



Australian Government

Australian Communications Authority

Final Report

Vision 20/20: Future Scenarios for the Communications Industry – Implications for Regulation

Final Report

April 2005

Foreword

The Australian Communications Authority (ACA) is pleased to release the final report for *Vision 20/20: Future scenarios for the communications industry – implications for regulation*.

Vision 20/20 was a foresight project, designed to develop a greater understanding about the future of communications and the consequences for regulation. The project recognised that, while the communications environment is likely to be a rapidly evolving and convergent environment in the next 10 to 15 years, the nature of that change is uncertain.

This uncertainty encouraged an assessment of the implications of the communications future on the overall regulatory framework. Through the use of a creative combination of methodologies, the project examined opportunities and challenges for consumers, industry and overall governance arrangements.

Vision 20/20 looks at the Australian communications environment within an international context. The proposed strategic action agenda is supported by a substantial body of project work, including the input of many people and organisations from within Australia and internationally.

The final report is not intended to be an ACA view of the world—the scope of Vision 20/20 is greater than the responsibilities of the ACA alone. The report, however, will serve to guide the Australian Communications and Media Authority on actions to take over the coming years, and provide a framework for discussion about the issues raised by the emerging communications environment in the longer-term.

I would like to take this opportunity to thank the many people that worked with the ACA in the collaborative development of this report and to encourage these strong networks to continue. The report provides a reference point for stakeholders and should contribute to discussions and strategic decision-making regarding the role and nature of communications regulation.

Dr Bob Horton
Acting Chairman
April 2005

Executive summary.....	i
Part 1: Background	1
1.1 Introduction	1
1.2 Objective.....	1
1.3 Overview.....	1
Part 2: Strategic landscape	3
2.1 Introduction	3
2.2 Scenario planning process	3
2.3 Communications elements	3
2.4 The future we know about	4
2.5 The scenarios – mapping possible futures.....	4
2.5.1 Overview.....	4
2.5.2 The best outcomes in the scenarios.....	6
2.5.3 Tensions in the environment	8
2.6 Strategic landscape	9
2.6.1 Power and influence	11
2.6.1.1 User power.....	11
2.6.1.2 Informed consumers	12
2.6.1.3 Digital content	12
2.6.1.4 Globalisation	13
2.6.2 Cooperation	14
2.6.2.1 Incentives to cooperate.....	14
2.6.2.2 Importance of competition and innovation	14
2.6.3 Ubiquitous communications.....	15
2.6.4 Pre-conditions for ubiquitous communications.....	16
2.6.4.1 Technology	18
2.6.4.2 Market dynamics.....	20
2.6.4.3 Users.....	22
2.6.4.4 Rules and guidelines	26
2.6.5 The alternative: fragmented, limited communications	29
2.6.6 Limits to openness, being always online	30
2.6.7 Next five to ten years.....	30
2.6.8 Longer term	31
Part 3: Regulatory implications	32
3.1 Introduction.....	32
3.2 Current regulatory framework.....	32
3.3 Regulatory challenges – what we found.....	33
3.3.1 Overview.....	33
3.3.2 What we need to do differently	34
3.3.2.1 From numbering to identity	34
3.3.2.2 Legacy network reliability.....	34
3.3.3 New approaches.....	35
3.3.3.1 Phasing out redundant elements	35
3.3.3.2 Recognising the impact of new forms of communications.....	36
3.3.3.3 Network integrity – taking responsibility, building awareness	36
3.3.3.4 Building new working relationships.....	38
3.3.3.5 Recognising the importance of cooperation	39
3.3.3.6 New uses of radiofrequency spectrum	39
3.3.3.7 Content more dominant	40
3.3.3.8 Rethinking peer-to-peer	40
3.3.3.9 Developing agreed e-government and e-commerce frameworks	41
3.3.3.10 Applying a layered approach	42
3.3.4 What we need to continue with	42
3.3.4.1 Consumer protection mechanisms	42
3.3.4.2 Competition regulation.....	42
3.3.4.3 Technical neutrality	43

3.3.4.4	EMR research	43
Part 4: Regulatory Challenges		44
4.1	Introduction.....	44
4.2	Regulatory themes	44
4.2.1	What should be done differently	45
4.2.2	Issues of particular interest to the ACMA	46
Appendixes		48
Appendix 1: Scenario narratives		49
Appendix 2: Clash of culture		63
Appendix 3: Spam – a case study		65

Executive summary

Introduction

In December 2003, the Australian Communications Authority (ACA) launched a planning project, *Vision 20/20: Future scenarios for the communications industry – implications for regulation*. Vision 20/20 was designed to understand the nature of the future communications environment, but not to predict it.

For this project, 'regulation' refers to the rules governing behaviour that may be implemented and enforced by government, industry or individual users themselves and includes co-regulation and self-regulation. 'Communications' includes the telecommunications, radiocommunications, broadcasting and information, communications and entertainment technology (ICET) industries.

This final report of the Vision 20/20 project is the result of a collaborative research process. It is designed to encourage discussion. It does not represent the views of the Australian Government about the role of regulation now or in the future.

The report identifies drivers of change and the potential implications for the development of flexible and responsive regulation to meet the emerging challenges.

Participants in the Vision 20/20 project represented a wide range of industry, government and consumer interests. Despite this diversity, there were strong common themes relating to future challenges in communications regulation.

This wide representation and the scope of the Vision 20/20 project means that many of the issues raised fall outside the scope of the ACA. Issues of specific relevance to the ACA are outlined later in this summary and in Part 4 of the report. The project methodology is on the Vision 20/20 website at <http://vision2020.aca.gov.au>. A detailed analysis of the scenarios and the strategic landscape is in the body report and the scenario narratives are in Appendix 1.

Strategic landscape

The Vision 20/20 process has been highly consultative, using interviews, workshops, literature research and continuing feedback to gather project material and prepare this report.

Relative certainties about the communications future were determined through this process. These are primary drivers of change as well as constraints, and provide a social, technological, economic, environmental and political foundation for analysis of the key *uncertainties* in the communications future. While they are referred to as certainties, they are influenced by other factors in the environment, which are discussed in more detail below.

The relative certainties may be summarised as follows:

- Communications is multi-dimensional and multi-functional, embracing telecommunications, radiocommunications, broadcasting and information communication and entertainment technologies (ICET).
- Communications technologies are increasingly IP-based.
- Communications is global and transcends nation state boundaries.
- Individuals, organisations and governance frameworks increasingly depend on communications technologies and infrastructures.
- Global trends include an ageing population, rising oil prices and the development of alternative energy sources, and the consequences of climate change.

The Vision 20/20 project identified the issues likely to have a major influence on communications over the next 15 years. Two fundamental uncertainties emerged. These are the:

- extent of cooperation and
- concentration or distribution of power and influence.

The extent of cooperation will determine how well—from seamless to fragmented—the various elements of communications work together. The concentration or distribution of power and influence will determine who or what dominates and how regulation is managed in the future.

The need for regulatory cooperation locally and internationally, between market players, law enforcement and national security agencies and regulators is being driven by global connectivity, convergence and globalisation. Working against such cooperation are national interest and self interest, as well as differences in culture and values. Where there is cooperation, the achievement of seamless connectivity in communications networks is possible.

The spread of power and influence—whether concentrated or distributed—will be shaped by trends and developments in geopolitics, globalisation, and integration of networks and systems.

High levels of cooperation combined with decentralised power and influence may result in ever-present communications with open access to information. This may mean increased individual and consumer empowerment, more competitive markets and individual and market-based responsibility, with a relatively minimal role for government regulation.

While high levels of cooperation with centralised power and influence may result in the ability to connect seamlessly, governments, corporate entities and other influential groups may largely determine and enforce rules, rights and responsibilities

Without cooperation, communications may be fragmented and limited. Cooperation may fail where industry, users and governments lack incentives to cooperate or have different views on regulation.

Decentralised power and influence with fragmentation will result in a world where rights and responsibilities are loosely defined and observed.

Centralised power with fragmentation will lead to a lack of trust and confidence because of ineffective regulatory mechanisms. Communications service provision will be dominated by ‘walled-gardens’ where these closed networks use different standards and systems.

Tensions in the environment

Analysis of the scenario narratives reveals five emerging tensions, the outcomes of which are likely to influence and shape consumer trust and confidence and the pace of change in the communications environment. These five tensions are as follows:

- Developing forms of regulation—these may be system-wide or fragmented, networked or institutionalised, and the emphasis may be on self-responsibility or consumer protection and corporate social responsibility.
- Uncertain network access and integration—networks may be open or closed, seamless or fragmented, ubiquitous or limited, multi-layered or discrete and independently managed.
- Changing attitudes to regulation—the community may either demand greater transparency or security threats may result in increased secrecy, and there may be greater personalisation as opposed to one-size fits all standardisation.
- Uncertain network integrity—network integrity could be co-managed with multiple parties, or may be built-in to the network and independently managed.
- Changing power and influence—global organisations may dominate or nation-states regain their influence, peer-to-peer decentralised networks may dominate over centralised client–server models with intelligence at the core, and differences may develop between the virtual and physical worlds.

Regulatory challenges

The Vision 20/20 project discussed the incentives for government, industry and users in realising the potential social and economic benefits of a world of ubiquitous

communications—an information-rich world of ever-present connectivity and distributed computational intelligence.

Ubiquitous communications technologies might include smart cars, smart buildings, location and self-aware applications and devices, personalised information and services and wearable devices. They may provide, for example, pervasive monitoring of the whereabouts of children or the health of elderly people in their homes. The result could be tension between ubiquitous communications, requiring personal identifying information, and the protection of privacy.

There are obvious challenges. These include establishing consistent national and international identity (and identity authentication) processes, ensuring secure and low-cost electronic commerce, integrating standards and regulatory processes, establishing the need for flexible dispute resolution services, and maintaining network integrity and reliability.

Participation is likely to be more critical in rapidly developing and uncertain environments. Vision 20/20 participants emphasised the social and economic impact of exclusion from communications devices and services. They also stressed the importance of universal design principles taking the needs of disadvantaged groups into consideration. Issues raised included access for people with a disability, affordability, access to skills development and geographic isolation.

The emerging communications environment is more complex than ever before, with new elements and new participants. In particular, the computing and consumer electronics industries are converging with the communications and media industries. The convergent elements are multi-layered and international, with global connectivity. Content and applications are no longer dependent on the underlying infrastructure.

Wireless technology is expected to have a more central role in communications in the future. Research into use of the radiofrequency spectrum is considering increased spectrum sharing and cognitive radio technologies. These cover self-sharing, ad hoc and viral communications networks created by users who bring their own infrastructure and share it, without centralised management.

Network intelligence is moving to the network edges. For example, peer-to-peer technologies are changing the way users interact with the network and each other. There are also likely to be increasing challenges in managing risks associated with the production and distribution of digital content.

The established trend towards international regulatory cooperation may result in international cooperation principles. These could emphasise defined public interest outcomes and promote trust in the system through transparency, monitoring and compliance mechanisms.

The protection of personal identifying information and privacy is likely to be increasingly important as more people place their personal information online and communications services are increasingly globalised.

One significant challenge will be to transform regulation to operate within a broader internationalised and interdependent environment. Critical challenges for government, industry and users also include the need to:

- understand all parts of the convergent communications industry;
- be flexible and responsive; and
- build regulatory coherence and cooperation between jurisdictions, industry bodies and communities of interest to promote equitable participation, network integrity, interoperability, and e-government and e-commerce frameworks.

In particular, understanding the emerging communications environment involves:

- evaluating emerging areas of societal risk in terms of self-responsibility relative to government intervention
- dealing with different cultures and values
- forming relationships with new entrants to the communication sector
- learning new skills and abilities, and

- analysing problems using a 'systems thinking' approach rather than just examining particular elements in isolation.

What should be done differently?

In highly urbanised areas, a transition period of 15 years or more to ubiquitous communications is plausible. During that period, transitional arrangements will be needed because legacy telecommunications and broadcasting regulations are likely to operate in parallel with regulations designed for emerging services.

The Vision 20/20 project identified aspects of the current telecommunications regulatory framework that will be tested by emerging developments. These are:

- Numbering plans are likely to continue operating for the next 10 to 15 years, but will start to decline in importance relative to electronic addressing, authentication and verification of identity. Fixed - mobile convergence may mean that separate national numbering plans are unlikely to be sustained over the longer term.
- Falling revenue streams from traditional services over legacy networks may pose a risk to network maintenance and investment expenditure. This may affect network reliability and carrier performance against specified social and legal obligations.
- Segmented regulatory arrangements such as licensing, specified quality of service standards and consumer satisfaction measures are likely to be less important in a relatively more complex, convergent and globalised communications environment.
- Law enforcement and national interest obligations, such as legal interception and location for emergency services purposes, may require supplementary solutions and changes to some existing assumptions.
- More emphasis on cross-jurisdictional relationships will be necessary.
- Smaller organisations entering the communications industry that do not have the capability (because of location or resource constraints) to be involved in traditional industry regulation forums will still need to be engaged in regulatory processes.

Emphasis should also be placed on the following:

- Emerging accessibility challenges—it is important to recognise the potential social impact of new forms of communications especially given a western population that is rapidly ageing and hence developing age-related accessibility issues.
- Trust and confidence—the need to promote trust and confidence in emerging communications services is likely to drive the development of new rights, responsibilities and obligations. Network integrity solutions appear to involve a mixture of government regulation, industry regulation and user responsibility. All need to be explored.
- Cooperation—the number of players in communications is increasing. Regulators will need to develop new relationships with global vendors, new network operators and IT systems providers to build and maintain sufficient expertise over the technical aspects of network regulation.
- Radiofrequency spectrum management—with the growing reliance on and importance of the radiofrequency spectrum, governments will need to improve the efficiency of spectrum allocation and use.
- Content—new challenges are emerging with the increase in online connectivity, private media and open distribution models, and digitalisation of content.
- Peer-to-peer—the recent rise of true or near peer-to-peer applications raises new challenges for communications regulation because of their decentralised nature.
- Layered approach—IP-based service provision may involve multiple layers that are managed or provisioned by separate entities, for example, content may be provided independently of the network operator. The multi-layered approach is a good tool for unbundling a problem into its component parts. It may be preferable to deal with content problems at the applications layer rather than the physical network layer.

Issues of particular interest to the ACMA

In the context of the upcoming merger of the ACA and the Australian Broadcasting Authority (ABA) to form the Australian Communications and Media Authority (ACMA), issues were distilled from Vision 20/20 project workshops, interviews, and research and analysis, as well as feedback to the project.

To keep regulation contemporary and effective, the ACMA will need to monitor developments in services convergence that may affect its regulatory responsibilities. The findings of the Vision 20/20 project emphasise the importance of developing and implementing a more comprehensive, whole-of-business approach to emerging regulation problems in consultation with other government bodies, industry and users. This approach would help in being responsive to:

- monitoring industry performance of network security and network integrity risk management
- managing issues arising from voice, data and multimedia convergence
- market-based approaches to voice over IP and public switched telephone network interconnection
- updating consumer information to reflect trends in services convergence
- risks to legacy network reliability and accessibility
- taking broader measures of consumer benefit and consumer satisfaction and
- working more closely with groups such as the Australian Competition and Consumer Commission (ACCC) on the technical aspects of Internet peering and interconnectivity arrangements.

Vision 20/20 participants also highlighted the importance of promoting a 'networked regulation' approach within and between government agencies and international regulatory bodies that:

- draws on specialist knowledge and networks between individuals and organisations
- incorporates the views of associated regulatory agencies to ensure a strategic 'communications systems' approach is taken, including cross-layer effects, to proposed interventions
- supports a self-organising 'viral regulation' dynamic—participative online inter-working that is responsive and adaptive, where solutions multiply, adapted to suit policy and cultural preferences—as an effective complement to more formal dialogue and
- allows government regulators to have more direct engagement with vendors and 'new players'.

There may be an increased role for the ACMA in providing education and information in the future, particularly in emerging areas of Internet communications risks and information authenticity.

The ACMA could further encourage efficiency in the use of spectrum, including better use of existing allocations, and continue to be responsive to innovative approaches to managing spectrum, including sharing spectrum and the increased use of class licensing to reduce regulation and enhance capacity.

In an uncertain future regulatory environment, the ACMA may need to develop and maintain new skills and abilities. The creation of ACMA will promote development of knowledge of less familiar market segments, such as Internet access and content providers. It will also promote development of regulatory skills in areas such as new media, multi-source content, interactivity and integration. The need to understand Internet architecture and its strengths and weaknesses is important in designing and managing effective regulatory and self-regulatory policies and programs.

Effective relationship management includes the need to work closely with groups supporting industry regulation, such as the Australian Communications Industry Forum, to ensure they

remain relevant to the industry and community they serve. It will also be important to develop relationships with new service providers and relevant virtual communities of interest.

Vision 20/20 project participants discussed the need for greater regulatory flexibility and responsiveness, most likely to be achieved through improved processing of information, more effective use of social and online networks and better communications.

Government regulators need to know how and when to intervene. Understanding and responding to complexity, uncertainty and dynamic change requires a systems-thinking approach and monitoring and analysis of emerging issues. An integrated forward-looking program to track network, services and content migration paths from legacy to IP-based systems would provide the ACMA with a greater capacity to analyse regulatory implications and respond to changes in the environment.

Part 1: Background

1.1 Introduction

In December 2003, the Australian Communications Authority (ACA) launched a scenario planning project, *Vision 20/20: Future scenarios for the communications industry – implications for regulation*.

Vision 20/20 has been a collaborative project, with approximately 200 people having participated through interviews, workshops and formal consultation. Guidance was provided by our Steering Committee, chaired by the ACA with representatives from the:

- Australian Broadcasting Authority (ABA)
- Australian Communications Industry Forum (ACIF)
- Australian Competition and Consumer Commission (ACCC)
- Department of Communications, Information Technology and the Arts (DCITA) and
- Network Insight Institute (NII).

A broad-based approach was taken to take account of the inter-relationships between government regulation, industry-regulation and convergent trends in the telecommunications, broadcasting and ICT industries.

A preliminary report was released in August 2004 for public consultation. We have considered feedback in response to the preliminary report and carried out additional research and analysis so that the final report:

- provides a holistic framework to examine the future strategic landscape
- identifies the best possible outcomes and pre-conditions
- covers the emerging IP-based architecture, digital content and convergent business models in more depth
- provides a more substantive assessment of the issues related to digital participation
- places current regulatory assumptions under more scrutiny and
- provides possible direction on strategic action.

Information about the issues we have considered, the project methodology, preliminary report and feedback is on the project website at <http://vision2020.aca.gov.au>.

1.2 Objective

Vision 20/20 challenges the assumptions that shape the current communications regulatory frameworks and discusses the emerging or potential regulatory challenges towards 2020.

By looking beyond the usual three-year planning environment to the year 2020, we can be better prepared for—and in a better position to shape and influence—tomorrow's regulatory outcomes.

Vision 20/20 does not predict the detail of the future. Critical uncertainties have been identified—those issues that would have a major influence on the regulatory environment.

Vision 20/20 provides guidance to assist in the strategic decision-making by the Australian Communications and Media Authority (ACMA) and contribute to the broader public debate about emerging trends and developments in communications regulation. The paper does not represent the views of the Australian Government about the role of regulation either now or in the future.

1.3 Overview

Part 2 of this paper describes the fundamental elements of communications and describes the five Vision 20/20 scenarios. It also describes the emerging tensions that are likely to

shape consumer trust and confidence in the communications environment and influence the pace of change.

The scenarios are the product of the different perspectives, expertise and vision of over 200 people within Australia and internationally. The paper examines the potential consequences of technical, market and regulatory convergence, integration and new forms of communication that may emerge.

A strategic landscape has been developed that integrates the scenarios and tensions into a framework to aid interpretation and analysis. The perceived best possible outcomes are outlined. This is balanced with an overview of what may go wrong—alternative futures where the best outcomes are not realised.

A preferred outcome is identified—ubiquitous communications. The pre-conditions for this are set out and analysed in terms of the technology assumptions, market dynamics, user experience and rules and guidelines.

Part 3 examines regulatory implications, firstly by describing the assumptions underpinning current regulations and then examining what needs to be challenged. The challenges in achieving network integrity, agreed frameworks for e-government, e-commerce, digital content and standardisation are outlined; more flexible use of the radiofrequency spectrum is explored and the need for regulatory coherence in a more complex and internationalised environment is addressed.

Part 4 outlines the regulatory challenges, what needs to be done differently, and issues of particular interest to the ACMA.

Part 2: Strategic landscape

2.1 Introduction

This part outlines the five Vision 20/20 scenarios, which provide a creative insight into possible communications futures. Communications elements are classified. The emerging tensions in the communications environment are assessed in relation to their ability to shape and influence change.

