocol Transport Layer Security or EAP-TLS).

NOTE: CDMA network technology is not used in Australia.

(d) **Use of the Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling or EAP-FAST**
where a user types in username and password.

5.7.5 Two methods to facilitate authentication are either:

(a) A Wi-Fi network operator pushes a policy 'over the air' to devices that connect to its network; or

(b) An end user downloads an app (e.g. an Android app for a large Wi-Fi network operator) to allow authentication to take place. As an example, AT&T has developed an Android app as a smart Wi-Fi client. While this is currently locked to download in USA only, it could become part of IEEE 802.11u.

5.8 Roaming arrangements

5.8.1 The GSMA and the Wireless Broadband Alliance (WBA) announced in March 2012 they are working together to simplify connectivity to Wi-Fi hotspots from mobile devices such as smartphones and tablets.

NOTE: Refer to the References section for a URL to the relevant media release.

5.8.2 Wi-Fi roaming will be based on the WBA's 'Next Generation Hotspot' programme and the Wi-Fi Alliance's 'Passpoint certification' technology.

5.8.3 This work will build on the GSMA's GPRS Roaming Exchange (GRX) and the WBA's Wireless Roaming Intermediary Exchange (WRIX) roaming models.

5.8.4 It will develop technical and commercial frameworks for Wi-Fi roaming to create a simpler consumer experience across both mobile and Wi-Fi networks.

5.8.5 Wi-Fi roaming will allow mobile devices to connect to a Wi-Fi hotspot using the SIM card for authentication, as well as enable mobile network operators to securely identify users whether they are on a mobile or Wi-Fi network.

6 FACTORS AFFECTING NETWORK DEPLOYMENTS

Below are a number of key factors that must be considered when planning and deploying a Wi-Fi network in order to ensure stability, ease of use and correct operation.

6.1 Managing interference in public spectrum

6.1.1 Wi-Fi devices operate in the unlicensed public spectrum of 2.4GHz and 5GHz.

6.1.2 When there are multiple Wi-Fi networks deployed at a given location (e.g. in a shopping centre, stadium, etc.) then in an ideal world, processes should be put in place to manage interference among the networks operated by carriers, site owners and retail outlets, all trying to use the same frequency bands.

6.1.3 The challenge however in using unlicensed public spectrum is the lack of control to shield from RF Interference generated by private (i.e. business or domestic) Wi-Fi networks and other devices that use the same spectrum in the vicinity of the public network. An intrusive Wi-Fi AP such as this is termed a "Rogue AP".

6.1.4 It is expected that due to explosive growth in the smartphones that use 2.4GHz spectrum, there will be heavy congestion experienced in the near future, forcing the widespread use of 5GHz spectrum or adapting smart antenna that actively mitigate interference. There are smartphones already in the market that have both 2.4GHz and 5GHz radio built in e.g. the Samsung Galaxy Note.

6.1.5 Most advanced Wi-Fi systems will use a Wireless controller to manage multiple APs in a coordinated fashion to minimise overlap and interference.

6.2 Availability of spectrum

6.2.1 There needs to be sufficient (unlicensed) spectrum for growth in Wi-Fi usage. At this moment Wi-Fi systems most commonly use 3 non-overlapping channels at 2.4GHz and/or 20 channels at 5GHz. It is quite feasible to use the remaining 9 channels at 2.4GHz. In fact, there are advanced Wi-Fi systems available today which intelligently select any of the 11 channels that have the maximum throughput capacity and use the IEEE 802.11h standard to request client devices to join that channel.

6.2.2 Another factor related to spectrum usage in deploying a network is how crowded are the spectrum bands in a given area. For example, in the Melbourne CBD there is some congestion in the 5GHz Wi-Fi bands, while the Sydney CBD is arguably satisfactory in the same bands.

6.2.3 Most advanced Wi-Fi systems now have the ability to force clients to connect at the higher 5GHz spectrum instead of the 2.4GHz by default. This is becoming a common practice across major wireless vendors and provides a better experience for the users (if the 5GHz isn't congested already).