These issues are then considered within the context of a defined strategic landscape.

2.2 Scenario planning process

Scenario planning was chosen as an effective and structured way to put aside current issues and think freely about what the future may be like. Creating foresight will improve capacity to deal with complexity and uncertainty.

Scenarios are an effective way to allow people to move away from clinical assessment or analysis. They provide a creative means for understanding the future. While scenarios indicate economic, business and governance models, they also emphasise the human drivers in society. They look at what motivates people, what they are concerned about and what they look forward to.

2.3 Communications elements

Vision 20/20 considers the communications environment to be composed of a number of interrelated and overlapping elements—these form a framework of groups or associations that allow interconnection. These elements are:

- technology—the physical networks and systems, and the devices adopted by users to participate in the communications environment
- market dynamics—business models, the marketplace and the nature of competition
- users—the people and organisations that operate and consume within the communications environment and
- rules and guidelines—governance of and in the communications environment.

Often the term 'regulation' is considered to mean government regulation. Within this document, the term is used more broadly recognising the various roles that government, industry and users play.

This paper defines regulation as:

an authoritative principle or condition that either governs or guides behaviour

Within this overall definition of 'regulation', we have defined four 'types' of regulation:

National government regulation—the form of regulation that has the strongest enforcement power as it is supported by law. Within Australia, regulators include the ACA, ABA and ACCC.

International agreements—this form of regulation is varied but includes existing forums such as the International Telecommunication Union (ITU), whose outputs are often implemented by government regulators. International trade agreements are similarly given effect through enabling legislation by participating jurisdictions. This type also includes coordinating bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN).

International standardisation—this can take many forms and includes 'standards bodies' such as the American National Standards Institute (ANSI), the European Telecommunications Standards Institute (ETSI), the Bluetooth Special Interest Group, the Third Generation Partnership Project Agreement (3GPP) and the Internet Engineering Task Force (IETF) that work at an international level. It also includes nationally focused groups such as the ACIF and industry representative or special interest organisations.

Individual or user responsibility—this is often overlooked, but is an important form of regulation. For example, within the Australian context, end-users have to take responsibility

for their own Internet-content filtering, as well as the level of exposure of their Internet-connected computer to cyber attack through their use or otherwise of firewalls or anti-virus software. End-users also contribute to code and standards development.

Part 3 of this paper discusses the current nature of communications regulation in Australia in more detail.

2.4 The future we know about

Relative ‘certainties’ about the communications future have been determined. These are both primary drivers of change and constants, and provide a social, technological, economic, environmental and political foundation for analysis of the key *uncertainties* in the communications future. While we refer to them as certainties, these issues are not absolute or unchanging and are influenced by other factors in the environment, as discussed in more detail below.

The relative certainties may be summarised as:

- Communications is multi-dimensional and multi-functional, comprising of at least telecommunications, radiocommunications, broadcasting and information communication and entertainment technologies (ICET).
- Communications technologies will be increasingly IP-based in a digitalised world.
- The communications future is a global context where nation-state boundaries, in terms of exercising controls, will not be easily applied.
- Individuals, organisations and governance frameworks have an increasing dependence on communications technologies and infrastructures.
- Global trends include:
 - o an ageing population
 - o rising oil prices and the development of alternative energy sources and
 - o climate change and its consequences.

2.5 The scenarios – mapping possible futures

2.5.1 Overview

Using the relative certainties outlined above as a foundation, a range of uncertainties were identified as being important in examining what the communications environment might be like in 2020, what the user experience might be, and the implications for regulation. The scenarios were created independently by five separate groups. The predetermined elements and uncertainties for each group’s narrative were identified from others as the ones that pose the most challenges for the future.

The scenario narratives assist in understanding the conditions and variables at a future point in time—a strategic perspective that offers an understanding of the challenges that may lie ahead.

Figure 2 on page 10 maps the scenarios to provide an overall frame of reference. The full scenario narratives, in Appendix 1, provide a deeper understanding of what participants assumed would be exciting or fearful about the future, and the attitudes, values and beliefs (worldviews) underpinning each scenario. The scenarios represent the views of the many people involved in the scenario building process—they are not intended to predict the future and they do not represent the views of the ACA or any individual participant.

Scenario 1: Sensitive new age future



"...individual self-reliance is paramount."

This is a communications environment with global networks, open standards and full interoperability—individual self-reliance and social responsibility result in trust and cooperation. There is good consumer choice and satisfaction.

Scenario 2: Big Daddy



"Increasingly, devices are easier to use ... (and) fully interoperable."

This is a story of realised technological possibilities—communications and commerce have converged. It is perceived that the government works to assure a greater good by actively monitoring its citizens—people are required to use government-issued identifiers. There is a high emphasis on subscription-based personal activities.

Scenario 3: Nano-boomers



"...identities may be assumed informally."

There is a fragmented global communications infrastructure and unrealised technological potential. The communications environment is converged, wireless and highly pervasive, but has poor performance in service delivery, particularly in verifying information.

This is an environment where the cyber world has as much or more meaning to people as the physical world.

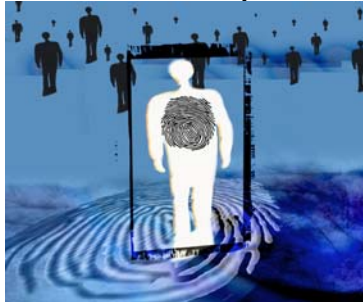
Scenario 4: Marching together into the future



"Communications is a key priority."

This is a highly cooperative environment of alliances and partnerships—there is a rapid pace of change, supported by unified national priorities. People share the view that self-interest should be aligned with the greater good for all.

Scenario 5: Green prison



"...a longstanding crisis of confidence in Australia."

There is a lack of trust in communications in an unstable 'war-time' economy—but there is a high emphasis on environmental accountability. Communications technologies are highly focused on surveillance and monitoring. Individuals are increasingly entrenched in the communications system, with personal identifying information required to access and use services.

2.5.2 The best outcomes in the scenarios

The optimistic views demonstrated in three of the five Vision 20/20 scenarios indicate that communications is expected to enable or support longer life, enable people and organisations to work smarter, provide access to more entertainment opportunities and support continued economic and social development.

The world described in Scenario 1, of seamless¹ communications, is where power and influence is distributed among individuals and organisations. It is a consumer-led world with information online to make informed choices. There are responsive, innovative and competitive markets with minimal government regulation. One of the most important and challenging assumptions is that communications is available and is able to be used by all—without the need for government regulation. Some believe this assumption is fundamentally unrealistic, because self-reliance would not drive an equitable and fair society, and that the market will always be driven by economic motivators rather than social inclusion.

Scenario 1 details the commercial viability of advanced artificial intelligence (AI), and technologies that support reliable content tracking, privacy protection, filtration/search/valet services, and multimedia display. Communications technologies are highly pervasive. There is a match between the rate of acceptance by individuals and technological developments.

The self-organising environment in Scenario 1 encourages rapid innovation in technology and applications. There is seamless integration and high connectivity, with global networks and open standards. Communications business models have developed around wireless

¹ Seamless roaming across networks with the effective elimination of network boundaries and full device interoperability

connectivity, which dominate local access through the use of spread-spectrum and software-defined radio.²

Advanced quantum computing, which can generate and harvest vast amounts of information and enable a high storage capacity and substantial processing power, is a feature of Scenario 2. The scenario also envisages audio-visual recognition systems, pervasive health monitoring devices and human 'chip' implants.

The major beneficial change in scenario four is attitudinal—the perception of communications and scientific research in general has evolved. There is concurrent development and adoption of technology that has become highly pervasive and invisible to the user. There is high reliability, mostly in new (post-2004) applications. There is a common infrastructure, carriage services are commoditised, broadcast markets are open and there is ubiquitous broadband, with applications in wireless, fixed and mobile. The communications business is creative and adaptable.

Virtual reality..... in the real world

Virtual reality, telepresence and artificial intelligence are not just concepts for the future—there are excellent real life examples of these technologies being used today to improve quality of life for everyday people.

The e-health program of the Australian Commonwealth Science and Industrial Research Organisation (CSIRO) is working to further the capability, reach and effectiveness of health services.³ By using virtual reality, in particular, haptic or touch technologies, the CSIRO is assisting in the development of surgical training programs. Taking advantage of high bandwidth availability, the CSIRO is using telepresence to create virtual care units—the specialist can be in a different physical location from the point of care.

² Spread-spectrum radio—a type of wireless communications in which the frequency of the signal varies resulting in greater bandwidth than the signal would have if its frequency were not varied.

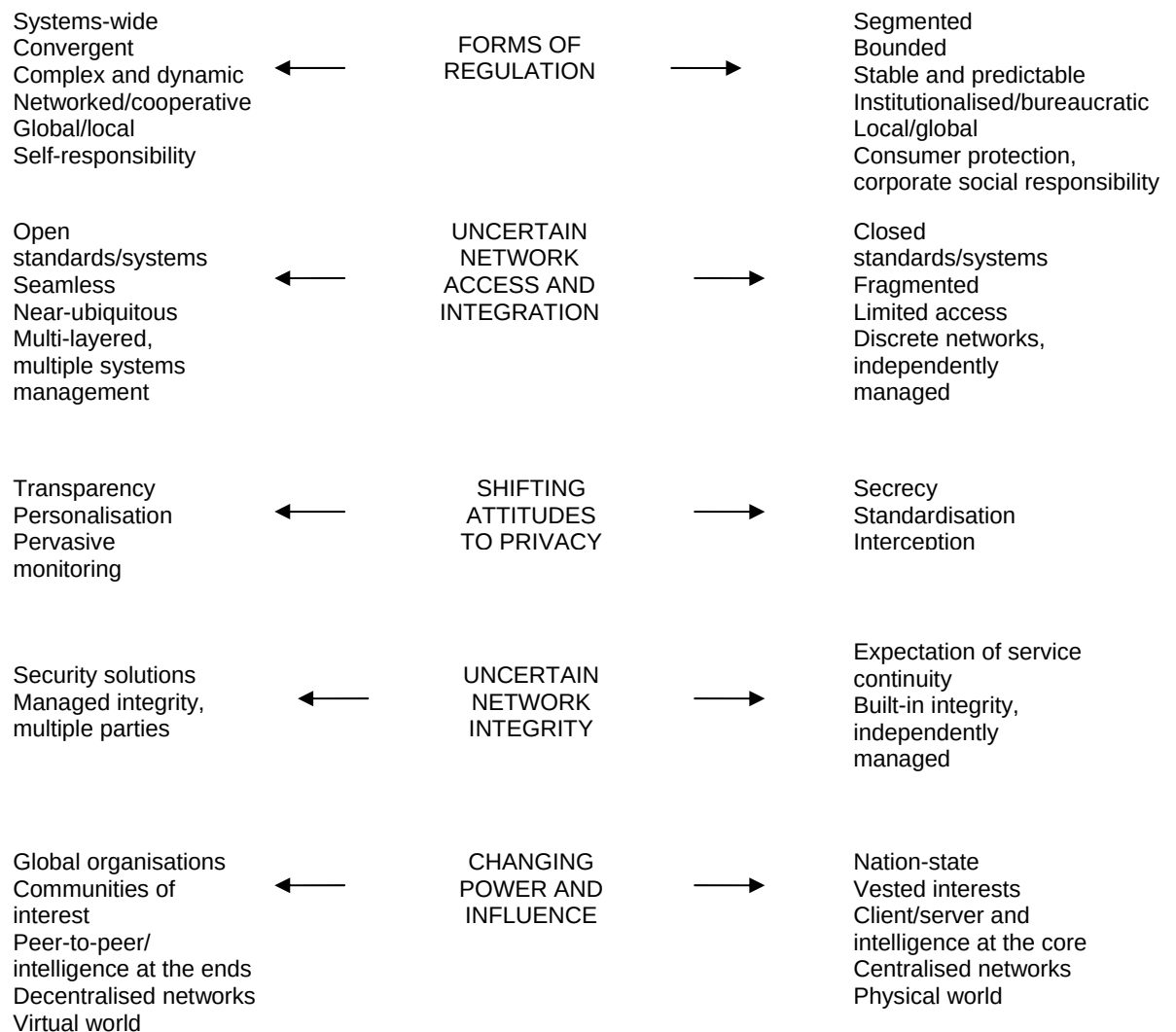
Software-defined radio—where channel modulation waveforms are defined in software.

³ http://www3.ict.csiro.au/ict/landing/channelandcontentoverview/0,,a16254_b340898,00.html

2.5.3 Tensions in the environment

Our analysis of the scenario narratives indicates five emerging tensions; the outcomes of which are likely to influence and shape consumer trust and confidence and the pace of change in the communications environment. Figure 1 provides an overview of these tensions.

Figure 1: Tensions in the environment



Current telecommunications and broadcasting regulatory frameworks assume a relatively stable operating environment with distinct boundaries, relationships and long-term planning. Experience to date shows that the bureaucratic processes for developing and implementing industry codes and standards can be time-intensive and slow to respond and change. Inertia in the system slows change.

The emerging regulatory environment—multi-layered and dynamic—requires more responsiveness and flexibility through cooperation both locally and internationally, between governments and among governments, non-governmental organisations and private interests engaged in regulatory processes.

Convergence between the heavily regulated telecommunications and broadcasting industries, and the IT and consumer electronic industries—which have traditionally not been regulated

on a sector specific basis—introduces cultural and institutional tensions in cooperate processes, such as standardisation. These tensions and value differences can act as weights on change. The near-term management of cultural differences, such as those between the telecommunications and IT industries (as set out in Appendix 2) is likely to have a significant impact on the pace of change.

Political judgements will be made about the responsibility that could be placed on consumers and the market in managing risks or whether societal risks as may be defined from time to time are managed through government regulation, legislation or other policy instrument.

There are numerous mind-shifts to work through in the emerging communications environment. Through developments in ICT, the life sciences and nano-technology, new personalised communications services and devices are expected to emerge, tailored to specific consumers and representing a major shift away from the traditional 'one size fits all' or standardised approach.

Social attitudes to privacy may go through a substantive change if consumers and citizens perceive that the benefits they gain from disclosing personal information online outweigh the disadvantages. There will be tensions and trade-offs between transparency and disclosure of personal information while protecting against harassment and the risks of cyber-crime.

Trends towards openness and disclosure are likely to be resisted where there are national security concerns or commercial risks to be managed. This may create tension between the desire for transparency and the need for secrecy.

Shifts in power and influence are expected through the continued growth and reach of globalised corporate entities, borderless peer-to-peer networking and virtual communities of interest.

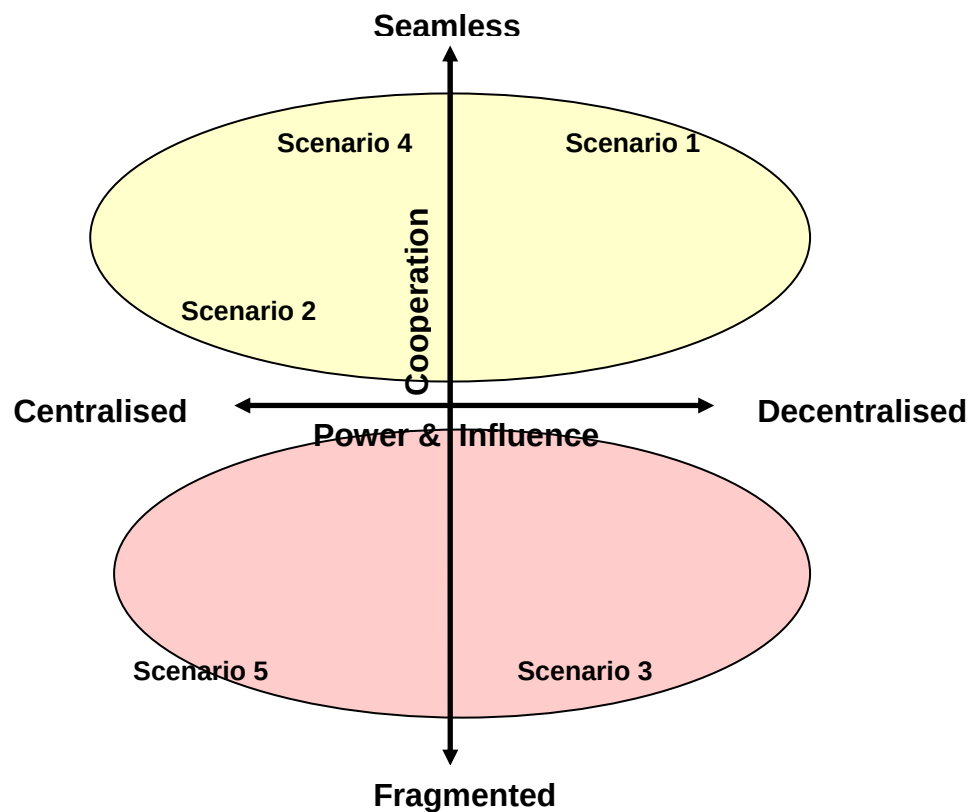
The emergence of decentralised and distributed networks, where intelligence lies at the edge and is independent of the network operator (such as user-generated content and applications) is driving changes in power and influence. The Internet provides an environment for globalised communications where new relationships can be formed and perspectives shared, forming new points of reference in shaping behaviour and values.

Internationalised communities of interest and organisations that operate beyond physical or cultural borders are likely to challenge interests that are based on incumbency and defined by geo-physical structures and localised institutions. Against these forces of change, the power of the nation-state could decline in relative importance.

2.6 Strategic landscape

The main uncertainties and themes derived from the five scenarios have been assessed and integrated with the emerging tensions outlined in Figure 1 into a strategic landscape, as set out in Figure 2.

Figure 2: Strategic landscape



In this landscape, the two key uncertainties for the future of communications regulation are high or low levels of cooperation and the relative concentration or distribution of power and influence.

Global connectivity is driving the need for cooperation locally and internationally, between consumer interests, market players, law enforcement, national security agencies and regulators. The key question is how strongly the counter-veiling forces of self-interest or national interest and different cultures and values will be. Where players in the communications environment cooperate, for example, in the development of open standards and interoperability, seamless connectivity is feasible.

The spread of power and influence of industry, government or the consumer—whether concentrated or distributed—will be shaped by trends and developments in geo-politics, globalisation, network and systems integration (client/server or peer-to-peer networking), whether systems and standards are open or closed, and the way in which people and organisations connect socially, culturally and economically.

High levels of cooperation combined with decentralised power and influence may yield a form of ever-present communications with open access to information. There would be individual and consumer empowerment, competitive markets, individual and market-based responsibility with a relatively minimal role for government regulation.

While high levels of cooperation with centralised power and influence may result in the ability to connect seamlessly, the many rules, rights and responsibilities may be dominated by governments and corporate entities and other influential groups.

Where industry and regulatory cooperation fails, the reality check is a world of fragmented, limited communication and unrealised potential. Cooperation may fail where industry, consumer representatives and government agencies lack incentives to cooperate, or where worldviews clash.

Decentralised power and influence with fragmentation is a random world of loosely defined and observed rights and responsibilities.

Centralised power with fragmentation is a world where trust and confidence is lacking through ineffective regulatory mechanisms. Communications service provision is dominated by 'walled-gardens'⁴ through closed networks using different standards and systems.

2.6.1 Power and influence

2.6.1.1 User power

Intelligence at the edge

The client-server model gained strength in the 1990s as the Internet became widely available; the worldwide web and email became critical in enabling a useful user experience. This client-server structure was supported by relatively low end-user computer power, compared with the power of the servers, and unreliable and slow Internet access, typically supplied via a dial-up modem.

More recently, peer-to-peer (P2P) network architecture has evolved where networked computers have relatively equal capability. Communications have moved out to the network edges where home computers are now communicating in a way that was previously reserved for substantial server computers.

This distributed and open communication infrastructure of P2P systems transfers power from the service provider to the user. Peer networks enable new forms of social interaction including P2P file sharing and networking. Open systems enable people to build their own networks, create their own multimedia content and make their own voice over Internet protocol (VoIP)⁵ calls, relatively independently of the carrier or carriage service provider. P2P networks can reproduce and distribute content at low cost.

Assuming that open access to systems and content in the pervasive networking future—described in some of the scenarios—is actually realised, there would be far-reaching implications from the growing power and influence of individual users.

The Internet is fundamentally a collection of networks managed by group consensus rather than decree, as are traditional circuit-switched networks. P2P systems are able to be implemented in a fully distributed manner and do not rely on any centralised control.

One of the most powerful characteristics of P2P systems is that P2P networking can grow organically rather than requiring a planned rollout implementation plan. Even transitional control measures that provide connectivity between the public switched telephone network (PSTN) and the domain name server (DNS), such as the ENUM⁶ protocol, may not be necessary in the longer-term, assuming open-source alternatives for locating Internet gateways to telephony services are mainstreamed and substitute the need for centralised systems. While the outlook is uncertain at this stage, it is plausible that open-source alternatives emerge as being complementary or even a substitute to the ENUM standard.

It is difficult to mandate new systems where everyone is required to implement specific changes en masse. Organic rollout, that is, initial implementation by a small number of users, which grows as more users find the application/system of value, is more likely to succeed than systems requiring a global mandate. This issue can be clearly demonstrated, for example, with the delay in implementing technical solutions to spam or IPV6.

Globalised peer networking expands social, cultural and political spheres for individuals and creates virtual communities of interest. While most social interaction will continue to be local, individuals and social groups that have traditionally been defined in terms of their local and

⁴ Where access is controlled, for example, by a subscriber-based service or restricted access sites, such as those with adult content, or through technical incompatibility

⁵ Voice over Internet protocol (VoIP) refers to the technologies that have been developed to transfer voice in digital format using the Internet protocol (UDP/IP).

⁶ <http://www.enum.org/>

national context alone will increasingly need to be considered in terms of their global social networks.

This 'power at the edge' is not to be underestimated. It has a fundamental impact on many traditional 'sacred cows' of regulation such as interception or network security, as well as impacting potential network integrity.

Traditional user devices such as first and second generation mobile phones, fixed telephones, analogue TVs have limited user-defined functionality and inflexible protocols because of inherent protection of the network on which they are or were located.

Powerful edge devices such as SIP⁷-enabled mobile handsets or Internet-connected PCs enable users to have an unprecedented impact on networks. This is demonstrated by the current problem of spam. Most spam is actually sent out by unsuspecting PC users having their computer compromised by a spammer.

2.6.1.2 Informed consumers

A consumer-led environment is more likely to develop in a world of seamless, ubiquitous connectivity than in one of fragmented communications. An educated, informed environment would evolve through multiple layers of information in the environment between buyers and sellers. Consumers would be likely to build on early examples of reputation-based or trust-based rating systems, such as that developed by eBay users.⁸ Service providers would have an incentive to go to the consumer online to understand their preferences rather than the consumer having to seek out information about what options are available.

2.6.1.3 Digital content

According to Merrill Lynch, the world is entering a new wave in technology development based on the production and interactive usage of digital content online, such as games, TV programs, and music and video.⁹

In a globally and locally networked world, local media channels compete with an increasing range of internationalised digital content sources. Mobile network operators and ISPs are investing in online content and working with content providers. User-generated content, such as videos or digital photos, weblogs (blogs) and file-sharing, is on the rise.

Content is no longer generated and distributed largely by the mass media alone—convergence is creating new channels for production and distribution of content such as TV programs, Internet content, video and audio streaming over fixed and mobile devices. Information services based on location will add to the increasingly personalised flavour of digital content. Due to younger people using digital technologies and the Internet, in 10 years the average age of consumers of information radio and TV channels in Europe could be more than 60 years, while TV network in the US is losing viewers and advertisers.¹⁰ The ability of the mass-media to influence large parts of society may be in decline.

⁷ SIP—session initiation protocol

⁸ <http://pages.ebay.com/securitycenter/index.html>

⁹ Cited in Alcatel's submission to the Vision 20/20 Preliminary Report

¹⁰ *The Future of Media & Entertainment*, background material for the Summit for the Future, January 2005, Club of Amsterdam

Online gaming – fun for all ages

In 2003, it was reported that online gamers outnumbered online shoppers by two to one in China and Malaysia, something reflected in areas like Korea, India, Singapore and Hong Kong.¹¹ Largely driven by the popularity of multi-party gaming, the trend is also encouraging the development of family-style, easy-to-play games.

The success of the SimCity games¹² is testament to this. The Sims lets you create and manage people, their lives and homes. Will Wright, the creator of the games said "I wanted a dollhouse that boys could play with and a strategy game that girls would enjoy..."¹³ Registered game users are of all ages, and almost 40 per cent are female.

2.6.1.4 Globalisation

All of the Vision 20/20 scenario narratives assume a globally integrated communications sector, albeit to varying degrees.

International standardisation is expected to continue, facilitating global connectivity. Scenario 1 discusses international standards, as does Scenario 2, with national variances and applications. Scenario 3 has global collaboration through bilateral agreements. In Scenario 5, there are also international standards developed through a shared national and international security philosophy. Scenario 4 describes a world that is dynamically globally engaged and Australia takes a leadership role, including in developing global spectrum protocols and communications system standards.

The effects of global connectivity are uncertain. Two plausible but quite different outcomes are possible. Greater global interaction may blur the significance of national sovereignty, creating divergent loyalties for individuals and communities of interest. Communications user access to multiple reference points internationally may influence behaviour and reshape values. Over time, this may limit the ability of any one jurisdiction to articulate shared values based on a broad national consensus.

Alternatively, in an increasingly diverse and complex world, citizens may turn to governments to represent and promote national identity and protect their cultural values.

Virtual communities of interest can be expected to take greater advantage of global connectivity to share information and cooperate in achieving shared goals. In the communications sector, these virtual influencers are likely to include consumer or special interest groups.

Globalised or regional communications entities have the potential to play either a domineering or a cooperative role in standardisation and regulatory coherence. In the absence of countervailing government-led measures at the global, regional or multilateral level, multinational corporations may be able to set their own communications standards, including those that affect social and environmental outcomes. Governments may fail to keep pace with change or have reduced capacity to exercise sovereign authority.

Continued globalisation is expected to drive increasing investment and innovation in rapidly developing countries such as China and India. These developments are likely to:

- shift the focus of standardisation from the West to the East
- place more emphasis on 'the Asian way' of building and maintaining social systems of trust and mutual obligations in business, regulatory and standardisation processes and
- infuse emerging communications applications and services with an Asian as opposed to Western flavour

¹¹ <http://asia.cnet.com/news/personaltech/0,39037091,39107161,00.htm>

¹² http://thesims.ea.com/index_flash.php

¹³ <http://archive.gamespy.com/articles/january01/interactive/>

The Vision 20/20 scenarios detailed expectations of unchecked globalisation—this was not universally endorsed in international feedback. Potential threats to ongoing economic integration include:

- because the advantages of globalisation are not distributed universally, reactionary forces may gain ascendancy or the ‘digital divide’ may grow to the point where growth is undermined
- there may be localised or global economic shock or
- a global pandemic.

2.6.2 Cooperation

The Internet is global and lies beyond the control of any one network provider or regulatory jurisdiction. This shared interest in the operation of the Internet is driving the need for cooperation locally and internationally.

A substantial regulatory challenge in an environment of complexity, uncertainty and fast-paced change is to be responsive. The emerging environment—multi-layered and dynamic—requires more cooperation both locally and internationally between governments and among governments, non-governmental organisations and private interests.

Scenarios 1, 2 and 4 envisage the development of seamless, ubiquitous global connectivity. The substantial scale of network and systems integration and device interoperability that would be necessary is considered to be plausible but challenging. These strategic environments presuppose a broad-based, internationally cooperative and integrated approach to the development and implementation of:

- seamless network connectivity, device interoperability through open standards
- an equitable user experience; social inclusion and affordability
- peering arrangements for network interconnection
- seamless portability of content
- new business partnerships within a multi-layered value chain
- inter-working of business and operational systems
- inter-working of national security and law enforcement
- coherent and compatible regulatory frameworks and
- agreed e-government and e-commerce frameworks.

2.6.2.1 Incentives to cooperate

Assuming that a cooperative infrastructure is possible, it will be important to determine the underpinning incentives and drivers. An industry prerequisite would be a business-based incentive, such as enhanced economic benefits of increasing user trust and confidence in communications services. Other drivers of cooperation include:

- globalised distributed networks and markets forcing international collaboration to solve shared problems such as spam and network integrity
- converging industries and regulatory frameworks driving the development of new operating systems, business processes, standards, guidelines and other rules, and
- the social and economic benefits from distributed networks offering new and dynamic channels, allowing information sharing and networking between individuals and organisations that is responsive, innovative and adaptable.

2.6.2.2 Importance of competition and innovation

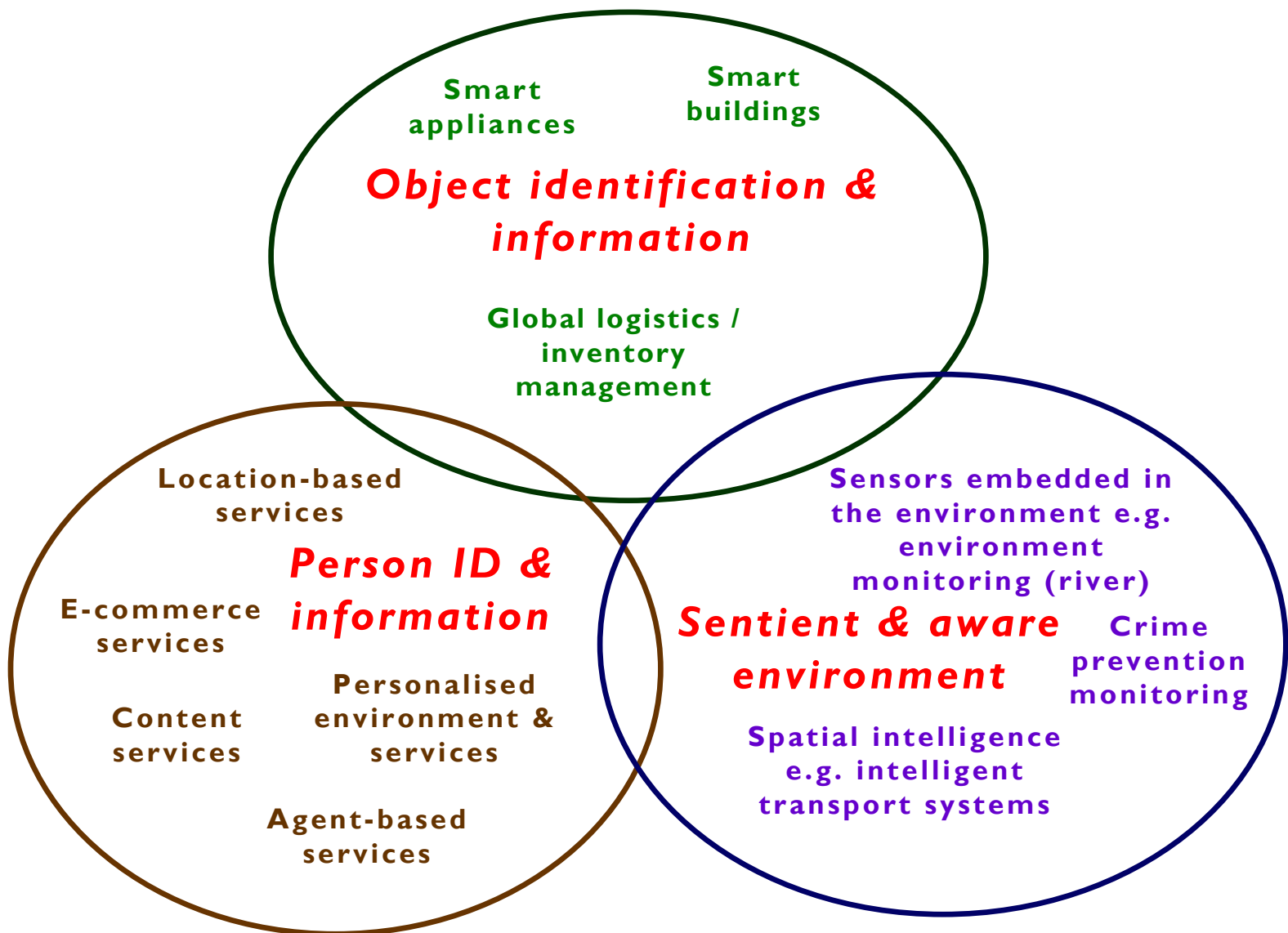
Cooperation is not a substitute for competition. A competitive marketplace is the main driver of innovation, choice, and quality of service. Cooperation plays a supportive role in

developing rules and standards for effective network interfaces, growing markets and building user confidence. Cooperative frameworks and processes must be dynamic and responsive to market forces.

2.6.3 Ubiquitous communications

Should a world evolve in which there are globalised, competitive markets, with high levels of regulatory cooperation and distributed power and influence, the conditions may be in place for ubiquitous communications as depicted in Figure 3.

Figure 3: Ubiquitous communications



In this world of ever-present communications, devices, machines, materials in the environment would have computing embedded along with network connectivity—a world in which there is object identification and information, an environment that is 'self-aware', with personalised information and services and any person-to-any person connectivity. The technical aspects of communications would recede into the background of our lives—it would simply be 'there', rather than having to go to a specific telephone, TV or other device.

Such an information-rich world where people, objects and sentient¹⁴ environments are 'always on, always connected'—being permanently connected to the Internet—could change the way

¹⁴ Feeling, conscious

in which we work, play and receive services. The Internet and other emerging communications technologies are enabling—they allow people to build new relationships and communities and encourage the exchange of information and services for mutual benefit. The consequential new wave of social, cultural and economic forces may drive profound changes in society and enable a complete change in the ways users interact with the network, as well as in the nature of networking itself.

Vision 20/20 has made certain assumptions about the feasibility and desirability of a world of ubiquitous communications. The project suggests that ubiquity could be a 'best possible outcome'. This pre-supposes that users want ubiquity and that a ubiquitous environment is promoted, or indeed provided, by government and industry.

2.6.4 Pre-conditions for ubiquitous communications

There are formidable challenges in the pursuit of ubiquitous communications—change may not occur rapidly, may not be universally experienced across all geographic and social groups, and is unlikely to be fully globalised. Table 2 sets out the pre-conditions for a ubiquitous communications world, categorised into the communications elements of:

- technology
- market dynamics
- users and
- rules and guidelines

The issues outlined in the table are discussed below. Consideration is given not only to the prerequisites for ubiquitous communications, but also the fragmented alternatives.

Even assuming substantive advances are made in meeting the challenges outlined below, it will take many years for legacy systems, legal systems, regulatory frameworks and processes to integrate with the new.

An optimistic forecast for those countries at the most advanced state technologically and economically is for the main components of ubiquitous communications as defined in this report to be in place by 2015.

Table 2: Pre-conditions for ubiquitous communications

Technology	Market dynamics	Users	Rules and guidelines
• Decentralised, distributed systems • Multiple IP-based access networks (wired, wireless and satellite) - o migration from circuit switched networks to end-to-end IP - o seamless handover between networks - o open platform interface architecture and systems integration - o self-organising wireless sensor networks, tracking and position location - o migration to IPv6 • Transition to digital TV complete • Peer-to-peer technology • Smart technology that enables the user to be unaware of the background technological complexity • Location-aware applications & devices • Information encoded in the physical-digital landscape • Flexible use of radiofrequency spectrum	• Partnerships and alliances • Multimedia and information service bundled as a standard • Content and service aggregators • Network access integrators • New business models • Global reach through global connectivity • Niche markets	• Simplicity of use • Confidence and trust through network integrity • Willingness to be always on, 'always connected' • Participation for all through digital accessibility, affordability and useability • Widespread acquisition of e-skills • Personalisation of services • Ability to avoid harmful, nuisance or illegal content • Reasonable personal privacy maintained within a global market	• Open standards enabling borderless interconnections between portable or wearable devices, and operating system and network independence, including peer-to-peer (P2P) networking • Agreed e-government & e-commerce frameworks - o online identity management and protection - o secure agent-based computing - o network reliability and security - o standardised, secure and easy to use payment systems, including micro-payments¹⁵ - o reputation mechanisms - o availability and reliability of alternative dispute resolution services that can handle end-to-end service delivery problems on an international basis - o ability to opt-out - o dealing with intellectual property rights (eg. automated DRM) • Seamless portability of digital content • Harmonised rules for technology neutral open access to content • Public confidence in EMR safety • Appropriate safeguards for country-specific issues such as USO and local content • Effective cooperation between national law enforcement agencies • Global standardisation bodies that maximise efficiency gained from cooperation while encouraging innovation • Network changes/improvements are be effectively coordinated and managed

¹⁵ Payments less than \$10

2.6.4.1 Technology

Infrastructure

While the transition to digitalisation and IP-based communication has begun, it is difficult to estimate the time it will take for legacy systems to be phased out. The pace of change will vary from country to country, region to region. Emerging networks, protocols and developments such as quantum computing are all expected to support higher data transmission and processing capacity over time. In urbanised Australia, a transition period of 15 years for near ubiquitous communications is plausible.

The multiple, IP-based networks of the future are likely to be combinations of optical fibre cable, fixed, mobile and ad-hoc wireless. Lower-cost digital satellite systems and broadband over powerline communications are evolving and may have significant potential. Advances in digital subscriber line (DSL) capacity may support a longer shelf-life for the copper network.

Radio networks play an important role in all of our scenarios. Wireless provides Internet connectivity on the move and away from the home or workplace—in other words, the convenience of being always on, always connected. Deployment of wireless networks in the home, car, public areas and road networks, as well as in buildings and the environment generally, will be necessary for near-ubiquitous connectivity. Ambient intelligence assumes low-cost, ubiquitous wireless networks.

Although wireless has significantly lower capital costs than fibre, some project participants were concerned about the viability of wireless business models. Developing economies in Africa and Asia may leap-frog the developed world by deploying wireless networks in preference to wireline infrastructure.

One threat to wireless networks may lie in growing negative perceptions about, or incontrovertible evidence being established about adverse electromagnetic radiation (EMR) health effects from mobile devices. The National Radiological Protection Board in the UK recently reported that taking a precautionary approach to the use of mobile phone technologies should continue to apply.¹⁶ In its submission to the Vision 20/20 preliminary report, the EMR Association of Australia also advocated a precautionary approach.¹⁷

It is likely that wired infrastructure will continue to play an important role. Even if wireless communications were to have a larger role, the need for a core network such as one using optical fibre cable is expected to continue and existing fibre networks would continue to be employed. The higher data rates and reliability of service currently provided by fibre networks makes them more attractive than wireless services.

Seamless handover

Being always on, always connected assumes that communications sessions—whether a phone or video call, viewing a TV show or movie, or sending and receiving messages—use devices or nodes that are capable of receiving and transmitting sessions to other devices over multiple networks with blanket.

IPv6

Internet Protocol Version 6 (IPv6) is the next generation protocol designed to replace the current IPv4. While IPv4 is used for most of the current Internet, there is a shortage of IPv4 addresses, which are required by all new Internet-connected devices.¹⁸

Perhaps the most well-known attraction of IPv6 is the exponential increase in the number of public IP addresses. Other enhancements that IPv6 offers over IPv4 include:

- improved security, with IPsec—IPsecurity, an IETF protocol to support the secure transmission of packets over the IP layer—being mandatory

¹⁶ http://www.nrpb.org/publications/documents_of_nrpb/abstracts/absd15-5.htm#exsum

¹⁷ <http://vision2020.aca.gov.au>

¹⁸ <http://www.ipv6.org/>

- improved quality of service—better transmission of real time, high-bandwidth videoconferencing and voice over IP and
- ease of network configuration and operating efficiency improvements.

Transition to digital TV/radio

The digital TV set may become a central portal for digital content in the home, assuming the deployment of high-bandwidth wireless connectivity to every other digital device. Digital TV or radio could transmit video or audio streaming from the Internet, assuming digital rights management (DRM) and payment issues are managed effectively.

The transition to digital TV and radio broadcasting will free up spectrum used for analogue transmission.

Dual mode mobile handsets that recognise digital terrestrial television and third generation mobile technologies have already been released for the Korean market.¹⁹

Peer-to-peer networks

It is likely the use of P2P will increase, due to a number of fundamental drivers:

- The philosophy of the original Internet design was for it to be P2P in use.
- Mobile devices with Internet connectivity and increasing computational power are emerging rapidly.
- Application developers have realised that P2P applications can be much more efficient than traditional client-server applications.
- P2P systems are much easier to roll out, providing a strong incentive for developers to develop P2P rather than client-server systems.
- The power, bandwidth and connectivity characteristics of edge-connected computers, that is, normal computers connected to the Internet, mean that they can now participate fully in a P2P structure, which was not the case even 12 months ago due to delays in consumer broadband internet access take-up.
- The traditional client-server structure is reaching the end of its development life and there are fundamental limitations associated with throughput and uptime—P2P structures offer technical superiority.
- P2P systems often allow users to circumvent the interception and censorship limitations of client-server systems due to the difficulty in defining a common 'interception point' within the service setup/delivery path. While an interception point may often be possible in a P2P transaction, it is important to differentiate between the act of interception—the physical collection/copy of data bits—and the practical aim of interception—actually deciphering the data bits to make sense). P2P allows for a unique encryption strategy to be determined between the two parties, making meaningful interception more difficult.
- Open source P2P protocols are emerging that provide similar functionality to the ENUM protocol in providing interconnection between VoIP and the PSTN, and the advantages include:
 - o being more technically robust than ENUM systems because they are distributed, it is much less likely to suffer single point sensitivity failure
 - o implementations can grow organically rather than being a 'single shot', as in the case of ENUM systems where governments typically provide implementation
 - o no action is required by government or regulators to implement
 - o developments of this kind may have a large-scale installed base before ENUM is commercially released, thereby making ENUM obsolete
 - o the spam and privacy security controls are superior to those for ENUM and
 - o systems can bypass artificial charging structures that local carriers may implement through ENUM and thus disrupt traditional carrier revenue streams.