6.2.4 A number of other technologies also operate within the 2.4GHz and 5GHz channel space, including:

(a) Bluetooth devices;

(b) DECT Cordless telephones;

(c) AV in-home repeaters;

(d) Garage door openers;

(e) Wireless security systems (e.g. cameras, IR monitors);

(f) Baby monitors; and

(g) Smart Meter systems, including ZigBee and Wi-Fi mesh.

6.3 Gathering usage statistics/information

6.3.1 Reasons to gather statistics on Wi-Fi network usage include to:

(a) ensure shop operators and building owners get information to help track revenue and customer movements;

(b) plan network augmentations and capacity upgrades;

(c) bill for Wi-Fi access; and

(d) assist with law enforcement.

6.3.2 Statistics on network usage can range from tracking the number of users over/at a given time through to detailed analysis on a range of dimensions including:

(a) traffic volume;

(b) channel usage;

(c) preferred sites;

(d) device type / operating system;

(e) session duration (e.g. average, range);

(f) time of day; or

(g) day of week.

6.4 Growth in small cell usage

6.4.1 Small cells (also known as femtocells) operate in licensed spectrum e.g. the recently launched Optus Home Zone product.

6.4.2 This leads to an interplay between Wi-Fi operation in unlicensed spectrum (i.e. both ‘public’ and carrier operated networks) and carrier operated small cells.

6.4.3 Additional types of small cells are likely to be added to the mobile carrier networks in coming years. These may be based on:

(a) Class licensed (no individual licences or fees – effectively unlicensed) spectrum (e.g. Wi-Fi);

(b) Spectrum or Apparatus licensed spectrum (e.g. 3G HSPA+); or

(c) a combination of both.

6.4.4 Initial deployments are likely to be in high density/high traffic user areas such as:

(a) road/rail corridors;

(b) shopping centres;

(c) office buildings;

(d) sports facilities; and

(e) airports.

6.5 Growth in network usage

6.5.1 This growth in network usage is partly due to the increasing number of IP connected devices being used for a range of existing and new activities.

6.5.2 This includes their use as an alternative or replacement to traditional communications (e.g. home and office LANs, fixed line voice, dial up modems, ISDN, fixed broadband, UHF band radio).

6.5.3 Examples driving the growth in network usage include the use of Wi-Fi for conducting:

(a) transactions;

(b) navigation (of buildings or between buildings);

(c) instant messaging (including email) to friends/family/colleagues; and

(d) comparison shopping.

6.5.4 Examples of new devices likely to rely on a Wi-Fi and/or mobile networks are:

(a) Digital signage/bill boards/information boards;

(b) EFTPOS and other POS systems;

(c) Security devices;

(d) User tracking devices; and

(e) Handheld devices (e.g. phones, tablets, radios, pagers).

6.5.5 Such growth in the number and type of devices also drives a need for additional spectrum to meet the anticipated demand.

6.6 Managing capacity issues in cellular networks

6.6.1 The focus for managing capacity in Wi-Fi networks is on managing data transmission capacity because IEEE 802.11u does not offload voice traffic i.e. it does not address the sending of voice telephony traffic over the data networks.

6.6.2 At present IEEE 802.11u does not use an end-to-end quality of service (QoS) feature. It is reserved for future use on voice services.

6.6.3 As an example of network capacity management, KDDI in Tokyo are rolling out 120,000 access networks, 6000 sites in the City of London to offload from carrier networks. This illustrates another model where a wholesaler that owns real estate is setting up networks for 3G offload.

6.7 Managing multiple radio networks

6.7.1 Infonetics Research noted in its *Carrier WiFi Offload and Hotspot Strategies: Global Service Provider Survey*[8] (May 2012) that while "*data offload is the current priority, in coming years operators will want to see a closer integration of WiFi with the mobile network so that offload becomes more intelligent, automated, and seamless. They want to utilize WiFi not only to augment mobile services, but to enhance the network itself by becoming an integrated part of the mobile network*."