¹⁹ strategy + business, *I want my DTT*, 1 Feb 2005.

2.6.4.2 Market dynamics

In transition

Convergence of the ICT, consumer electronics, broadcasting and telecommunications industries is being driven by digitalisation, increasing computing power, higher-bandwidth IP-based access networks (wired and wireless) and open standards. Previously distinct services are coming together as part of the emergent Internet environment.

In revenue terms, IP-based communications may exceed 50 per cent of telecommunications revenues in Australia within the next five years. VoIP may drive a rapid decline in voice revenues. Scenario 4 assumes an industry-wide agreement to provide voice calls at no cost.

As revenues from traditional (not online) broadcasting and voice services decline, established telecommunications and broadcasting operators will need to develop new products and services with new pricing models and payment systems. New entrants to the market may also have a dynamic effect on market structure and the pace of change.

Businesses that fail to adapt quickly with new business models and technology are likely to go out of business. While at one level this can be seen simply as the free market operating as it should, the loss of large businesses can have a disruptive impact in areas including employment and quality and continuity of service. This disruption can affect market or consumer confidence and negatively affect commercial investment.

Business models – value lies at the ends

The value of IP-based communications lies in the end uses—not in the carriage of services, but the use of it. As such, there are likely to be emerging niche markets for value added services. This is encouraged by the multi-layered nature of IP-based networks that de-couple the underlying infrastructure from applications and content layers. While new business models will evolve, the emphasis in the near term will be on building new partnerships and alliances within the multi-layered IP-based environment to drive innovation.

Decentralised and distributed communications systems may destroy older business models and allow innovative services to develop. Over time, the more successful business models could build economies of scale and scope, tending towards centralisation and market dominance.

In IP-based networks, voice, multimedia content and data are no longer discrete services over separate networks. These different modes of communication are expected to merge together to a fluidity of choice—for example, talking to the sender of a message if they are online and 'present' at the time.

Innovative uses of P2P systems are emerging, such as providing controlled content distribution²⁰ and peer-based access to trusted webs of communication servers for telephony purposes.

Businesses that provide software agents and devices (which one Vision 20/20 participant described as the 'external brain') to make it easier for people to process information and use communications services and applications, through bundling, personalisation of entertainment and voice or video calling and messaging integrated at the customer interface, are likely to succeed. The human—individual and organisational—need to process and control information is likely to drive innovative applications and services.

Retailers of entertainment services online could add voice, information and payment services together with least-cost network access to provide their customers with integrated communications service packages. The Internet provides an opportunity for a relatively small firm to achieve broad scale and scope through lower barriers to entry and global connectivity. An exponential increase in competitors would complicate the supply chain.

Emerging business models focusing on m-commerce services, such as the financial services sector, large-scale retailers or media companies, may act as mobile virtual network operators to promote their brand and facilitate electronic commerce.

²⁰ Instead of being a peer-only network, a centralised computer would control what content to make available for peers to download.

Creators of music, movies or other forms of entertainment can place their work online, independently of legacy distribution and reproduction channels. The same 'direct to the consumer' channel is available to music and movie producers as well, bypassing wholesale and retail distribution channels.

The Vision 20/20 scenarios assume that services will be provided globally and independently of the physical location of the service provider by 2020. Global networks and concentrated markets are likely to increase the role and influence of the big consultancy firms and influential individuals that shape corporate governance principles and practices.

Vendors are moving up the value chain to provide network operations services to incumbent telecommunications providers, leaving the latter to concentrate on revenues and marketing. Systems architecture and hardware suppliers might move up the value chain to supply bundled content and other services, such as music, movies, digital TV, games, voice/video, messaging and information services—directly to end users. Just as mobile phones are subsidised to build the market, consumer electronics and home network devices may also be subsidised to encourage take-up.

There is growing interest from utilities and transport network providers to make their networks available for communications purposes and to invest in emerging broadband wireless networks.²¹ In a world of ubiquitous connectivity and computing, utility-like network providers could provide end-users with systems integration or bandwidth as required—whether the end use is for video streaming, interactive games or integrated messaging—with payment adjusted according to use.

There is likely to be a continued demand for legacy mass media broadcasting services in the forecast period, although the size of this segment will diminish over time. Digital natives—those people that have grown up with digitalisation—are more likely to opt for alternatives such as interactive multi-party games, webcasting and user-generated media. It is plausible that broadcasting channels will evolve into networked content aggregators targeting passive consumers with a preference for packaged news and entertainment services.

A key uncertainty is whether effective digital rights management (DRM) standards are developed and, if so, whether the standards are open or proprietary. Control of DRM standards would provide market power. It is likely that new developments in payment and business process operating systems that enable transaction or subscription-based access to content will emerge. Such developments may encourage a modularised market structure to emerge.

Investment drivers

There are uncertain and complex relationships between investment in network infrastructure and IT systems architecture and devices with Internet connectivity such as consumer electronics. These investment risk factors may drive consolidation of business interests through mergers or business partnerships, increasing size and scale in the emerging communications sector.

Over the next five years, network infrastructure investment decisions are likely to be based on perceptions of emerging communications value chains for the next 10–20 years. Our scenarios and international research include the possibility of:

- carriage as a commodity that is separate from the delivery of applications and content
- systems integrators offering bundled services at the customer interface, presumably on an 'always best connected' choice of network
- global and regional network service providers
- modularisation—different combinations of physical and logical network layers to provide content services
- the growth of private networks and private media and

²¹ A recent example is US utility Columbia Energy's Wi-Fi network covering 9,500 sq km. See http://www.infoworld.com/article/04/08/23/HNwifiwash_1.html

- open wireless and 'infrastructure-free' radio networks accessible on an ad hoc basis.

Other drivers of market growth over the next few years are the migration to broadband access in the fixed network, a more rapid transition to broadband wireless networks for mobile connectivity and continued growth in computing power and network data rates.

The design of network infrastructure will be directly affected by the willingness of users to pay for content. Given the likely level of traffic for higher-valued content, one of the key uncertainties is how such price discrimination would be made available for investment decision-making and access pricing at the physical layer.

The situation can be made more complex depending on assumptions about ongoing peering arrangements—whether termination fees replace them. These assumptions include the competitiveness of other network interconnection agreements between carriers and ISPs, and the potential for carriers to manipulate end-to-end quality of service such as voice or real-time video traffic, depending on the originator of the traffic. Market dominance issues may justify government regulation where competitive arrangements are not set by commercial agreement.

One of the challenges in achieving ubiquitous communications across jurisdictions is whether regulations provide the right conditions for firms to invest in innovative services. Regulations that are hard to follow or that are inconsistent, within jurisdictions and between jurisdictions, are likely to act as disincentives to investment.

Trends in convergence and increasing demand for globalised networking are likely to place pressure on governments to remove regulatory barriers that may lie in the way of development. Regulatory coherence is as important as the path that regulatory convergence might take.

2.6.4.3 Users

Network reliability and integrity

Network integrity is often misinterpreted as 'network security'. Integrity relates to the more humanistic concepts of trust, belief in and intactness. Security is a subset of this issue and refers to prevention of access to, or use of, data and resources without authorisation. In this project, when looking at the communications network, consideration was given to how the converging domains of IT, traditional circuit-switched telecommunications, next generation networks, the Internet and content provision are managing the issue of integrity.

In an increasingly information-rich environment, the integrity and reliability of the communications infrastructure—and of the data collected, used, shared and stored—is critical. The ability for individuals and organisations to confidently release information into the communications network, private or open, to be able to authenticate and verify information and to know that the right information will be available at the right time is essential. The ability to have uninterrupted supply of communications services will increase in importance.

As governance and communications infrastructures become more intertwined, the relationship between communications, the integrity of the system and the individuals and organisations that operate within it must be understood. It is also important to identify areas of weakness or vulnerability that undermine both the communications infrastructure and the trust that people may have in their communications.

By its very design and nature, a traditional telecommunications network has built-in integrity. The protocols used between operators or carriers were designed to ensure that only trusted information could pass between parties. With limited exceptions, for example, listening in to first generation mobile phone conversations with a radio scanner, it is technically very difficult to compromise the network.

A network attack—an event where often malicious traffic attempts to overload a part of the network and reduce network performance—is near impossible in traditional circuit-switched networks. Such networks have the so called 'five nines' of network uptime—99.999 per cent uptime—less than four minutes downtime per year. It has become a social expectation that the network will always work and always be secure, for example, even when the power goes off, users still expect the telephone to work.

The rise of broadband-connected home PCs has highlighted an emerging network integrity problem, with such PCs often not having the security systems such as firewalls and anti-virus software that business users have. Consequently, there are literally millions of computers at the network edge that can cause significant network disruption, for example, through virus attacks or spam. There are strong cultural drivers within the ICT industry that encourage unregulated device connection and the number of network-aware devices is expected to rise exponentially.

The transfer of power to users raises network integrity control risks. Under distributed, decentralised systems, it is difficult to determine where responsibility lies for the management of risks such as spam, spyware, phishing and denial of service attacks. Due to the open nature of the Internet, one person or a small number of people can do immense damage, either knowingly or unknowingly.

The Internet's designers—the Internet Architecture Board (IAB)—state²² that primarily it is the ‘...responsibility of the end users to protect themselves’ in issues related to confidentiality and authentication when using the Internet. As the Internet has expanded its user base to include less skilled parties, the question of whether all users are able to protect themselves has arisen.

Solutions to network integrity problems are likely to involve vendors, service providers, industry and government in developing guidelines or rules, such as:

- end-user education and awareness
- technology solutions built in to devices and terminals
- ‘fit for use’ compliance regimes for devices
- mandatory risk management for users, such as requirements to keep virus and spyware protection software up-to-date
- strong network boundary management, where tight control is made of traffic flowing in and out of a particular network at a carrier, regional or national level and
- mandatory denial of connection to the network for failure to protect devices.

Carriers may also invest in the provision of public or private IP networks—either not connected to the Internet or where Internet traffic is through partitioned routes—that offer enhanced security and quality of service while supporting a range of IP-based applications. A downside to this would be the loss of peering.

There is likely to be more separation between infrastructure layers and content than has been the case historically. Customers continue to complain to their infrastructure provider about issues beyond their control, for example, complaints to ISPs about spam and obscene web content. This trend will create challenges for boundary management. Traditionally, most consumer problems could be addressed by the local carrier, but this is less likely to be the case in future.

Problems that cause denial of service, network disruptions and computers that ‘crash’ will need to be resolved. The answer may lie in automation. Rather than having IT staff employed by organisations or consumers managing their own risk with home networks, systems architecture would evolve to the point that computers and networks would be able to self-configure, self-heal, self-optimize and self-protect.²³

This automated vision assumes the existence of smart networks, as opposed to, or as well as, intelligence at the edge, with the following features:

- interoperability
- open standards and
- backwards compatibility with legacy systems.

²² RFC 1958 June 1996 Architectural Principles of the Internet IAB

²³ “Spare me the details”, A survey of information technology, The Economist, October 30, 2004

Participation

The current policy objective of regulation is to secure access to communications services for everyone at a reasonable price. While access will continue to be of high importance, the ability to use computerised devices will be critical to the effective uptake of e-government and e-commerce, and to allow people to effectively interact, cooperate and to share information.

For Vision 20/20, ubiquitous communications assumes that virtually everyone would be permanently connected to the Internet and the concept is inclusive, not exclusive—the experience is available to all.

Everyday use of ubiquitous communications accessible by all assumes there are no or minimal technical or user interface barriers to take-up or use—ubiquity assumes simplicity of use and universal design. It also assumes availability—that the consumer can afford to buy, install and maintain their personal communications devices, and that ongoing services and support are available.

Communications technologies can minimise and exaggerate lack of opportunity or ability and any progress towards communications ubiquity will need to take these challenges into account.

The nature of communications-related social, economic and digital exclusion must be understood—the gap between people who can make effective use of communications technologies and those who cannot. Consideration must be given to the ways in which technology can bridge the divide between differing levels of infrastructure, literacy and economic participation.

The rate of change driven by digitalisation and Internet technology in the last five years has already left many citizens behind. For example, many people are simply priced out of the market. Many websites and digital or pay TV services are not readily accessible to blind people. The failure to meet this challenge is the foundation of the so-called ‘digital divide’ in society. From one perspective, emerging technology and devices are merely tools that illustrate and exacerbate existing areas of social disadvantage.

Consideration must also be given to the right or desire to opt-out, or take information holidays. Some people just aren’t interested. A 2003 Greater London Authority report, *Connecting people: tackling exclusion?* looks at individuals that simply lack interest in using ICT devices. The report states that, while numbers of non-users by exclusion have decreased since 2001, the number of people who *choose* to be non-users has remained relatively constant.²⁴

The ability to control and process information will be an important factor—people cannot opt out of something they are not aware of. In the extreme, it is plausible that content may not differentiate between fact and fiction, which may have new and potentially troubling social consequences. Information management, including consumer information awareness programs, is likely to emerge as an important issue for regulators.

Exclusion by language is a factor—the Internet is a predominantly English forum and yet probably less than 10 per cent of the world’s population speaks English as a first language. Within Australia, Indigenous and migrant populations may be excluded not only by language and culture, but also by infrastructure.

In addition to pricing, consideration must be given to the development of adequate e-skills and the implementation of ‘universal design’ functionality. Regulators and the industry will need to consider not only the availability of infrastructure and consumer awareness programs, but also information literacy skills and the needs of groups in society on the basis of physical, mental and intellectual ability, English language ability and text literacy skills. For example, prerequisite skills would be necessary to use online dispute resolution services.

Personalised service delivery and the ability to take advantage of choice require individual empowerment. Devices or applications that are not able to be used by some people due to disability or lack of skills not only creates but worsens existing disadvantage and social exclusion.

²⁴ <http://www.london.gov.uk/gla/publications/e-london/connecting-commties.pdf>

What is universal design?

Universal design is a proactive approach to designing and delivering products and services that are usable by the widest range of people, irrespective of ability or disability.

Universal design takes into consideration the changes experienced by everyone during their lifetime. Rather than focus on adapting things for an individual at a later time, an accessible environment is created from the beginning.

An example is the OXO Good Grips range of kitchen utensils²⁵, developed in the United States in response to a potato peeler that was unwieldy and painful to use. The founder of a major industrial firm worked with designers to create a peeler with a rubber handle. The Good Grips range was expanded and universally adopted—because the products were easy to use, even for people with limited strength or dexterity. Incidentally, these products were more expensive—the market was and is willing to pay a bit more for the right product.

Privacy

All of the Vision 20/20 scenarios assume pervasive monitoring of the individual. By 2020, all electronic communication sessions and commercial transactions may be tracked and recorded. While the potential convenience and productivity gains from ubiquitous connectivity is conceptually attractive to many people, it is also plausible that people will have an adverse social reaction to sensory environments and the tracking and storage of personal information by third parties.

The scenarios identified a wide range of potentially intrusive regulatory activities and they suggest that individuals may try and hide. The public may be less tolerant of intrusion and more suspicious of surveillance.

People are likely to be always connected, always online and increasingly reliant on personal identifying information to gain access to and use services. Innovations in data storage and processing powers could mean that a lot of personal information is collected with consequential privacy and security implications.

The expected introduction of location-based services will be an early test of privacy frameworks. Social attitudes to privacy are likely to be shaped by consumer and citizen perceptions of benefits gained from the disclosure of personal information, and how information can be used to identify a person and their habits.

The globalisation of services also adds significant complexity to the privacy debate. Often countries have quite different privacy requirements and it is increasingly becoming the case that services are delivered via multiple countries. For example, a mobile user could access a WAP service from a content provider in country A, the users' mobile provider in country B and the actual carrier in country C. In such cases, it will be difficult to guarantee that all countries involved handle privacy to the user's expectations.

The ability to control identifying information is an important factor in consumer trust and confidence—awareness of consumer protection mechanisms and of the ability to simply opt out remains an issue. Small businesses and individuals are less likely or less able to protect their privacy. Consumers need to gain a greater awareness of how their information is used and they need to be taught how to protect themselves.

Identity management, and the ability to verify and authenticate this identity, is becoming increasingly important. There is a new understanding of how individuals and the equipment they use can be identified, how identity can be exploited and undermined, and how identity, privacy and security are inherently interrelated.

The Vision 20/20 findings support the principle behind the Australian Federal Privacy Commissioner's proposal to move privacy protection away from the sole and current concept of identification, as currently represented in the privacy framework.²⁶ As people's lives are increasingly led online, identifiers may not bear a resemblance to traditional physical concepts

²⁵ www.oxo.com

²⁶ <http://www.privacy.gov.au/>

of identity. While individuals may move away from traditional identifiers, the newer protocols such as email addresses, avatars and Internet banking passwords are no less indicative of identity.

Many people are not necessarily opposed to sharing personal information that is collected about them—feedback indicated that people who are aware that their identifying data is being collected are less worried about the collection than the declared and actual use of that data. This is currently evident in the rapid take-up of consumer schemes such as frequent flyer or supermarket points programs.

It is worthwhile to note that the various telecom operators in Australia are rapidly moving towards open platforms for their technology base. This will mean that many more parties will be involved in the delivery of customer services. For effective convergence to be achieved, user information will need to be transferred quickly and seamlessly between various systems and corporate entities on a global basis. From a user perspective, the service may appear to be delivered by the local operator but in fact the delivery chain may involve multiple suppliers that are distributed globally. This will make the coordination of privacy issues significantly more complex.

2.6.4.4 Rules and guidelines

Clash of cultures

Generally, countries have an incumbent telecoms operator that traditionally was, or continues to be, partially or wholly government-owned. As a consequence, there is generally a close and historical relationship between the telecommunications industry and government. While most countries including Australia have gone down a path of privatisation and deregulation, this cultural legacy continues. Telecommunications operators expect, but don't necessarily like, government to be heavily involved in all areas of their business.

While from some perspectives the Internet²⁷ is owned by the US Department of Commerce, it is generally considered to be a self-governing group of cooperating entities and individuals and there is often strong resistance to any form of government regulation. Calls by various groups such as elements within the ITU and many developing nations, to bring the Internet under control have been met with scepticism and often open hostility.²⁸

Like most analysis of culture, to say that one culture is bad, old or simply out of date and another is good or new is simplistic at best. The cultural future of these two groups almost certainly lies together. The cultural mix has already started as converged networks, for example, the universal mobile telecommunications system (UMTS) become dominant. The IT world has begun to realise that to run large-scale technology systems like the telecommunications industry has managed for 100 years, the solution is not in the technology but rather in processes and methodologies.

It will take visionary leadership to provide direction and achieve the expected benefits from a cooperative environment.

Law enforcement and security

As communications infrastructures become increasingly intertwined, the potential impact of external disruptive forces or discontinuities, such as terrorism, local or global economic collapses or pandemics, becomes more important. These developments provide another layer of complexity and compliance costs that may shape communications systems architecture design and business models, and the overall regulatory framework.

In one interview for the Vision 20/20 project, communications was described as the "fundamental cornerstone of intelligence and law enforcement"—that understanding and managing the relationship between communications, security and enforcement is important.

National and trans-national security risks are a key driver of communications monitoring and surveillance initiatives. Communications service providers are under increasing pressure

²⁷ Currently ICANN manages DNS and IP address management under contract from the US Department of Commerce.

²⁸ For an example of this discussion refer to Telecom Asia Jan8 2005 article "Who will rule the net?"

from government security and law enforcement agencies to disclose information and track communications. An increase in communications over IP-based networks can make interception difficult—no longer is it a matter of intercepting a telephone call. In the same way, it may be easier to collect more information about people as increasing levels of personal data are released into the network.

In traditional networks, there are a limited number of connection points out of the country and each are well controlled. This means that governments can easily block traffic to and from particular international destinations because they only have to coordinate with a limited and known number of gateway providers. These providers are also typically very large carriers that are familiar with the administrative burden of boundary management.

Countries that wish to enforce strong control over what their population can view or do with the Internet attempt to achieve this by following the same design philosophy as that used in circuit-switched networks. They have only a few international gateways and thus are able to block particular services, such as VoIP services, en masse. The Chinese implementation of the Internet is a well-known example of such an architectural design.