6.7.2 Given this, and with popular (mobile) devices now capable of operating on multiple radio networks (e.g. 3G and Wi-Fi) then it is important for a network operator to be able to manage access to and handover between multiple radio networks.

6.7.3 While IEEE 802.11u can assist a network operator in terms of managing authentication to multiple networks there are a

[8] http://www.infonetics.com/pr/2012/Carrier-WiFi-Offload-and-Hotspot-Strategies-Survey-Highlights.asp

number of issues to address, including those identified on handover in section 4.4.

6.8 Managing battery usage

6.8.1 A device may require Wi-Fi to be on all the time to detect the choice of available networks. Therefore an important consideration for the user experience of a Wi-Fi network is how to manage battery usage.

6.8.2 Some devices may only check for network availability when user activity requires data access (e.g. on an iPhone). This can extend battery usage but may not be aware of alternate networks that become available.

6.8.3 An example of another way to manage battery life is via a smart client/app developed by AT&T. Once it senses a Wi-Fi AP the device running the app will turn on by itself. If no radio beacon is detected then the app will shut down the radio transmission for a number of minutes to extend battery life.

6.9 Substitutability of unlicensed Wi-Fi and licensed networks

6.9.1 In planning network deployment one should consider the potential for the transfer of traffic between network types, with consequential impact on different service types.

6.9.2 For example, if there is no viable Wi-Fi connectivity in a busy venue (e.g. a shopping centre) then that will create an additional data load on a mobile carrier network, which might then affect telephony performance.

6.10 Timely, reliable data

6.10.1 While some applications using a Wi-Fi network for connectivity can tolerate dropped packets or delays, there is a range other applications that may be less tolerant.

6.10.2 For example, commercial premises (e.g. shopping centres) will be built to a 5 or 6 green star rating, and a priority for them is to manage energy consumption. A Wi-Fi network might be used to transfer energy metering data which might require reliable transmission.

7 COMMERCIAL ISSUES

Below are a number of key factors that should be considered when planning and deploying a commercial Wi-Fi network.

7.1 Factors to consider – regulatory and legal

7.1.1 If a provider of a Wi-Fi service is charging an end user for the service then one needs to consider whether or not this leads to carrier obligations or is exempt.

7.1.2 If a service provider asks merchandisers for advertising fees but did not charge the end users for Wi-Fi access then one might be able to argue this is a non-commercial service and so could operate without a carrier license.

7.1.3 Operation of a Wi-Fi network on single site or on multiple sites can affect the treatment of the network(s) in terms of whether or not it requires a carrier license. For example, if each site is operated by a distinct entity but there is an organisation coordinating the sites, there is a question as to whether one or more entities may require a carrier license.

7.1.4 The *Competition and Consumer Act 2010* outlaws the use of 'third line forcing' e.g. if a property owner leases space and then it must not require purchase of a carriage service from a particular CSP. However leasing a site and requiring purchase of a carriage service (with lessee to choose the CSP) might be acceptable.

7.1.5 Refer to section 3 (on regulatory issues) for more information e.g. on emergency calling.

NOTE: In all cases a provider should obtain its own legal advice and not rely on the content of this document alone.

7.1.6 Possible models for rollouts include:

(a) End to end ownership and operation;

(b) Discrete ownership e.g. separate entities/owners for the site, the backhaul network connectivity, the access network equipment, the service provision;

(c) Joint ventures bringing together expertise from different areas by a number of parties;

(d) Alliances where each party operates independently but with an agreement in place for working together; or

(e) Some mix of discrete ownership, joint venture and/or alliance.

7.2 Roles and Responsibilities

7.2.1 Roles and responsibilities that need to be clarified in operation of Wi-Fi networks and services include the:

(a) role of the carrier (network owner);

(b) role of service provider(s) (e.g. a reseller/resupplier);

(c) role of the building/site owner;

(d) relationships between retailers/wholesalers for the service;

(e) relationships between building/site owner(s) and lessee(s);

(f) extension via a wholesale agreement of an existing carrier network e.g. for Wi-Fi offload from a 3G network;

(g) use of roaming agreements;

(h) responsibility for interception e.g. interaction with law enforcement agencies;

(i) responsibility for content filtering; and

(j) responsibility to monitor/prevent infringement of the law on copyright infringement and spam.

7.2.2 Some practical examples where roles and responsibilities need clarification include:

(a) in an airline's frequent flyer lounge where one gets 'free' access as part of being a member of the frequent flyer scheme or paying for lounge access;

(b) in a carrier's or system integrator's supply of a 'data only' service over a private network;

(c) in a coffee shop franchise where one gets 'free' access in return for a product purchase; and

(d) in a shopping centre where one gets 'free' access as a service to encourage a longer visit to the centre or to assist with shopping.

7.2.3 Using the above examples, questions that arise about roles and responsibilities include:

(a) which entity supplies the service to the customer?

(b) who takes on responsibility for the delivery of the service e.g. the airline, the franchisee, the franchisor, the shopping centre?

(c) Can this responsibility be contracted out to a third party that takes on the carrier and/or carriage service provider responsibilities?

7.2.4 Using the above examples, some illustrations of differing levels of awareness about responsibilities include:

(a) an existing carrier/CSP might act on behalf of an airline in in the airport lounge, with a formal agreement in place between them;

(b) the system integrator might supply a corporation with a private 'data only' network with external access but an employee uses their own VoIP adapter for telephony;

(c) the coffee shop might give people access to its DSL service via an AP but the DSL service provider is not aware of it;

(d) for '3G offload', can some/all responsibility be transferred between the operators of the Wi-Fi network and the mobile data network?

7.2.5 Other questions about roles and responsibilities that should be addressed include:

(a) What happens when there is pre-authentication?

(b) Who has responsibility for ensuring the quality of a service?

(c) Who has responsibility for addressing the handling of copyright material?

(d) How might these questions be addressed in the end user license agreement (EULA) or terms of service?

7.2.6 For cases where end users are accessing prohibited content, one might be required to identify the users and then:

(a) log the usage; or

(b) stop access to the content.

7.3 Order of rollout

7.3.1 Initial deployment sites tend to favour environments with a high concentration of potential users (e.g. in a sports stadium) in order to maximise return.

7.3.2 Another trend is for initial deployment sites tend to focus on indoor locations with outdoor sites occurring later on.

7.3.3 With the initial rollout complete then over time there develops support for a range of use cases e.g. high density.

7.4 Billing

7.4.1 Parties to the supply of services via a Wi-Fi network should define:

(a) processes for the notification and acceptance of roaming charges by end users;

(b) mechanisms for payment for third party content; and

(c) record keeping rules (e.g. for billing and interception).

7.4.2 Policies should be established for the retention and disclosure of records e.g. in the event of a billing dispute.

7.5 Authentication and Login

Parties to the supply of services via a Wi-Fi network should define:

(a) The terms for engagement with end users at the time of login (e.g. through the use of standard EULA terms);

(b) a clear process to notify customers of charges to connect to the network;

(c) rules for privacy and protection of customer data (e.g. transfer of customer data and credit card information to third party networks);

(d) process to manage unauthorised login to open networks by end users;

(e) how to prevent innocent end users inadvertently accessing private networks; and

(f) session timeout rules, including the notification to give an end user when the session comes to an end).

7.6 Potential revenue models

7.6.1 Some models for generating revenue via Wi-Fi networks might include:

(a) Making the Wi-Fi service available at zero or low cost to encourage users to extend their time in a location e.g. in a shopping centre.

(b) charging a temporary visitor for Wi-Fi access e.g. as occurs in the hospitality industry.

(c) establishing accounts for frequent users.

7.6.2 Of course this is not intended to be an exhaustive list of revenue models and other models may emerge over time.

8 FACTORS AN END USER SHOULD CONSIDER

As for any service, when operating a Wi-Fi network one should always consider the end user perspective. This section highlights some of the factors an end user should consider when using a Wi-Fi network.

8.1 Balancing end user expectations

8.1.1 Some people like having the convenience and connectivity offered by ready availability of Wi-Fi networks while others object to the extra towers/base stations/APs required to deliver the additional networks.