Problems arise with the 'classic' Internet structure—there are significantly more international gateways that are difficult to coordinate because they are managed by many often very small network providers. It can be difficult to determine who is providing gateway access. In Australia, for example, it is not clear exactly how many such gateways there are.

Although Internet networks allow for the option of blocking a particular service type, such as email, web access or VoIP, in addition to blocking a source or destination, filtering particular services on a gateway is computationally intensive. In traditional networks, there is typically only one service type, generally voice, associated with a particular source or destination, so the blocking is simpler.

Some technical implementations of VoIP that have distributed control mechanisms, such as Skype)²⁹, and where users have the ability to be mobile provide particular challenges for mandatory interception capability. With no fixed interception point, governments would have to mandate changes to the fundamental architecture of the systems for such services to be meaningfully intercepted—where the data can be understood.

While law enforcement benefits from communications mobility, coverage and range, enhancements in these areas are also used—and driven—by the criminal element. For example, Internet communications have introduced and encouraged various forms of user risk, including identity theft. More traditional law enforcement issues, such as international money laundering and other economic crime, and smuggling of people or goods, are now achievable more quickly and easily.

Standardisation

Industry collaboration in the development of standards is critical for the building of new markets and achieving economies of scale. In a multi-party operating environment, a network cannot exist without an effective method for the creation and implementation of common standards. As the Internet has grown and its use has become more complex, the standardisation environment has also become more complex and uncertain.

There is uncertainty around:

- geo-political tensions that constrain coordinated approaches, for example, differences between Europe and the US, and north-east Asia as the emerging standards leader
- cultural differences over freedom of access to information
- cultural differences between the once distinct but now convergent telecommunications and IT sectors and uncertainty about the future role of their respective international standardisation bodies
- the quality of patent-management regimes and social and cultural attitudes towards cooperation are both highly influential in the role that open or closed systems and standards play in achieving ubiquitous communications, and

²⁹ www.skype.com

- the timeliness of standardisation development processes that lag the pace of technology development.

Standardisation varies in form from organic, such as what side of the road a car drives on, to highly structured, such as the metric system. Generally speaking, the telecommunications world comes from a more formalised standards-making process where decisions have been made at a national and international level. Although more market-based approaches to standardisation have been taken by various industry groups over recent years, historically, most telecommunications standards were developed by groups such as the ITU or ETSI.

The IT world comes from a very different mindset. Most standards have been generated by vendors, for example, the PC, or vendor groups, for example, DVDs, or alternatively by what are essentially 'interest groups' such as the IETF.

While the IETF may appear similar to other standards-setting forums such as the ITU, from a cultural perspective it is very different. The IETF seeks to influence but not control the way people use, design and manage the Internet to make the Internet work better.³⁰ The IETF makes decisions through reaching a rough consensus—the combined judgement of participants. Individuals engage in the IETF as individuals rather than as organisation-based representatives.

ITU membership is primarily based on government or organisation representation. While it also reaches standards decisions through consensus, formal voting plays an important role in conferences and assemblies.

The fact that the telecommunications and IT industries have very different 'world views' in terms of standards-making philosophy means that the various bodies will tend to compete for dominance rather than cooperate.

Developing standards for digital rights management, content management, e-commerce, e-government and network security requires cooperation across previously distinct industries with separate standardisation and regulatory regimes.

This will be a major challenge with a complex mix of political, cultural and technical issues. Some groups feel that global communications should be solely market-led and managed, while others believe in a world governing body such as the ITU being the key driver with support from industry groups.

Historically, governments have made decisions on the choice of technology to use within their domain, such as TV and telephone network standards, to achieve outcomes of importance to them. Given the increasing globalisation of technology and its applications, governments will more likely need to draw on their skills to engage internationally through regional and global forums and to work with communities of interest to achieve their national objectives.

E-government and e-commerce frameworks

The migration to e-government and e-commerce is likely to influence everyday life, with largely beneficial consequences for employment, education and health, communication with friends, family and associates, and leisure and entertainment. Government and industry have roles in promoting interoperability and consumer trust and confidence in e-government and e-commerce through security and privacy protection and in migrating to e-services.

Currently, there are a number of user identification formats and systems, and consumers could end up with multiple electronic keys or industry may agree on a single universal format. The future of electronic payments markets is dependent on the development of remote and secure authentication, real-time access anywhere, integrated loyalty schemes and other business operating processes.

These large-scale issues are associated with standardisation and coordination. Does government need to be involved? For example, governments may act to facilitate, educate or lead in systems deployment.

The communications environment is increasingly independent of national jurisdictional borders. The ability of privacy frameworks to address this will be an increasing challenge and

³⁰ Network Working Group Request for Comments: 3935, October 2004.

will directly influence levels of consumer and organisational trust in existing and emerging communications infrastructures.

In an analogous area, the ACA's experience with spam enforcement has found that two types of international coordination are needed:

- strategic coordination between countries where long-term initiatives can be planned and discussed and
- operational coordination between countries to support case investigations within short timeframes of hours or days.

Ability to avoid harmful or illegal content

The ability to restrict access to harmful or illegal content is likely to increase in importance. Some users are already opting for dial-up as opposed to broadband access to minimise the risks, particularly for children, associated with an always on Internet access service.

Digital rights management

Resolving DRM has technical as well as legal aspects. Content sharing and transfer are consistent with the ubiquitous communications vision, but a technical solution to providing DRM over multiple devices has yet to be developed. Building DRM into the system is a likely outcome. Standardised encryption and identification validation processes are likely to be developed, although such standards may not be universal because attitudes to intellectual capital vary.

One approach that recognises this diversity is the concept of 'generally accepted digital rights principles'. The Vision 20/20 project's International Road Test Report outlines this approach in more detail.

2.6.5 The alternative: fragmented, limited communications

Scenarios 3 and 5 present a less optimistic view about the scale of network integration and device interoperability, with competing and incompatible proprietary systems and networks. Failures in payment systems, identity management and consumer protection mechanisms erode consumer and business trust and confidence and slow the rate of change.

Scenario 3 describes a failure of technologies and/or the protocols and frameworks that support them, namely in security and authentication processing. The development of divergent communications spheres—physical and virtual—has resulted in weak technical infrastructures both locally and globally. While convergence has technically occurred and there is high investment in wireless infrastructure, networks are widely dispersed with parallel communications systems prevalent. There is poor service delivery performance. There is a mismatch between human 'wants' and technological capacity.

In Scenario 5, although there is high reliability in government-supported areas, including national security, law enforcement and the environment, there are integration difficulties with other sectors. Fragmentation problems are likely to arise where:

- the development and use of open standards and compatible regulation does not eventuate, whether due to geo-political or cultural differences or different worldviews
- 'walled gardens' or proprietary systems that do not interoperate dominate and
- segmented approaches between sectors such as banking and finance and national security to rules and guidelines, for example, identity management and authentication.

Proprietary systems, standards and devices that are not interoperable would act as weights on the development of seamless connectivity.

Other factors that could drive a more fragmented future environment include the following:

- Powerful lobby groups representing particular market segments may adversely influence government decisions and stifle new business models and market innovation. Particular areas of risk are from legacy businesses.

- Failure to develop effective forums to enable industry players such as governments, operators, user groups and vendors to develop standards, interoperability systems and network improvements.
- Failure of government agencies within jurisdictions to cooperate in the development of convergent regulations.
- ‘Simplicity of use’ is one of the key factors that will influence whether a service or device is a commercial success or not. As the technical and commercial aspects of delivering services become more complex, there is a real risk that the complexity effectively limits use to the ‘tech-savvy’ only. An analogy can be seen with the motor car. The early automobile, a relatively simple machine by today’s standards, was very difficult to drive because it had a non-synchronised gearbox and manual choke, throttle and gears. It is only with the complexity of the modern technology—features such as cruise control, automatic braking systems, traction control, automatic transmission, electronic fuel injection—that the machine is relatively simple to use.
- Failure of traditional business models that would result in disruption and instability in the market. This is a particular risk for incumbent carriers that have used cross-subsidisation between high profit, for example, long distance call charges, and low profit, for example, local call charges, products to fund development and maintain low profit business. These carriers typically also have extensive infrastructure investment—copper cables to homes—that is perceived to be of value largely with traditional technologies.

2.6.6 Limits to openness, being always online

Ubiquitous communications is likely to be balanced with national security needs and commercial drivers to provide a secure environment for commerce and the protection of physical and intellectual property rights. It is possible that a mix of closed ‘walled gardens’ and open networks, which may share infrastructure, could emerge.

The Vision 20/20 report was developed largely from an Australian perspective and the scenarios are indicative of Australian values and preferences. Different cultures will have varying attitudes to openness, for example, some jurisdictions and service providers already exclude access to certain types of content and, in the case of North Korea, to ban the use of mobile phones.³¹ In the future, it is plausible that nations or regions with similar cultural and social values develop bilateral or multilateral protocols that place restrictions on access to specified content or services.

Being always online may have negative effects on personal lifestyle choices and physical and social well-being. Spending long periods online with little other social contact may result in ill-formed social interaction skills and harmful health consequences, such as those resulting from sedentary lifestyles and long periods in front of a display screen. Developments of this nature may drive some societies or communities to place restrictions on the use of communications services.

The potential emergence of quantum encryption may also give rise to new challenges for industry and governments in the future. Open systems have posed challenges to centralised power as outlined above, and controls may need to be developed to avoid a completely unbreakable system that is free to be used in harmful ways.

2.6.7 Next five to ten years

The pace of development toward ubiquitous communications over the next five years is predetermined to an extent by the product development and commercialisation cycles of the major vendors.

The uncertainty lies in:

- how users will react to the technology
- commercial drivers that would allow the technologies and business systems to ‘interface’

³¹ ‘North Korea recalls mobile phones’, *Sydney Morning Herald*, 4 June 2004.

- how the technology will be shaped to fit social expectations and
- what political, social or economic weights on change might slow the pace of change.

The process of digitalising everything has already commenced.³² New forms of multimedia-rich interpersonal communications, entertainment, e-commerce and information services are expected to evolve. Within this context, a new wave of digital content and web services and the convenience and productivity from broadband wireless connectivity are all expected to be key drivers in user migration to digital devices.

Expected developments in the near term include devices with a standard protocol for initiating an interactive user session or experience that involves multimedia elements such as video, voice, chat, gaming, virtual reality, instant messaging and digital photos. 'Triple-play'—the combination of voice, TV and Internet services that neatly captures the essence of services convergence—is expected to be a major growth area.

Voice and broadcasting services are likely to become a subset of bundled applications including Internet access, content, multimedia and payment applications.

2.6.8 Longer term

The physical landscape that might emerge from ubiquitous communications, as early as 10 years away, is a world:

... in which we can move about physical places, accessing not only what is stored in our brains but also multiple layers of information that have previously been inaccessible: experiences of friends, colleagues, and complete strangers in the same space; information about who lives and works in the place, their demographic characteristic, and perhaps their political affiliations; crime statistics for the area; the history of community events, from celebrations to calamities; information about businesses in the area and their products; changes that have reshaped the natural environment over time, and much more.³³

Wireless technologies such as adaptive radio and sensor networks are expected to be five to ten years away.

At some point over the next 15 years, it may be possible to purchase a device with every movie ever made, accessible only on a pay-per-view basis.

Huge efficiencies in managing data and information would be likely. Payments could be scalable. For example, as your wage goes up, your tax is increased at your next pay and, if the government underspends or projected expenses are not required, taxes reduce. These changes could be made automatically.

Developments in nano-technology, the life sciences and quantum mechanics (including quantum encryption) will continue to evolve over the forecast period and may have profound implications for communications. Although it is difficult to forecast technology developments, it is plausible that within the next 15 years, telepresence, augmented and enhanced reality³⁴ and advanced forms of artificial intelligence may drive new forms of communication. As well as enhanced forms of electronic video, audio and cognitive experiences, we can expect our future communications experiences to include touch, taste and smell.

The emergence of viral communications, or infrastructure-free communications, is a plausible outcome in the forecast period that would drive disruptive change in radiofrequency spectrum use and management, and the provision of communications because communications may be something you do, not something you buy.

³² One example is <http://www.archive.org/>

³³ *Infrastructure for the New Geography*, Institute for the Future, August 2004

³⁴ Telepresence is the experience of being fully present at a live real world location remote from one's own physical location. Enhanced reality is achieved by electrochemical stimulation of the brain. Augmented reality uses a combination of the real scene viewed by the user and a computer-generated virtual scene.

Part 3: Regulatory implications

3.1 Introduction

This part examines the regulatory implications of the strategic landscape identified by Vision 20/20. Assumptions underpinning the current regulatory frameworks are set out and then compared with the strategic landscape assumptions outlined in Part 2 to test what needs to be challenged and why.

This part provides an understanding of:

- the current regulatory frameworks in Australia and
- what needs to change, evolve or remain in order for 'preferred futures' to be achieved.

3.2 Current regulatory framework

The current communications regulatory framework in Australia is segmented into traditional/legacy communications spheres, with DCITA³⁵ managing the policy context. The overall regulatory focus is on promoting the competitiveness of industry, and protecting public, consumer and national interests. Self-regulation—in effect, industry regulation as defined in this report—is promoted in all areas. Government regulators have powers to intervene if industry self-regulation is not working effectively in specific instances.

Telecommunications and radiocommunications regulation is currently administered by the ACA and the ABA has responsibility for broadcasting, datacasting and Internet content. The ACA also enforces the *Spam Act 2003*. These two bodies will merge to form the Australian Communications and Media Authority (ACMA) by July 2005.

The ACCC is responsible for compliance on competition, fair trading and consumer protection issues. It manages administration of the access regime, regulates anti-competitive conduct and facilitates general consumer protection and competition regulation across all industries, including those that are communications-related. The ACCC's monitoring responsibilities include reporting on telecommunications, broadband take-up, emerging market structures, record-keeping rules and review of price control arrangements.

Telecommunications regulation as administered by the ACA governs access and technical, interconnection, consumer and customer service standards. Delivery of carriage services, including the standard telephone service,³⁶ is a primary focus. The ACA licenses telecommunications carriers and ensures compliance with licence conditions and service provider rules.

Service provider rules include the need to provide access to emergency call services and assistance to government agencies in the national interest, and the ability of consumers to pre-select a service. Compliance with the universal service obligation, the Customer Service Guarantee and standard terms and conditions is monitored.³⁷ The ACA also administers the Telecommunications Numbering Plan.

Radiocommunications regulation provides for the management of the radiofrequency spectrum in Australia. The underlying assumption is that spectrum is a scarce, limited resource. The regulatory framework is designed to efficiently allocate and use spectrum to ensure maximum public benefit through the provision of a wide range of services of appropriate quality. Regulation works to ensure adequate provision for agencies involved in national security, defence and emergency services and for use by other public or community services.

A primary aim of radiocommunications regulation is to provide an efficient, equitable and transparent system for charging for the use of the spectrum and to provide a regulatory environment that maximises opportunities for the Australian communications industry in domestic and international markets.

³⁵ www.dcita.gov.au

³⁶ provision of voice telephony or equivalent to people with special needs, any-to-any connectivity, technical neutrality

³⁷ As specified in the *Telecommunications (Consumer Protection and Service Standards) Act 1999*

Broadcasting regulation promotes the availability of a diverse range of broadcasting services to audiences in Australia and the development of an efficient, competitive broadcasting industry that is responsive to audience needs.

An important broadcasting objective is promoting the role that broadcasting services play in fostering an Australian cultural identity and respecting community standards. Components of this include protecting children from exposure to material which may be harmful to them and the provision of the means to address complaints about electronic media.

Broadcasting regulation applies to providers of broadcasting, datacasting and Internet services and Internet content hosts. Specified services include national, community and subscription broadcasting and open and international narrowcasting.³⁸

The Office of the Federal Privacy Commissioner administers the *Privacy Act 1988* and the way in which personal identifying information is collected, stored and used.

Organisations responsible for consumers, other users and industry interests include:

- Australian Consumers' Association
- Australian Communications Industry Forum
- Australian Computer Society
- Australian Direct Marketing Association
- Australian Electrical and Electronic Manufacturers' Association
- Australian Information Industry Association
- Australian Interactive Media Industry Association
- Australian Mobile Telecommunications Association
- Australian Subscription Television and Radio Association
- Australian Telecommunications Users Group
- Commercial Radio Australia
- Community Broadcasting Association of Australia
- Consumers' Telecommunications Network
- Free TV Australia
- Internet Society of Australia
- National Electrical and Communications Association
- Service Providers Association Incorporated
- Small Enterprise Telecommunications Centre Ltd
- Telecommunications & Disability Consumer Representation
- Telecommunications Industry Ombudsman

3.3 Regulatory challenges – what we found

3.3.1 Overview

One of the most challenging tasks over the next five years will be to transform regulation that has been designed for the relatively mature telecommunications and broadcasting industries, where discrete networks have been independently managed, to operate within a broader internationalised and interdependent environment.

There is currently a global regulatory vacuum at all levels (government, industry).

The need to understand the world differently may be the most difficult regulatory challenge for the communications sector.

Critical challenges for government, industry and users include:

- dealing with different cultures and values

³⁸ Programming designed to reach a specific group defined by demographics and/or program content

- forming relationships with new entrants to the communication sector
- moving away from dealing with specified elements within vertically integrated and centrally controlled networks—the emerging communications space needs to be understood through all of its parts, considering the:
 - o emerging areas of society risk attributable to new forms of communication and political decisions about the role of individual or market self-responsibility to manage risks relative to government regulation, legislation or other policy instrument
 - o move from centralised control to distributed, globalised networks where intelligence lies at the edge and there is distributed power and influence
 - o complexity in the multi-layered infrastructure, logic and content layers
 - o service delivery that is becoming more complex, less segmented and involving multiple players often spread globally
 - o number of parties involved in delivering services to the public increasing in number but decreasing in size and ability to engage in regulatory dialogue and the
 - o need for cooperation
- promoting equitable participation, network integrity and agreed e-government and e-commerce frameworks
- moving toward more flexible standard making processes
- enabling more flexible use of the radiofrequency spectrum and
- learning new skills and competencies.

3.3.2 What we need to do differently

A transition period of 15 years to ubiquitous communications is plausible. Transitional arrangements will be needed. Legacy telecommunications and broadcasting regulations may need to operate in parallel with emerging regulations designed for new IP-based applications and services.

3.3.2.1 From numbering to identity

Numbering plans are likely to operate for the next 10 to 15 years, but will start to decline in importance in the near future relative to identity management systems. When we think of contacting someone, we think about their name and not a 10-digit E.164 number. As people move from legacy systems and are always online, always connected, numbers will not be needed and IP addresses will lie in the background.

Our scenarios suggest that formalisation of identity could be the responsibility of the government, industry or the individual. Personal and national security may drive government-centric identity management. While the strategic context is understandable, it remains to be seen whether sovereign states would have the capacity to control the electronic identities of individuals or entities that are real or virtual, that could be based anywhere in the world, and could have an electronic presence in any number of countries.

The integration of mobile and fixed line services may mean that separate numbering plans are unlikely to be sustained over the longer term. Industry experts agree that the effectiveness of the current numbering plan is limited, with a lifespan of perhaps five to ten years at most.

Market-based open source interconnectivity solutions to VoIP/POTS systems are emerging that could offer superior solutions than ENUM systems. The ACA sponsorship of ENUM needs to be monitored in the light of these developments, consistent with the principle of technology neutrality.

3.3.2.2 Legacy network reliability

There is a potential risk that falling revenue streams from traditional services over legacy networks would pose a risk to network maintenance and investment expenditure. The

potential risks may include declining network reliability and carrier performance against specified social and legal obligations.

Declining revenues might have consequential access pricing implications, for example, the costs of network access may need to increase in real terms, raising equity of access concerns and risks to the sustainability of maintaining legacy services. Government regulators may need to develop transparent early-warning systems involving information from industry and assure the community that strategies are in place to manage longer-term risks.

3.3.3 New approaches

3.3.3.1 Phasing out redundant elements

Regulatory instruments designed specifically for voice telephony, data transfer or mainstream broadcasting that are linked to specified transmission networks, specified and uniform standards of service, customer equipment and business logics are likely to be of less relevance to convergent, IP-based networks. For example:

- Voice, multimedia content and data are all mixed together over the Internet. Two or more modes may be mixed together in any one communications session. The importance of one mode over another is likely to be less of an issue relative to having choice of communication modes.
- Licensing arrangements and associated obligations designed for structural elements of legacy systems may have less relevance over time.

Commercial enterprises that are new to communications could integrate connectivity within consumer and business products and appliances. Products that were not traditionally part of a network, such as game consoles or consumer electronics, are migrating to networked solutions. These products are not subject to the device regulation or licensing associated with the telecommunications industry, for example, mobile and PSTN phones, and PABXs, need to be approved to connect to the network. Connectivity could be made by self-organising nodes independently of a core network. These developments may redefine and blur the participant boundaries of the communications industry.