8.1.2 The balance of these two forces remains a topic for consideration by policy and regulatory bodies.

8.2 Consistency of experience – logging in/out

8.2.1 When moving from one Wi-Fi hotspot to another, it helps if end users have a consistent log in experience.

8.2.2 The anticipated growth in availability of Hotspot 2.0 enabled Wi-Fi networks is expected to make it easier for end users to log on in a consistent manner on different Wi-Fi networks.

8.2.3 Connection via a Hotspot 2.0 enabled network makes it feasible to log in once to a Wi-Fi network and then use a profile created for that log on process for subsequent connections to compatible networks.

8.3 Consistency of experience - billing

8.3.1 An end user should consider their billing arrangements when agreeing to connect to a network.

8.3.2 There are similarities to the billing choices available on other technologies where once can choose between:

(a) being able to log on once and roam across different networks with the potential for seamless connectivity (similar to existing mobile networks with roaming agreements).

(b) choosing on an ad hoc basis the networks to connect to and in doing so any associated expenditure (similar to existing methods for connecting to Wi-Fi networks).

(c) being able to log on once with a limit on spend (similar to existing mobile prepaid services).

8.3.3 When one comes within range of an authorised prepaid network connection, what are the implications for an end customer from a billing perspective? e.g. one does not want users to receive unexpected roaming charges.

8.4 Security – Methods

8.4.1 Security is not addressed directly in IEEE 802.11u because the scope of the standard is about selecting and connecting to a network.

8.4.2 However the support of EAP and WPA2 through the implementation of IEEE 802.11u and Hotspot 2.0 creates a more secure environment for users of Wi-Fi networks.

8.4.3 In IEEE 802.11u the onus is on the carrier to handle security.

8.4.4 Refer to Section 5 for more information on some of the technical issues to consider related to security and some of the choices available for securing a connection.

8.5 Security – The Importance of trust

8.5.1 An important issue for end users is how to tell if a Wi-Fi hotspot can be trusted.

8.5.2 One wants to guard against 'man in the middle' or 'evil twin' style attacks from an ad hoc network pretending to be a public access Wi-Fi network in order to gather user data.

8.5.3 Unfortunately the omission of public key infrastructure (PKI) makes it difficult to challenge the authenticity of a public AP.

8.5.4 Establishing a trust mark (to give confidence in networks) has costs associated with auditing such a mark (to ensure compliance) that then reduces its attractiveness.

8.5.5 Possible methods to limit abuse of network access include:

(a) Limiting the session duration; and

(b) Monitoring MAC address logging.

8.6 Device upgrade paths

8.6.1 An upgrade path for a device could add functions for Wi-Fi operation via the operating system on a device (e.g. Android, iOS, Windows Phone 7 or 8) through a software upgrade.

8.6.2 However experience with devices has been that the majority of customers do not upgrade, even on iOS which has arguably the best process for an upgrade.

8.7 Privacy

8.7.1 Existing arrangements for privacy, that are not specific to Wi-Fi networks, include the Privacy Act, and the Telecommunications Consumer Protections code. These should be referred to prior to developing any privacy arrangements that are technology specific.

8.7.2 The risk of using a Wi-Fi network as a shared medium (e.g. use of a common SSID on an AP) can raise concerns about end user privacy.

8.7.3 It is possible for tracking of Wi-Fi users to occur with varying levels of granularity. Methods include those based upon:

(a) Anonymous data (i.e. simply device count metrics);

(b) Terminal MAC address;

(c) End-user credentials (i.e. username/password, IEEE 802.1X certificate); or

(d) Web cookies (e.g. inserted via logon page).

8.7.4 Consent to tracking may be achieved via an agreement presented at network logon, or under the conditions of entry to the facility.

8.7.5 In 2011 Google proposed the use of a '_nomap' suffix to the network SSID as a method to avoid the SSID being included in its location register. Refer to the References section for a URL to the relevant blog post.

8.8 Roaming

8.8.1 There are a number of end user factors to consider in relation to roaming e.g. roaming between a 3G broadband service and a public Wi-Fi network, depending on service availability. Refer to section 7 for some examples.

8.8.2 Hotspot 2.0 has a core component about roaming since it includes auto sign on.

8.8.3 An area for further study is how to handle roaming between wireless Wide Area Networks (WANs) and/or Metropolitan Area Networks (MANs).

9 REFERENCES

Publication	**Title**
Industry Standards	
IEEE 802.11-2006	IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications IEEE 802.11 documents are available via the Get 802® Standards webpage http://standards.ieee.org/about/get/802/802.11.html
IEEE 802.1u	Amendment 9: Interworking with External Networks IEEE 802.11 documents are available via the Get 802® Standards webpage http://standards.ieee.org/about/get/802/802.11.html
Legislation	
Competition and Consumer Act 2010 *http://www.comlaw.gov.au/Series/C2004A00109*	
Do Not Call Register Act 2006 *http://www.comlaw.gov.au/Series/C2006A00088*	
Privacy Act 1988 *http://www.comlaw.gov.au/Series/C2004A03712*	
Spam Act 2003 *http://www.comlaw.gov.au/Series/C2004A01214*	
Telecommunications Act 1997 *http://www.comlaw.gov.au/Series/C2004A05145*	
Telecommunications (Consumer Protection and Service Standards) Act 1999 *http://www.comlaw.gov.au/Series/C2004A00441*	
Radiocommunications Act 1992 *http://www.comlaw.gov.au/Details/C2010C00220*	

Regulation

Telecommunications (Emergency Call Service) Determination 2009

http://www.comlaw.gov.au/Series/F2009L04720

Telecommunications Act 1997 - Determination under subsection 51(1) (No. 1 of 2002)

http://www.comlaw.gov.au/Series/F2004B00444

Radiocommunications (Low Interference Potential Devices) Class Licence 2000

http://www.comlaw.gov.au/Series/F2005B00339

Other documents

ACMA information paper on Low interference potential devices

http://www.acma.gov.au/WEB/STANDARD/367875/pc=PC_1278

ACMA webpage Wireless LANs in the 2.4 GHz band FAQs

http://www.acma.gov.au/WEB/STANDARD/923035/pc=PC_1794

ACMA fact sheet: Wireless LANs – design and security fact sheet

http://www.acma.gov.au/WEB/STANDARD/923035/pc=PC_1740

ACMA factsheet: Wireless LANs – what and how fact sheet

http://www.acma.gov.au/WEB/STANDARD/844582/pc=PC_1739

Industry Documents

Wireless Broadband Alliance

Industry Report 2011 Global Developments in Public Wi Fi

http://www.wballiance.com/component/files/dltrack.html?files=3b01001fba73a5422ad8e666052437b791a63974

Industry Report 2011 summary infographic

http://www.wballiance.com/component/files/dltrack.html?files=9db3ec3cff1f25ad99b982e9c231663d0fdae054

Google blog post about the use of a _nomap suffix to network SSID to "opt out of having your wireless access point included in the Google Location Server".

http://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html

Wireless Broadband Alliance and GSMA media release

"GSMA And WBA Collaborate to Simplify Wi-fi Hotspot Access for Smartphones and Tablets"

http://www.gsma.com/articles/gsma-and-wba-collaborate-to-simplify-wi-fi-hotspot-access-for-smartphones-and-tablets/23082 and http://www.wballiance.com/images/news/pdf/gsma_wba_joint_initiative_pr.pdf

APPENDIX

A BACKGROUND INFORMATION – ABOUT WI-FI

A1 What is Wi-Fi?

'Wi-Fi' is the term used for wireless access devices and networks that use the IEEE 802.11™[9] series of standards on Wireless Local Area Networks (WLANs). For additional technical information on Wi-Fi and IEEE 802.11™ refer to the 'Technical' section of the document.

A2 Who develops arrangements for Wi-Fi?

There are a number of organisations facilitating the development, adoption and rollout of Wi-Fi devices, networks and services.