- Industry codes or standards for segmented services would be irrelevant to billing that covers a variety of charges, or services on a subscription basis rather than on a time or session basis. Bills are likely to be less like telephone bills and more like financial services bills, raising the question of how long communications-specific regulation would continue to meet the needs of consumers.
- Regulations designed for legacy elements, such as content controls for traditional broadcasting or stand-alone telecommunications disputes resolution services, will be of declining relevance over time.
- Alternative and more flexible approaches are likely to be required for obligations such as legal interception and location for emergency services purposes.

While cyber-crime issues have long been examined from a law enforcement or intelligence perspective, the ability of the existing legal framework to manage active and emerging threats to communications will be challenged in the future. More emphasis on cross-jurisdictional and international cooperation is necessary, as well as improved interoperability.

New approaches that assist information sharing, risk assessment and security coordination in the converging communications sector would help. While law enforcement benefits from communications mobility, coverage and range, enhancements in this area are also used—and driven—by the criminal element.

P2P communication is difficult to intercept because of the lack of a centralised interception point, which is straightforward in architecture based on a client server. Technical solutions may involve changing the structure of the Internet, or placing government filtering mechanisms at various gateways. Alternatives to interception may

gain importance, perhaps using emerging communications developments such as sensor networks.

- A complex communications future would pose significant if not insurmountable challenges in the measurement of consumer satisfaction on a legacy or segmented service basis.
- Quality of service assumptions of legacy services will have less relevance in the future. Many of the traditional systems are being migrated to emerging IP-based platforms, for example, POTS telephone services are being replaced by VoIP services, where there may be the expectation that the same level of performance will be achieved. This is not necessarily the case.³⁹

3.3.3.2 Recognising the impact of new forms of communications

Australians are entitled to reasonable access on an equitable basis to specified telephony and data services where service provision is not commercially viable. Access to broadband connectivity in the home and workplace is likely to displace these legacy services in terms of social and economic importance at some point over the next five years. The importance of access to broadband is likely to evolve over the next five to ten years. These developments pose challenges for regulators in meeting the accessibility needs and service quality expectations of users.

- Ubiquitous communications assumes widespread empowerment of use. Prerequisites socially include having the capacity to use and pay for services. Challenges for industry include removing complexity of use, and to forge a mind-shift change to recognise the broader commercial incentives in adopting 'universal design' functionality.
- Rapid change and internationalisation is common to all of our scenarios, which would challenge the ability of mechanisms to provide for the needs of vulnerable people in society, and to maintain effective consumer protection measures and regulatory harmonisation. More flexible and responsive approaches are required that consider public interest outcomes in the design of devices and services.
- In a world where there are many diverse ways to communicate, individuals could tailor their communications services to meet personal preferences. Standardised services/service contracts may have less appeal.
- The emergence of software agents and the transfer of social and contractual functions to alternative means, such as AI applications, are likely to give rise to a new body of law and regulations to codify roles and responsibilities.
- In the longer-term, governments may come under pressure to extend rights and responsibilities to virtual identities in a similar way as in the physical world.

3.3.3.3 Network integrity – taking responsibility, building awareness

Trust and confidence in communications is likely to drive the development of new rights, responsibilities and obligations. Regulatory solutions for maximum network integrity range from government regulation, industry regulation and user regulation—all need to be explored. The issue is made more complex due to the clash of cultures between the telecommunications and IT industries.

- Legacy network management assumptions do not apply to the Internet. For example, the traditional 'networks' are independently managed by each of the network owners (carriers) as they are autonomous structures with limited interconnect. Network management could successfully be done on an operator basis. However, the Internet is in many ways a 'single network', but only discrete elements are managed by any one operator. The feasibility of a holistic network-management approach to the Internet could be considered.

As discussed throughout this paper, the 'Internet' is not a network in its own right, but an agreed interconnection of autonomous networks. It appears that this concept of

³⁹ See the ACA discussion paper, *Regulatory Issues Associated with Provision of Voice Services Using Internet Protocol in Australia* for more details, www.aca.gov.au

'networks within networks' will continue. Traditional networks have very strict network boundary control with few 'cross-network' services, thereby minimising the need for strong operational inter-network owner communication.

The emerging trend is towards complex services that cross multiple network boundaries in their delivery. The consequence of this change is the need for tight operational coordination between parties. This coordination could be expressed in a number of ways, including, for example, a national network operations centre (NOC) or a telecommunications information sharing analysis centre (ISAC), where the network providers could exchange information and make operational decisions in real time. A number of countries have already realised the need for such cooperation, for example, Japan and South Korea, and have already established such centres primarily focusing on their national internet network management. These country-based centres also have operational ties with other centres around the world.

- Traditional circuit-switched networks manage device risk with a mixture of technical (devices could only cause limited damage technically) and regulatory (devices have to be 'approved' to connect) measures. Similar approaches may need to be implemented for the IP environment.
- Providers of connectivity, such as ISPs and domain-name registrars and vendors, must accept some responsibility for how connectivity is used. Individual users or groups of users may also be required to assume more responsibility for their use where it is a threat to other users of the network

Privacy and security issues are driving the need to develop reliable mechanisms for authentication of identity and to verify information. Privacy regulation needs to be taken to the global level. With increased connectivity and global service delivery, privacy needs to be considered globally while managed locally.

The advent of pervasive monitoring and ubiquitous connectivity may mean that a major 21st century regulatory challenge is to limit the intrusiveness of communications systems and minimise the negative impacts on citizens and consumers, while maintaining access to the information commons and the convenience of being always on, always connected.

It could be the role of the Privacy Commissioner, other government agencies or industry to educate individuals and organisations about the protection of their identifying information in international environments such as the internet. Under an open systems approach, together with a socio-political environment of individual responsibility assumed in Scenario 1, self-interest would generally drive user authentication and encryption take-up, but the more vulnerable members of society would be exposed to risks.

Industry is likely to respond to demands for privacy and security, including government interests in e-government, through built-in authentication and encryption in network and systems architecture design. Public concern about national security may lead to government-prescribed identity authentication. Either development may limit access to, or place limits on the use of the Internet as a public domain.

- Having confidence in the continuity of supply and in disaster-recovery mechanisms for communications systems will be of increasing social and economic importance.
- Enhancements to the efficient operation of the Internet, such as IPv6, are desirable for public interest outcomes as well as for commercial purposes. Governments and industry may face growing pressure to intervene should market-based action in this area continue to lag. International collaboration between governments, industry and non-government organisations may be necessary to drive the mind-shifts required.
- Small enterprises and individuals are less likely or less able to protect themselves against issues such as viruses, spam or cyber-crime, despite being increasingly exposed to these risks.
- As previously discussed, a guiding principle for the Internet is that end-users need to protect themselves. This philosophy suggests that, while applications are available to manage risk, it is likely that industry and government-sponsored consumer education and

awareness programs will be required to build awareness and to provide protection to people who may not otherwise have the knowledge or ability to manage their own risk.

As discussed earlier in this paper, network intelligence is moving to the network edges. Mobile phones are becoming more powerful and home PCs now have huge capacity equal to major servers of a few years ago. With power comes responsibility; users are often not aware of the power their systems possess or the dangers associated with this, hence the success of viruses compromising primarily home PCs to propagate themselves. The owners of these edge systems need to be made aware of what their systems can do and the inherent dangers therein.

Solutions are complex, not least because of the large number of people involved. The various international government activities associated with reducing spam, with the message being essentially one about improving PC security, may give some guidance. Typically with spam, governments have tried to communicate through a number of channels:

- o directly via brochures and direct advertising, such as on websites, in media releases or on radio
- o partnerships with ISPs, who have direct relationships with their customers and pass on information through mailing lists or websites
- o interest groups, such as Internet user groups or associations, who communicate through working groups or newsletters
- o vendors who integrate the message into product promotions.

3.3.3.4 Building new working relationships

New and evolving business partnerships and alliances are expected to emerge over the next few years that will have a dynamic effect on the relationships of importance to regulators and the applications and relevancy of regulatory obligations.

For example, national telecommunications regulators have traditionally worked with carriers and carriage service providers, but the entities running the networks are now often global vendors, outsourcing contracts. The ICT industry is playing an increasingly important role. Regulators will need to develop relationships with the new network operators and IT systems providers to maintain knowledge over the technical aspects of network regulation.

The number of players in the communications space is increasing. Recent m-commerce content and billing issues and spam initiatives indicate that this is already an issue.

New organisations are likely to emerge replacing legacy institutions as convergence rolls on. This is already evident in the Australian Government's decision to merge the ACA and the ABA. New groups may emerge to represent the views of P2P users, virtual communities and groups representing new alliances formed in the multi-layered communications value-chain.

Convergence, internationalisation and the global nature of the Internet raise complex issues, including the following:

- Who should set standards—the ITU, the IETF or some other organisation? The emerging importance and influence of developing economies needs to be considered.
- To avoid fragmentation, an integrated approach is necessary to deal with issues that cut across regulatory frameworks, agencies and jurisdictions, such the development of reliable authentication systems.
- Mechanisms to track international trends and developments will be necessary to determine the appropriate scale of regulatory intervention. Some matters will continue to be addressed at the local level. Fragmentation between governments would leave globalised organisations free to set their own standards. Other interventions may need the cooperation of either large corporations or the international community, or both. Knowing who should intervene, how and when will be critical.
- There are likely to be growing concerns about regulatory coherence. Current trends suggest the potential for further regulatory convergence or overlap of varying degrees

between the communications, IT, finance, national security, privacy, transport and general consumer protection frameworks.

- The preferred path is towards regulatory harmonisation to achieve network integrity, personal security and privacy, identity management, location, presence, payments and billing standards and codes across the service layers.

3.3.3.5 Recognising the importance of cooperation

More regulatory cooperation will be needed in the convergent, fast-changing and globally connected future. Cooperation models that might apply to communications regulation would most likely be a combination of:

- an architecture for cooperation that is open, participative, responsive and self-managing, designed to keep pace with change and
- networking between people and groups within agencies, between agencies and convergent industry players in a way that draws on specialist knowledge and trusted processes.

Effective cooperation frameworks would need to respect national and international diversity in culture and values. Other problem areas to consider in the design of cooperation models include:

- the risk of rule-breaking, free-riders and other 'tragedy of the commons' issues
- game-theory problems and
- the difficulty of decision-making with multiple parties and competitors involved.

Demonstrations of transparency and surveillance would be necessary to maintain the integrity of, and trust in, cooperative processes. Coercion may be necessary to force group cooperation.

The use of generally accepted principles may help to build international consensus on common regulatory problems that require a cooperative approach while providing flexibility to adapt solutions to suit local needs or preferences. Agreed principles could be codified to suit national, social or cultural objectives in statutory instruments or industry codes and guidelines.

3.3.3.6 New uses of radiofrequency spectrum

With the growing importance of the radiofrequency spectrum, governments are likely to be under pressure to implement measures to facilitate spectrum efficiency and promote innovative use. Likely measures include market-based spectrum allocations, encouraging intensive users of spectrum to make better use of their allocations and to free up surplus spectrum for others to use, and expanding the spectrum allocations for class-licensed services.

Service convergence, such as telecommunications companies providing TV services and broadcasting companies providing voice telephony services may erode the rationale for separate frequency band allocations by mode of service.

Emerging open wireless technologies such as cognitive radio are designed to make more efficient use of the radiofrequency spectrum. Understanding cognitive radio would require an understanding of IT systems architecture to ensure regulations are effectively applied. As these technologies evolve, assumptions about exclusive band allocations may also need to be challenged.

Some researchers are expressing a view that, with viral communications, the radiofrequency spectrum would not be a scarce resource as each node that is added to the network would increase capacity. Should viral communications develop, regulations may be needed to ensure that devices and nodes were properly configured to avoid interference with other users of the spectrum, and that devices are used in a way that is safe. The design and implementation of effective spectrum use regulations would require an understanding of IT systems architecture.

3.3.3.7 Content more dominant

Regulatory authorities and industry will be faced with the challenge of supporting a smooth transition of content to a more dominant role in communications regulation. The power of the media to influence public opinion forms the basis for government controls on broadcasting and narrowcasting services, such as:

- separate broadcasting radio-frequency service bands
- licensing of TV and radio stations
- rules on political announcements and advertising
- fostering an Australian cultural identity
- reporting news fairly and accurately
- respecting community standards and
- protecting children from harmful content.

Under legacy broadcasting and media business models, controlling harmful or damaging content was a relatively straightforward exercise. Questions that will need to be answered include:

- the extent to which private media is shaping public opinion and
- whether digital content ought to be managed similarly to broadcast mass media—promoting what is a social good and discouraging the bad.

The importance of promoting the Australian cultural identity may be challenged through global mobility and connectivity. Consumers may develop a preference for more global or special interest content over local content. Others will demand the promotion of local content to protect cultural values and national or local identity. In an increasingly diverse and international context, it may be difficult to maintain an ongoing consensus to support specified levels of local content.

Consumer awareness programs will play a substantial role in content management.

There is likely to be more pressure on regulators and the industry to implement content controls on areas of growing concern. For example, as one of the people we interviewed suggested, think about the so-called 'three Gs'—girls, gaming and gambling. Multimedia applications and broadband connectivity is likely to generate more private media and content from geographically dispersed parts of the world. How far could regulatory controls over private content reach?

Adverse consumer reaction to content risk is likely to prompt industry initiatives to manage risk. This may take the form of blocking access to certain websites through system architecture design. Initiatives of that type could also have the effect of partly closing the Internet or information commons.

Regulatory or self-regulatory standards and codes need to be developed either to suit the diversity of delivery channel, or to be designed to apply consistently irrespective of the mode of transmission.

3.3.3.8 Rethinking peer-to-peer

While not a new concept, the recent rise of true or near true P2P applications requires regulators to rethink some of their previous assumptions about what is possible to regulate. These assumptions include:

- all services finally have a 'home' that will have a geographical presence and therefore can be under the control of a government
- interception will always be possible
- censorship can be achieved and
- services can be effectively regulated.

P2P systems are 'everywhere' and 'nowhere'. From a third-party perspective, such as government, P2P is hard to regulate or control because the service does not have a 'home' or server residing in a specific location or administrative domain. Such characteristics have made music-sharing systems such as Kazaa⁴⁰ difficult to regulate. To stop, or at least control, the 'owners' of the service, end-users have to be regulated. This is difficult because of their large numerical base—potentially millions—and geographic distribution—potentially global.

Some P2P systems can dynamically negotiate their own specific characteristics as part of the transaction. This means that the two parties can create unique encryption systems that are difficult for third parties, such as law enforcement or crime, to successfully intercept. Furthermore, security barriers or filtering systems such as firewalls can be circumvented at either or both ends of the transfer. The 'signature', such as the port used, of the P2P application is difficult to detect and therefore difficult for government, security organisations or ISPs to regulate.

External censorship is difficult to implement for applications that run P2P. Traditional blocking (censorship) is achieved on the assumption that there are a relatively small number of identifiable computer servers located in particular geographic locations. With a P2P system such as Kazaa, the offensive content can be physically located on multiple—potentially hundred or thousands—of machines, distributed globally.

3.3.3.9 Developing agreed e-government and e-commerce frameworks

There is ample scope for industry regulation and user responsibility, including the development of:

- new forms of reputation systems
- collaborative cross-border disputes resolution services and
- online information and management strategies about security and privacy risks.

Traditionally, the use of a simple password and user ID has been the common method of user verification but this method is increasingly vulnerable, as the spate of phishing and spam outbreaks shows. These emerging problems stand in contrast to the legacy PSTN and mobile networks that have verification systems that are built-in and difficult to bypass.

There are two likely solutions. One is a fragmented and uncoordinated approach where the party that wants to provide user identification, such as a bank, will provide their own solution. This will potentially result in users having to deal with multiple interfaces depending on what system they are accessing, for such things as banking details, airline bookings or email accounts.

Another solution is where government or industry, or both in cooperation, provide a common approach or solution—possibly an open standard or co-use of government authentication. There may be opposition to such an approach on grounds of the infringement of privacy or civil liberties by government monitoring.

There are alternative customer dispute resolution mechanisms in Australia that are relevant to communications and e-commerce, including the Telecommunications Industry Ombudsman (TIO) and the Banking and Finance Industry Ombudsman, as well as the communications and broadcasting authority complaints mechanisms.

Currently, the TIO does not have jurisdiction over content or international service providers. In an increasingly complex and convergent service delivery system, is there a need for a centralised 'one-stop shop'?

⁴⁰ <http://www.kazaa.com/us/index.htm>

3.3.3.10 Applying a layered approach

Applying a layered approach to regulation based on the physical network layer; the logical network layer; applications layer and the content/transactions layer on top is not a new concept and has been discussed in many papers, including the ACIF New Generation Networks (NGN) report.⁴¹ In IP-based networks, these layers are generally managed or provided as separate entities. In traditional networks, most of these layers are managed as a single system.

The multi-layers approach is a good tool for unbundling a problem into its component parts. Regulation to solve a problem may only need to be applied to a specified layer, because intervening in more than one layer may damage the working of the multi-layered nature of the Internet. For example, intervening at the physical layer to regulate content would be an unnecessarily blunt approach.

The layered approach ought to be applied selectively because of the inter-relatedness of the multiple layers that constitute the communications system, the open nature of the systems architecture and global connectivity that can only be understood from a systems perspective.

The layered approach to regulation, as formulated by Kevin Werbach,⁴² could be applied to interoperability issues, content distribution and wholesale market regulation. Regulatory attention could shift from the pricing of individual services and applications, to the interface between competing services—horizontal to vertical—focusing on where market dominance is an issue. The primary focus, consistent with existing legislation, will continue to remain on the inhibitors of effective and efficient competition.

3.3.4 What we need to continue with

3.3.4.1 Consumer protection mechanisms

This area requires review as well as continuity. Given the prospect of even greater change in the future, and the ageing population, the need for safety nets is becoming more important. There is a need to reshape the design of industry standards and delivery of services to ensure that citizens are not marginalised and can participate in the communications future.

The scale of regulatory action should decline over time through simplicity of use being designed into the communication system—ubiquity of use requires simplicity. Complexity will no doubt remain an issue for systems architects and designers and may become more so, while the customer experience gets less complex. Simplicity of use is likely to be an investment and marketing driver for many years to come.

Decision points over the need for or scale of government regulation are likely to include the cost of broadband access, the relative availability and integration of infrastructure, the way in communications systems and devices are designed and the types of applications that will be available.

3.3.4.2 Competition regulation

Market concentration and dominance issues are likely to be ongoing areas of regulatory interest. The increasingly global communications environment requires an increase in collaborative regulatory action internationally. Peering arrangements and interconnection agreements will continue to be of interest to competition regulators.

Measures of market power may need to be evaluated on a layers-basis to avoid unnecessary restrictions on a cross-layer basis. Access to information and content are likely to be just as important as access to networks.

⁴¹ http://www.acif.org.au/__data/page/275/Policy_&_Regulatory_report_final.pdf

⁴² Kevin Werbach, *A Layered Model for Internet Policy*, September 2000

Quality of services in the transmission layer provided at the wholesale level will become of more interest to regulators. Traffic shaping⁴³ of network traffic by a back-haul provider can easily be used negatively, and arguably anti-competitively, to affect downstream competition.

3.3.4.3 Technical neutrality

In an environment of rapid change, a policy of technical neutrality is likely to be even more important to promote new and innovative networks and systems architecture.

Current research into new and innovative access technologies and systems architecture suggests the need for a broader application of the technological neutrality principle in designing regulatory and self-regulatory frameworks, and management of the radiofrequency spectrum. Industry pressure to provide regulatory certainty for network investment decisions made over the next three to five years may challenge the sustainability of maintaining a technology-neutral approach.

The ACA would need to retain its recently released regulatory philosophy guiding neutrality:

‘Neutrality—The ACA encourages innovation with regulation that does not favour a particular technology solution or practice. This allows regulation to be flexible and capable of responding to new technologies and services.’⁴⁴

3.3.4.4 EMR research

In recognition of concerns about the possibility of health effects from radiofrequency EMR, the ACA should continue to support ongoing independent research in this area.

⁴³ ‘Traffic shaping’ is the technical process by which IP flows are classified, queued, and delivered to a network to improve efficiency and minimise packet loss for traffic classified as time-sensitive or high priority.

⁴⁴ http://www.aca.gov.au/aca_home/issues_for_comment/index.htm#policy_philosophy

Part 4: Regulatory Challenges

4.1 Introduction

This part summarises the main regulatory themes from parts 2 and 3 of the full final report. An overview is provided about what should be done differently in terms of legacy arrangements and emerging challenges followed by issues of particular interest to the ACMA.