The Institute of Electrical and Electronic Engineers[10] (IEEE) is the organisation that defines the IEEE 802.11™ series of technical standards for Wi-Fi.

The Wi-Fi Alliance[11] was formed in 1999 as a global non-profit organization with the goal of driving adoption of high-speed wireless local area networking. This includes getting devices to have the built in capability to support the various developments in IEEE 802.11, with one of the most recent developments being IEEE 802.11u.

The Wireless Broadband Alliance[12] (WBA) was established in 2003 as a global forum to facilitate the adoption of Wi-Fi enabled services through improvements in user experience, interoperability and service delivery across technologies, devices and networks. Part of its role is in helping define policy for network operators on roaming and billing. Another part is testing end-to-end interoperability of equipment and services.

[9] http://standards.ieee.org/about/get/802/802.11.html
[10] http://www.ieee.org/
[11] http://www.wi-fi.org/organization.php
[12] http://www.wballiance.net/about-us/wba-overview.html

APPENDIX

B BACKGROUND INFORMATION - TECHNICAL

B1 Spectrum and licensing for Wi-Fi networks

Wi-Fi networks operate in Australia using spectrum at/around 2.4GHz and 5 GHz.

WLAN modulation schemes are licensed under the *Radiocommunications (Low Interference Potential Devices) Class Licence 2000* (the LIPD Class Licence)[13]. Therefore public Wi-Fi networks operate under a class licence and do not receive protection from interference from other users of the spectrum.

B2 Emerging standards – Hotspot 2.0

Wi-Fi hotspots have been around for ten years or more, now seeing the Wi-Fi Alliance specification for operators of Wi-Fi networks, referred to as Hotspot 2.0.

The Wireless Broadband Alliance has contributed to the development of the standard IEEE 802.11u, which can facilitate auto login.

As more devices become capable then one will be able to have a network of wireless networks that are capable of implementing IEEE 802.11u, Hotspot 2.0, etc.

The WBA is testing end to end interoperability with a focus on three areas:

(i) conformance to IEEE 802.11u,

(ii) encryption (using WPA2), and

(iii) authentication (using EAP).

In February 2012 the WBA announced successful trials "*to test the Next Generation Hotspots (NGH) requirements for network discovery and selection, security, automatic authentication in a production environment on, and between, different operators' actual networks using equipment and devices from various vendors*"[14].

B3 Emerging standards – IEEE 802.11ac

The IEEE Project IEEE 802.11ac ("Very High Throughput <6Ghz") is currently at ballot[15] and will support equipment use in 5GHz spectrum.

An alternate approach for equipment manufacturers is to develop advances in Multiple Input Multiple Output (MIMO) antenna technology.

There are choices between the two paths in terms of resource allocation and likely return arising from mass adoption.

[13] Source: *Wireless LANs in the 2.4 GHz band FAQs* webpage http://www.acma.gov.au/WEB/STANDARD..PC/344824/pc=PC_1794

[14] http://www.wballiance.com/images/news/pdf/ngh_trial_results_press_release_vfinal.pdf

[15] http://www.ieee802.org/11/Reports/802.11_Timelines.htm

PARTICIPANTS

The working group that developed the information paper consisted of the following organisations and their representatives:

Organisation	**Representative**
AAPT	Josef Barter
Alcatel-Lucent	Rob Haylock (Chair)
Alcatel-Lucent	Jason Leung
AMTA	Lisa Brown
Baker & McKenzie	James Halliday
Carwardine Legal	Austin Carwardine
Huawei	Julian Ho
Market Clarity	Shara Evans
Optus	Sam Mangar
Pie Networks	Stuart Snell
Pie Networks	Craig Turner
Telstra	Michael Swadling
Research In Motion	Erica Fensom
Ruckus Wireless	Steve Chung
Ruckus Wireless	Carl Jefferys
Westfield	Peter Bourke
Westfield	Shailendra Singh

This working group was chaired by Rob Haylock. James Duck of Communications Alliance provided project management support.

Communications Alliance was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507

Care should be taken to ensure the material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact Communications Alliance