4.2 Regulatory themes

Vision 20/20 participants represented a wide range of industry, government and consumer interests. Despite this diversity, there were strong common themes relating to future challenges in communications regulation.

Vision 20/20 discussed the incentives for government, industry and users in realising the potential social and economic benefits of a world of ubiquitous communications - an information-rich world of ever-present connectivity and distributed computational intelligence.

Ubiquitous communications would allow for pervasive monitoring; perhaps of environmental pollution, of where one's children are or, of the health of elderly people in their homes. Examples of ubiquitous communications technologies might include smart cars, smart buildings, location and self-aware applications and devices, personalised information and services and wearable devices. There is a possible tension between ubiquitous communications, which may require provision of personal identifying information, and the protection of privacy.

There are obvious challenges, including establishing consistent national/international identity - and identity authentication - processes, ensuring a secure and low-cost electronic payments market(s), integration of standards and regulatory processes, the need for flexible dispute resolution services, and maintaining network integrity and reliability.

Participation is likely to be more critical in rapidly developing and uncertain environments. Vision 20/20 participants emphasised the social and economic impacts of exclusion from communications devices and services. They also stressed the importance of universal design principles that take into consideration the breadth of exclusion – issues include disability, affordability, skills base and geography.

The emerging communications environment is more complex. There are new elements and new participants. The computing and consumer electronics industries are converging with communications and media. The convergent elements are multi-layered and international – there is global connectivity and content and applications are decoupled from the underlying infrastructure.

Some research into use of the radiofrequency spectrum is considering spectrum sharing and cognitive radio technologies – self-sharing, ad-hoc and potentially viral communications networks (where the network is created by users who bring their own infrastructure and share it without centralised management). This is indicative of the more important role that wireless is expected to play in the emerging communications environment.

Network intelligence is moving to the network edges. For example, peer-to-peer technologies are changing the way users interact with the network and each other. There are likely to be increasing challenges in managing risks associated with the production and distribution of digital content.

There is an established international trend towards international regulatory cooperation. It is appropriate to suggest that international cooperation principles may result - these could emphasise defined public interest outcomes and promote trust in the system through transparency, monitoring and compliance mechanisms.

As more people place their personal information online and communications services are increasingly globalised, the protection of personal identifying information and privacy is likely to be of increasing importance.

Vision 20/20 assumes that international relationships and standardisation bodies, national governments, industry and users all have roles to play—in terms of their respective rules and guidelines—in striving towards ubiquitous communications.

One of the most challenging tasks will be to transform regulation—designed for the relatively mature and distinct telecommunications and broadcasting industries where discrete networks have been independently managed—to operate within a broader internationalised and interdependent environment.

Critical challenges for government, industry and users include the need to:

- view the world differently—the convergent communications industry needs to be understood through all of its parts
- be flexible and responsive and
- build regulatory coherence and cooperation between jurisdictions, industry bodies and communities of interest to promote equitable participation, network integrity, interoperability, and e-government and e-commerce frameworks.

In particular, understanding the emerging communications environment involves:

- evaluating emerging areas of societal risk in terms of self-responsibility relative to government intervention
- dealing with different cultures and values
- forming relationships with new entrants to the communication sector
- learning new skills and abilities and
- analysing problems using a 'systems thinking' approach rather than just examining particular elements in isolation.

4.2.1 What should be done differently

In highly urbanised areas, a transition period of 15 years or more to ubiquitous communications is plausible.

Transitional arrangements over that time will be needed because legacy telecommunications and broadcasting regulations are likely to operate in parallel with regulations designed for emerging services. The Vision 20/20 process identified certain aspects of the current telecommunications regulatory framework that will be tested by emerging developments. These are:

- Numbering plans are likely to continue operating for the next 10 to 15 years, but will start to decline in importance in the near future relative to electronic addressing, authentication and verification of identity. Fixed - mobile convergence may mean that separate national numbering plans are unlikely to be sustained over the longer term.
- Falling revenue streams from traditional services over legacy networks may pose a risk to network maintenance and investment expenditure. This may affect network reliability and carrier performance against specified social and legal obligations.
- Segmented regulatory arrangements such as licensing, quality of service standards and consumer satisfaction measures are likely to be of less importance in a relatively more complex, convergent and globalised communications future.
- Law enforcement and national interest obligations such as legal interception and location for emergency services purposes may require supplementary solutions and changes to some existing assumptions.
- More emphasis on cross-jurisdictional relationships will be necessary.
- Smaller organisations entering the communications industry that do not have the capability (because of location or resource constraints) to be involved in traditional industry regulation forums will still need to be engaged in regulatory processes.

Emphasis should also be placed on:

- Emerging accessibility challenges—it is important to recognise the potential social impacts of new forms of communications especially given a western population that is rapidly ageing and hence developing age related accessibility issues.
- Trust and confidence—the need to promote trust and confidence in emerging communications services is likely to drive the development of new rights, responsibilities and obligations. Network integrity solutions appear to involve a mixture of government regulation, industry regulation and user responsibility—all need to be explored.
- Cooperation—the number of players in the communications space is increasing. Regulators will need to develop new relationships with global vendors, new network operators and IT systems providers to build and maintain sufficient expertise over the technical aspects of network regulation.
- Radiofrequency Spectrum Management—with the growing reliance on and importance of the radiofrequency spectrum, governments are likely to be under pressure to implement measures that assist spectrum efficiency.
- Content—new challenges are emerging with the increase in online connectivity, the emergence of private media and open distribution models, and the digitalisation of content.
- Peer-to-peer (P2P)—the recent rise of true or near P2P applications raises new challenges for communications regulation.
- Layered approach—IP-based service provision may involve multiple layers that are managed or provisioned by separate entities, for example, content may be provided independently of the network operator. The multi-layered approach is a good tool for unbundling a problem into its component parts. It may be preferable to deal with content problems at the applications layer rather than physical network layer.

4.2.2 Issues of particular interest to the ACMA

These recommendations represent a distillation of the output from the multiple workshops, interviews, research and analysis and feedback in the course of the Vision 20/20 project.

To keep regulations contemporary and effective, the ACMA will need to monitor developments in services convergence that may affect its regulatory responsibilities. The findings of Vision 20/20 emphasise the importance of developing and implementing a more comprehensive, whole of business approach to emerging regulation problems in consultation with other government bodies, industry and user groups. This approach would help in being responsive to:

- (a) monitoring industry performance of network security and network integrity risk management
- (b) managing issues arising from voice, data and multimedia convergence
- (c) market-based approaches to voice over IP and PSTN interconnection
- (d) updating of consumer guidelines and fact sheets to reflect trends in services convergence
- (e) risks to legacy network reliability and accessibility
- (f) broader measures of consumer benefit and consumer satisfaction, and
- (g) working more closely with groups such as the ACCC about the technical aspects of Internet peering and interconnectivity arrangements.

Vision 20/20 participants also highlighted the importance of promoting a 'networked regulation' approach within and between government agencies and international regulatory bodies that:

- (a) draws on specialist knowledge and networks between individuals and organisations

- (b) incorporates the views of associated regulatory agencies to ensure a strategic 'communications systems' approach is taken, including cross-layer effects, to proposed interventions
- (c) supports a self-organising 'viral regulation' dynamic (participative online inter-working, that is responsive and adaptive – where solutions multiply, adapted to suit policy and cultural preferences) as an effective complement to more formal dialogue and
- (d) allows government regulators to have more direct engagement with vendors and 'new players'.

There may be an increased role for the ACMA in providing education and information in the future communications environment, particularly in emerging areas of Internet communications risks and information authenticity.

The ACMA could further encourage spectrum use efficiencies, including better use of existing allocations, and continue to be responsive to innovative approaches to managing spectrum, including shared spectrum, non-interference and capacity-enhancing class-licensed use.

In an uncertain future regulatory environment, it is likely that the ACMA will need to develop and maintain new skills and abilities. The merger of the ACA and the ABA will provide a good opportunity to develop knowledge of less familiar market segments, such as Internet service providers (ISPs) and content providers, both within Australia and internationally.

The merger will also support the need to develop regulatory skills in areas such as new media, multi-source content, interactivity and integration. An understanding of Internet architecture and its strengths and weaknesses is a prerequisite to the design and management of effective regulatory and self-regulatory policies and programs.

Effective relationship management will include working closely with groups supporting industry regulation, such as the ACIF, to ensure they remain relevant to the appropriate industry groups and the community that they serve. It will be important to develop relationships with new service providers and relevant virtual communities of interest.

Vision 20/20 participants discussed the need for greater regulatory flexibility and responsiveness, most likely to be achieved through improved processing of information, more effective use of social and online networks and better communications. Networks with colleagues and associates should form the basis for strategic conversations and planning.

A critical measure of success for government regulators is knowing how and when to intervene. Understanding complexity, uncertainty and dynamic change is likely to require the development of knowledge and skills in systems thinking and emerging issues analysis.

Consideration could be given to the development of an integrated forward-looking program to track network, services and content migration paths from legacy to IP-based systems. This would provide the ACMA with a greater capacity to analyse the implications for regulation and be responsive to emerging changes in the environment.

Appendixes

Appendix 1: Scenario narratives

The five scenario narratives, as developed by the workshop participants, are set out below. The Vision 20/20 project team compiled the text and ideas provided by each group to convey the nature of the alternative futures.

Through the eyes of one central character, Tom Bowler, each scenario is explored in some detail. This provides the reader with an initial understanding of the themes and characteristics of each plausible future, including the business models, government frameworks and human drivers.

The scenario narratives do not belong to the ACA. They belong to the collective wisdom and forethought of a vast range of notable people in Australia and overseas. Neither does any scenario have ACA endorsement. However, they do provide an audit matrix of possibilities that should not only assist the regulator, but also the broader purposes of other organisations which may find the work useful to their own future thinking in either a policy, business or social sense.

Scenario 1: Sensitive new age future



“...individual self-reliance is paramount.”

By 2020 there is an environment of almost ‘pure’ communications without boundary—from human to machine, machine to machine, between networks, families, friends, colleagues and the community generally. Individual self-reliance and social responsibility together with flexible, fluid markets and publicly accessible information produced an environment of trust and cooperation.

Global networks and open standards allow full interoperability in global markets. Wired local access technology has become redundant, replaced by open, ubiquitous wireless networks using spread-spectrum and software-defined radio.

Distributed power and influence motivates private and individual self-reliance with a minimal role for government. There are strong private sector governance frameworks and heightened transparency in all layers of the communications system.

An open Australian economy is supported by technological optimism, achievement and take-up in such areas as advanced artificial intelligence (AI) with ‘flow-on’ social benefits in health, education and the environment.

“Consumers, at one point scarcer than the network, led the drive towards built-in privacy and security”

There is a high level of communications pervasiveness and this is managed by consumer-led accountability mechanisms. There is good consumer choice and satisfaction.

Consumer confidence in the market in Scenario 1 led to the removal of the universal service obligation (USO) and government-defined consumer codes—these services were automatically delivered by the market. There is subsequent vulnerability for the consumer because it is the responsibility of the individual to ensure access and connectivity beyond the USO-level arrangements.

Scenario 1 narrative

Australia in 2020 is an environment of unified communications. Any-to-any connectivity, global networks and open standards allow full interoperability in global

markets. There is more connectivity from human to machine, machine to machine, between networks and between families, friends, work colleagues and the community generally.

In this environment, individual self-reliance is paramount. There are fewer rules and a high level of industry self-reliance. This encourages innovation and growth. Consumers have maximum choice, but take on more risk, with less honest entrepreneurial types taking advantage of uncertainty and flexibility in the marketplace to exploit vulnerable sectors of society.

People's lives are seamlessly intertwined with the technology they use. The products they use deliver the kinds of services they desire without the need for government intervention and regulation. There is unification of consumer needs and market delivery.

Consumers have stopped worrying about the computer virus wars of the early 'noughties', which are now a distant memory, but at the time caused severe problems, including crippling the power supply.

After the energy crises of 2008 and the subsequent world disequilibrium, communications infrastructure converged and became more concentrated. The rejection of the Longhorn transaction model, coupled with an identity management crisis, caused Microsoft to collapse under its own weight in 2010. This led to the development of an open source creative 'commons', accompanied by active protocol negotiation.

Consumers led the drive towards built-in privacy and security. A new market for authentication and security agencies, notaries and brokers emerged in 2011. It was possible to be an active consumer in a world supported by software agents.

The USO and the 000 service became redundant as universal and emergency call services were delivered by the market. Wired local access technology became redundant, replaced by spread-spectrum radiocommunications, software defined radio and wireless applications.

Rapid advances in AI led to the establishment of the AI Alternative Disputes Resolution (ADR) panel. In 2015, the High Court determined that AIADR decisions were binding when electronic monitoring data was the only form of evidence.

Tom Bowler, 45, is no longer concerned that a power blackout will occur because the market eventually developed sound backup systems. By 2010, the companies that didn't evolve had failed. It was after this that smart houses proliferated and retrofitting to 'get networked' replaced renovating as the new national pastime.

Tom now has all his house appliances connected to super-fast broadband. Efficiencies gained through real-time energy use monitoring have contributed greatly to Tom's energy-savings targets.

He is working face-to-face with his boss today, a rarity in a world of vidmeet that uses full wall video and surround-sound. Nothing quite matched the rich coffee and leather aroma and the actual views from the corporate display office—investors still like the marble foyer. It was his home duty to stack the dishwasher today, which he hates—when in this insanely high tech world was someone going to get a robot that could scrape and stack the dishes! Waiting to see the manager, his alert tone sounds.

"Yes?"

It's Lavinia his attractive VA (virtual assistant) who appears on his spec screen as someone who resembles his first girlfriend—a coincidence he has not shared with his wife. "Boss, the dishwasher has malfunctioned. Your household VA can't find what's wrong with it and communications with the service company are a no go. You need a flesh tech to check it over."

"OK, let's get it organised."

"Right boss" Lavinia drops her private persona and assumed her formal manner, because what follows will be recorded for his audit trail. The AIADR (or 'Big Momma'

as VAs sometimes referred to it in privacy mode with their clients) likes things serious and precise. People had lost cases in the AIADR because it decided they'd been joking—machine AI can be very literal. Because of those cases, most people and their AI agents switch to formal mode and auto-recording for transaction interactions.

"Executive confirm. Dishwasher malfunction. Remote assist cannot rectify. Service call negotiated. Cost acceptable. Service personnel access authorisation required—one time entry protocol prepared. Do you wish to proceed?"

Tom contemplates drilling into the cost and dismisses the idea instantly. Last time he asked Lavinia about a cost negotiation he hadn't been able to shut the VA up for at least a minute—he will have to get the agent valet service to fine tune the budget reporting sub-system. The financial parameters work and that's what matters.

"Proceed with access authorisation—one time today only," he says.

"Tradesman authorisation confirmed."

Lavinia vanishes from the screen. Tradesman access means full video monitor and full recording of movements, alarm for activity outside the designated service area and a discreet indicator to inform house occupants about entry and access.

Lavinia will also inform the VA agents of his family members. These agents will alert them if it is relevant or necessary and place an item in their schedule for reference.

Tom has a few moments to spare and places a call to his mother, Anne.

Since having a stroke in 2014, Anne's health has been poor, but advances in health care mean she has been able to remain in her own home. She has delegated authority for her privacy protection to an agent, which automatically ensures her personal information is used in accordance with legislation and in a manner Anne feels happy with. Because of this service, Anne was entirely comfortable when her health records were downloaded to an ambulance last week, enabling treatment to be swift and effective.

Three hours later, Tom is in the company brainstorm (B/S) centre. Taking advantage of his face-to-face time, he is catching up with a couple of people in person and another via vidmeet with a shift buddy from LA. "But how do we get consumers to pay for 3D content?" he is asking when Lavinia whispers in his earpiece, "Dishwasher trouble."

"Excuse me," he says to his colleagues. "What is it?"

"It needs a new part—burnt out torque rectification bush or so the flesh tech says."

"Patch me through to him. Do you mind if I grab a wall guys?"

One of the walls of the B/S room switches from its usual corporate display to Tom's kitchen from the angle of the house cam. A repair man looks at the camera and holds up a small white object. "Burnt out here," he says, pointing.

"Zoom in on that," says Tom. The hi-definition screen shows the burnt-out part.

"Check quote."

But Lavinia has already queried several sources and previous jobs on the Honest Tradesman Register (HTR). "No problem. Audit trail ready to log."

"Tell him to go ahead," Tom says.

The wall screen resumes its corporate display. The part will be replaced and the bill automatically processed. If the repair fails within 12 months, not only will it be fixed free, but a negative report will go into the HTR. Video entry logs to the house will be deleted tomorrow; financial logs are kept indefinitely, in case AIADR needs them.

Scenario 2: Big Daddy



“Increasingly, devices are easier to use... (and) fully interoperable.”

In this scenario, the network is dominated by a few big players. An interventionist ‘parental state’—protecting you for your own good—has influenced the development and use of national technical communications systems. While there is a strong emphasis on accessibility and useability, it has been accepted that some elements of society will be left behind in the pursuit of a global, market-driven (yet heavily policed) economy.

“People are online all of the time and access is a right”

There is trust in the network. People must use a government-issued identifier to have access to services. The centralised identification system, CentID, was originally used as the password to all government services, but by 2020 is the key to individual connectivity. The majority of consumers have traded data privacy for benefits including monitored healthcare, education and national security.

It is perceived that the government works to assure a greater good by actively monitoring its citizens. There is a high emphasis on subscription-based personal activities.

It is a story of realised technological possibilities, including quantum computing and a refined human machine interface. Communications and commerce have converged, with multiple service offerings through aggregation.

After a decade or more of social and political turbulence, the majority of Australians have compromised personal privacy and other individual rights to ensure their security and receive benefits in health care and education. Communications technologies are highly pervasive, with people only realising the true reach of these applications after they are in place. The narrative details a generational conflict relating to the application of communications technologies.

In a slightly different environment, consumers in Scenario 2 are protected by expanded USO-type arrangements as defined by the government. These arrangements ensure universal access to a basic level of services—access is a right up to a point, beyond which it is a subscriber-based system.

Scenario 2 narrative

It is a world of open seamless connectivity. Mature markets have modularised and it is a plug ‘n’ play world, except that there is no need to plug. People are online all of the time and access is a right. Increasingly, devices are easier to use across the population and are fully interoperable. There is trust in the network and decreasing levels of resistance to connection, because people must conform to have access to services.

Communications and commerce have converged, with multiple service offerings through aggregation. The network is dominated by a few big players. However, innovation is encouraged and the role of IP has never been more important—the *Economic Sustainability (Innovation) Act of 2015* enforces this.

The nature of the Australian workforce has changed—work is exported rather than labour imported. There is an increasing emphasis on a skilled workforce and access to education has been streamlined to facilitate this. At the same time, the wealth divide is increasing and some professions requiring intensive and hands-on education, such as medicine, are increasingly the domain of the privileged.

While there are open systems for connectivity, services are differentiated and pay-as-you-go with e-money (cash is an increasingly outdated concept). Occasional

communications vandalism such as viruses still jolt the system, but perpetrators are increasingly rare because of better detection and apprehension.

It is also a monitored society, where individual privacy has been eroded. Over the years, it has been recognised that advances in communications technology provide a greater ability to monitor and protect the health and safety of citizens.

From the early 2000s, a gradual increase in monitoring has been generally supported as the benefits for the ageing and infirm—as well as the advantages for law enforcement—became obvious. Fear and uncertainty regarding personal and national security became entrenched, and monitoring has been enforced through government policy and the Australian legislative framework. The intelligence model has replaced traditional policing.

ENUM, approved for use in Australia in 2006, quickly achieved a second purpose, that of a personal identifier. Convenience and simplicity meant that ENUM led to CentID, which became the central access point to a person and for a person to access services.

Resistance to this 'Australia Card revisited' was active from 2008, but there has only been a low level of disassociation from 'the system'—by then people were too dependent on the technology and the access it afforded them.

The defining moment was the biological attack on the MCG in Melbourne in July 2012. The person who activated the dirty bomb did not have a registered CentID. A centralised identifier would have allowed law enforcement agencies to prevent the attack. The government enacted emergency legislation—the Centralised Citizen Identification Act—resulting in compulsory CentID allocation for all Australian residents—identity conscription.

By 2020, there is pervasive monitoring of the individual and all transactions are tracked, monitored and recorded. Huge advances in quantum computing in 2010 created the necessary storage capacity and processing power. Society has become information-rich—data and information is constantly generated and harvested for government and commercial purposes. Audio-visual recognition systems are in place to track movements.

Tom Bowler, 45, is a piece-worker, taking online contract research work as it is available. He works for firms all over the world and consequently his hours are irregular.

His current contract is with the government of a nation deemed 'sensitive' under the new Employment Disclosure Act. The content of all voice and data sessions between Tom and his project leader are recorded and stored by the Department of Employment.

One morning, Tom is engaged in a videoconference with his project team when he receives an alert from his mother's health service—she has removed her monitoring bracelet again. He sighs as he realises his father is at work—returning at age 70 when the government decided that only those with no superannuation at all would receive the pension.

Tom excuses himself from the conference to 'dial' into his mother's home. He still thinks of it as making a telephone call, although the process is voice activated and he can make and receive multimedia sessions from any of his devices.

Tom's mother Anne was registered on a health monitoring program in 2014 after a stroke and now wears a subtle device around her wrist that monitors vital signs—any major change or removal of the bracelet results in family members and emergency services being notified. Section 8.4 of the Conditions of Privacy Act allows these authorised persons to have unrestricted communications with Anne at these times.

"What do you want?" his mother snaps as Tom's face appears on her in-home communications screens. Anne is reminded about the way her lifestyle has been restricted by the monitoring forced on her by her family. "It's as though no-one remembers the luxury of being truly alone," she thinks to herself, careful not to get too

angry and raise her heart rate. That would really excite everyone who is busy watching her.

“Mum, are you ok? Did you remove your bracelet again?” Tom bites his tongue so as not to mention the fee associated with the alert from the monitoring service. A sensible man, he appreciates that the cost of monitoring allows his mother an independence that was not possible in the past. He thinks of his grandmother, stuck in a nursing home for years, surrounded by people all of the time and TV and books her only entertainment, unlike the multimedia opportunities available now.

Anne puts her bracelet back on and waves it around for Tom’s benefit. “See? Happy now?” She hopes Tom can’t see the letter she has started writing by hand, on the table behind her. She’s not in the mood for being laughed at.

Later that day, Tom renews several subscriptions including, of course, the payment to the health monitoring service. Payments are electronic and centralised, but require his approval and identity verification using CentID. Tom appreciates this efficiency and thinks back to the days where he had to access his bank’s website to pay bills, and had different passwords and reference numbers for every account.

His membership of ‘EnviroMo’ is of interest to the government because it identifies him as owning a 2004 Holden Monaro. Under the provisions of the Environmental Monitoring (Individual Emissions) Act, Tom’s car is not allowed to be used regularly. Global emphasis on environmental obligations has resulted in Australia adopting closed loop covenants for improving the national environment.

For a fee, Tom is allowed to drive his car if pollution levels are low enough. His in-car sensor, compulsory in all cars, can be accessed by all of his communications devices. It advises him when pollution levels are low enough for him to be permitted to drive. Sometimes he likes to drive to the country and visit a farmers’ market, finding it quaint to touch the produce and pay in cash, rather than ordering and paying for groceries online.

Tom also subscribes to the location service for his nephew. Peter, aged 6, was implanted with a small chip at birth which allows family and friends to track his days (subscribers must undergo a comprehensive vetting process before gaining access to this service). Peter’s school allows registered users to check on students as they work.

Peter, one of the first children to be implanted, is too young to understand the full extent to which his every action is monitored. However, he does notice that his mother seems more relaxed about letting him go out alone than the mothers of his older friends who do not have implants. Peter is allowed to walk by himself to his grandmother’s house. She is currently teaching him how to write—this was dropped from the primary school curriculum in 2016.

Peter is also enrolled in the government-initiated Balance program, where exercise and calorie intake is monitored. If Peter has not reached his daily goal of physical activity his family and the school administration are alerted and advised to amend his food intake. Peter has already worked out how to manipulate this data to allow him to replace his lunchtime apple with a packet of chips.

Scenario 3: Nano-boomers



“...identities may be assumed informally.”

In this scenario, there is a fragmented global communications infrastructure and unrealised technological potential. The communications environment is converged, wireless and highly pervasive, but with poor performance in service delivery, particularly in verifying information.

This is an environment where the cyber world has as much or more meaning to people as the physical world—this has led to different forms of social interaction and degrees of connection, where individuals have the freedom to define and redefine their identity as they wish. These shifts in identity have contributed to a highly volatile sector.

It is an older, less trustful Australia where people are more fiercely protective of individual rights.

As with Scenario 1, in Scenario 3 there is high acceptance of the virtual world. The difference lies in the distinction between the virtual and physical worlds—in Scenario 3 they are not integrated and act within different governance frameworks. In the 'traditional' sphere, government defines the legislative and regulatory frameworks in an otherwise self-regulatory environment. The virtual world is largely unregulated, but offers many of the same services as the physical context. Identity can be situational, which leads to both alienation and the development of new communities of interest.

Scenario 3 narrative

It is 2020 in a world where identities may be assumed informally, in both the physical and virtual worlds. Government plays a central role in the development and maintenance of legislative frameworks, but people can opt in or opt out by choice within this framework. They have freedom and choice in a world of converged and wireless communications.

While the individual is able to maintain control of their social environment, there is a lack of trust in the ability of the system to verify identities or an organisation to identify a customer. Security and authentication processes are commonplace, but networks are widely dispersed. This has resulted in erratic and sometimes poor service delivery. This has frustrated and alienated sectors of the ageing population.

2020 is a time of transition, where frustrations and opportunities can be managed together.

Tom Bowler, 45, is driving his mother Anne, 76, to the funeral of her friend Jim Smith. Heavy rain starts as he approaches the venue. He has forgotten his umbrella. The forecasting service has neglected to alert him it was likely to rain. Every car space outside the venue is full, so Tom drops his mother off and asks his car to find the cheapest available space nearby.

Tom's nephew Peter, 6, has personalised a few applications in Tom's car. The voice of 'Beep', the lead character in the most popular children's cartoon since 2015, guides him to bay 5 on level three of the car park and tells him he's about to miss the eulogy. Tom hopes his automatic payment system has processed the fee.

Running into the venue, Tom asks the AI receptionist for directions.

"Take the elevator to the fifth floor and it is the second reception room on the right. Room 504 to be exact!"

"Thanks, most helpful", Tom says, puffing.

"You're welcome, Sir!"

Tom slips into the room just before the doors close.

Anne met Jim when they were both in hospital in 2014. Anne had suffered a stroke and Jim had developed a rare health problem late in life—something to do with blood clotting and restricting blood circulation. To combat this complication, he was regularly injected with a new antigen agent that flowed through his blood, monitoring and initiating or requesting repairs as needed.

There has been a lot of innuendo about Jim's death—had the health system network failed or had his identity been confused? The investigation into his death will involve

MEDALERT in Seattle and Netprov Transnet in Beijing. Jim's status as co-founder of the Virtual Identity Rights Group (VIRG) will mean the findings are public.

"Good afternoon, brothers and sisters, persons and virtuals. Thank you for coming together on this second day of April, 2020. We come not to mourn the untimely passing of a friend, struck down in the prime of his third age, but to celebrate his life.

"James Phillip Smith was known to the government as AUSTID 4075/235253/AM, but to you and me, he was simple Jim Smith, a quiet, unassuming corporate citizen of our great country.

"Jim ended a long career with the telecommunications industry in 2005 and moved to enjoy a comfortable third age. He was just entering his prime when he was taken from us at the age of 76.

"Jim was married twice and is survived by his daughter Mary, his daughter's partner Maria and their daughter, Jim's granddaughter, Nikita. We're glad they can join us today by NetLink from Lima.

"Jim was well loved and well known in the suburb of Camberwell here in Melbourne. This location, so close to public transport, served him well during the petrol problems of the terrible 2010s.

"In early years, Jim was heavily involved in community activities, with a strong interest in technology. He received the honour (he believed) of being considered a full digital native."

Tom drifts off as he considers his own status—very much a digital migrant. Even in his 20s, Tom was never an early adopter; he was always too aware of the cost of individual services. As applications and networks converged and prices dropped, his interest grew, but the e-voting fiasco of 2012 made him nervous. Some people lost all records of their life.

After that, you couldn't escape the privacy campaigns emphasising the need to prevent the misuse of technology and ID controls. It was perceived that the way identity was managed and used was considered to be outdated and out of touch with current values. And so began the great identity reconciliation.

A referendum resulted in the government taking control of identity management. This was supported by the insecurity surrounding the protracted war on terrorism, the Sydney water supply attack in 2005 and the 2008 flu pandemic. Tom voted for the change because he wanted to feel secure and to know his bills would be paid on time.

Tom's focus returns to the front of the room as a young woman stands up to speak.

"Hello, my name is Sarah. I didn't know Jim Smith in the way that some of you may have. Actually, I never met Jim. However, I was good friends with Anastasia, one of Jim's virtual identities, and it is why I came here today—to pay my respects to Jim, her creator. Anastasia has also departed from her virtual existence.

"I was involved with Anastasia through Actors Equity Online. Since the majority of films are now digitally created, there is a thriving alternative industry outside of the traditional industries. Anastasia was a highly regarded virtual actress and was a board member in Actors Equity Online.

"Anastasia was married five times—although some did only last a few weeks. To my knowledge, she never bothered with divorce because it was such a costly process even for virtuals. I will always remember Anastasia. She will remain as she was—beautiful and ageless. Her intelligence will live on. Thank you".

The second speaker joins by NetLink.

"Hello, I won't stand at the podium (laughs from guests) and will be brief because I don't wish to be a target in case any of YOU are THEM. I too didn't know Jim Smith; I'm here to talk about the person I knew—Neon. Neon and I were part of a group of environmental activists, campaigning against polluters and destroyers of the planet. I

remember the day we draped a virtual wall banner around one corporation's network systems, shutting them down for weeks.

"Neon and I couldn't use the accepted virtual meeting places and channels, with their identification and authentication procedures. We needed to hide our identities. Instead, we used the alternative media and back channels. But you couldn't trust anybody, there were infiltrators and spies.

"Except Neon, he was special. That's why I am suspicious of his death. I know Neon was on a deep cover assignment and could not be contacted. To hear of his death is tragic but suspicious. I must go now—there are people with dark sunglasses about."

Anne rolls her eyes at Tom. He smiles and, as people stand up around them, he wonders what secrets he'll discover about his mother when her time comes.

Scenario 4: Marching together into the future



"Communications is a key priority."

This narrative describes a highly cooperative environment where there is a rapid pace of change, supported by unified national priorities.

This is a joined-up sector, with alliances and partnerships. The scenario assumes that people share the view that self-interest should be aligned with the greater good for all. The formation of an Australian communications institute signifies both collaboration and a tendency towards centralisation of power and influence.

The technology focus is on developing 'killer' applications⁴⁵ and funding the necessary research and development related to those applications. This emphasis is consistent with global efforts in this area.

"Australia is now on the receiving end of the brain drain."

There is a stable Australian economy, with attractive financial and business development options that give industry greater freedom to operate.

Communications applications and frameworks are highly pervasive and invisible to the user. There are knowledgeable consumers and high trust in the system, but there are some vulnerabilities relating to consumer protection.

Scenario 4 narrative

In 2020, communications is a key priority. Users are open to new applications and services and there is a high level of trust in the systems. The government and the broader Australian community realise the importance of communications. It ranks with sport in the Australian psyche. Research and development has been nurtured and industry development and innovation encouraged. Australia is now on the receiving end of the brain drain.

This has created a capacity to not only manage crises effectively, but to emerge from them in a stronger position. Australian borderless enterprises enhance our economic and environmental well-being and underpin effective delivery of global online services.

Given the churn of innovation, the capacity to manage complex jurisdictional and consumer protection issues is somewhat diminished. Public interest and confidence is

⁴⁵ Applications that are innovative and popular

reasonably high, but there are still vulnerabilities regarding some emerging technologies for early adopters who are not yet protected.

Tom Bowler, 45, has received an invitation to a function—the Australian Institute of Communications (AIC) has been awarded the Australian Achievement award. The communications sector is coming together to celebrate its success, recognising their status at the forefront of productivity and export performance for three years running. It is a significant accomplishment.

Ten years ago no-one believed the information, communications and entertainment technology (ICET) sector would make such a rapid and significant turnaround. But all the foundations were in place. Although it had a rocky start, the role of the AIC in managing the radio spectrum crisis of 2008 had established its international research and industry development bona fides.

Leveraging this success and maintaining neutrality in the European–American conflict over standards and regulatory regimes, Australia (alongside Ireland) initiated regional and global dialogue about the future governance frameworks for the communications sector. A principal achievement was the adoption of integrated consumer protection standards.

Countries in the region—particularly those looking for a safe investment haven—began to invest in Commvnt, the venture capital fund the AIC had carefully nurtured since shortly after the turn of the century. Training of young technologists and investment in the fledgling integrated communications science lead to some early successes and contributed to a growing export record.

In Tom's opinion, the greatest benefit of the AIC's work has been the invention of *whats~~that~~*, an information framework, which helps consumers to easily determine their unique communications needs. For Tom, a digital migrant, this eliminated much of his confusion in the early 2000s caused by the array of communications technologies, services and applications available.

Tom arrives at the venue and takes his seat. International guests have linked in from the comfort of their own living rooms around the world and their images are displayed on screens around the world. There is a buzz of excitement in the room.

The voice of Sammy, the virtual bilby mascot of the AIC, opens proceedings. "Tonight we are joining the AIC in celebrating their Australian Achievement award. Please make our host for the evening very welcome!"

Tom joins in the applause as the CEO of the AIC appears on stage. "Thank you so much for joining us here this evening. I am pleased that so many of you could make it to our physical venue, and I know those using our virtual facilities will be impressed with the number here.

"I am delighted to accept this award on behalf of everyone at the AIC. It recognises the fact that Australian communications industrialists and service providers are shaping our economy and society in a very positive way.

"The AIC has coordinated multiparty investment in an innovative industry, supported by technology and convergence. This has resulted in the development of a sound and flexible framework. The industry decision to provide no-cost voice calls, a common infrastructure, commoditisation of carriage services, open broadcast markets and near-ubiquitous broadband—wireless, fixed and mobile—has underpinned creative, adaptable global companies and service alliances. The AIC is proud to be a part of this."

From the audience, Tom thinks about the changes in communications he has seen since the early 2000s. He doesn't think that the technology itself has changed profoundly, but the manner in which it is realised and applied has. Nothing that emerged in the last 10 years was necessarily a surprise. However, sometimes people were. He chuckles to himself as he recalls the immense popularity of the virtual yoyo for Christmas 2017.

He sees the way in which the efficiency and consolidation of communications has helped his parents. His mother Anne, 76, had a stroke in 2014, but excellent coordinated care resulted in a quick recovery that enabled her to return home. Medical services are 'always online' for her, but she initiates that contact. Should she fall or not be able to request assistance, subtle sensors in her clothing and home would alert her family. The sensors are aware of movement and body heat and have no other data collection use.

There are some residual concerns from the privacy crisis of 2012, but people are generally quite confident that the glitch was well-managed and the appropriate verification mechanisms put in place. Australia's trust gateways are now unrivalled in terms of international reputation.

The simplicity of technology—the user does not need to be aware of the behind-the-scenes complexities—has encouraged a high take-up, with even Tom's father becoming a user. The savings achieved through increased efficiencies has convinced most people that the communications sector is a good news story.

A practical man, Tom also appreciates the way his administrative life has been simplified. The Government Online Service (GOS) is an excellent example. Delivery of government services has been centralised and access is universal. Investment in communications associated with the delivery of health, education, exports and other essential services have underpinned the current high standards of delivery and public support for GOS. The best part is that taxes are periodically adjusted to reflect the efficiency and effectiveness of improvements achieved through online delivery.

Tom isn't so sure about other changes. Erratic weather patterns, rising sea levels and urban sprawl have had a significant impact on where people work—most Australians now prefer to work at home, commuting only when absolutely essential. Of course, the technology and systems support this choice.

Many of today's young entrepreneurs have only experienced the virtual workplace. Tom thinks of his nephew Peter, 6, who may never know how it feels to drag himself out of bed every morning and shuttle into the CBD. He may never realise the difference between talking face-to-face and virtual interaction. As his attention returns to the speeches, Tom wonders if this is a good or bad thing.

Scenario 5: Green prison



“...a longstanding crisis of confidence in Australia.”

In Scenario 5 there is little trust—it is a culture of fear in an unstable ‘war-time’ economy. The public are sceptical about those in positions of authority although there is a high emphasis on environmental accountability.

The unstable geopolitical environment has motivated a concentration of power and influence in both government and market dominance terms. Government introduced a central identifier using RFID and led the development of measures to allow data-mining and surveillance. The communications sector is dominated by large global companies that are hard to regulate from a national perspective.

Communications technologies are highly focused in certain sectors, namely national security and law enforcement, in areas such as surveillance and monitoring. Applications are funded when they provide a useful platform to meet national strategic priorities.

Although there is collaboration in standards development, communications technology is pervasive—it is intrusive and regulation cannot keep pace with change. System failures and quality of service problems are the result of a fragmented and limited communications system.

Scenario 5 has a strong regulatory and legislative framework that industry and citizens must adhere to; for example, a universal service obligation for broadband suppliers. For the consumer, service delivery consolidation within Australia and with global partners provided some simplicity in day-to-day transactions, but resulted in loss of individual privacy. There is unreliability in systems.

The social context of Scenario 5 is government controlled and monitored. The individual has no right to privacy under the guise of a strengthened information management framework—but there are set service standards within these boundaries.

Individuals are increasingly entrenched in the communications system, with personal identifying information required to access and use services. Social and economic reliance on continuity of service is likely to become more pronounced. Ensuring uninterrupted service will clearly be of considerable importance.

Scenario 5 narrative

It is 2020 and there is still a very real community concern regarding the application of information and communications technology—a longstanding crisis of confidence in Australia. The majority of people desire the positive benefits of communications technologies, but the rights and obligations surrounding communications can’t keep up with the rate of change.

Communications technology is pervasive and intrusive. It is a world in which making the choice to opt out is very difficult and developing an effective system to respond to consumer preferences is equally problematic.

Tom Bowler, 45, is on his way to visit his mother, in her nursing home. Anne, 76, had a stroke in 2014 and her family found they couldn’t afford home care. After the super funds crisis in 2007, his father’s savings were wiped out and he was forced to return to work. While in good health, his father’s shifts and his financial situation did not allow him to provide Anne with adequate care. They were lucky to find a publicly-subsidised placement.

Tom experienced long periods of unemployment from 2008—international tensions and the renewal of the nuclear debate on the southern Asia peninsula exacerbated internal fiscal woes. Any remaining enthusiasm for the Beijing Olympics had been stifled by rigid security arrangements, and China suffered massive financial losses with huge flow-on implications for the region. The Australian Government, struggling to support the influx of people into the welfare system, withdrew funding from tertiary education and state-sponsored research and development.

This morning, Tom is taking the train. “This is one thing we can rely on”, Tom thinks to himself as he looks around the carriage. Clean and efficient, the trains are driverless and essentially emission free. Payment is easy, with the fare deducted when his RFID is automatically registered. Tom loves the fact that he doesn’t have to think about it, although he does sometimes miss the sound of change jangling in his pocket.

Stepping off the train, Tom makes his way across the road to the nursing home. Narrowly avoiding being hit by the latest model hybrid car, Tom thinks longingly of his 2004 Monaro, permanently garaged at home. It is now illegal to drive or even register it.

Since the Greens gained the balance of power in the Senate in 2010, environmental issues have been a primary government focus. The use of cars, water, public transport and other services is heavily controlled. Pervasive technologies were embraced by the government to reduce costs and because of the positive impact on the environment—additional applications were soon realised.

Tom’s identity is automatically identified at the door of the nursing home. As Anne’s son, he has full access to common areas and her room, but an alarm sounds if he enters another person’s space. He learned this to his embarrassment when he took a wrong turn on his first visit.

As Tom wanders through the hallways, he considers other information that is collected about him. He knows his shopping habits are monitored, as are his financial transactions. His compulsory health insurance has required a genetic profile for years now, something which makes him nervous and has caused his premiums to rise steadily since his mother’s stroke.

Tom remembers supporting the government push towards a strengthened national information infrastructure/critical infrastructure (NII/CI) after 2005. It made sense, at a time of heightened security concerns, and the technology was there to allow effective data-mining and surveillance. It made him feel safe.

Communications technology really started to take off after that. After the worldwide economic downturn, Australia focused itself on standardisation and effective utilisation of networks and services. The government led a major push to align Australia with Europe and the US. A universal service obligation was enacted for broadband suppliers, to control the largely unregulated sector.

The government then decided to coordinate service delivery across the federal, state and local tiers through a consolidation of identity and technology—with radiofrequency identification (RFID) as the central identifier. This opened a large opportunity market for niche security agencies.

When RFID was widely introduced, Tom was concerned about many things, including possible health implications and the collection and use of his personal data. He could see immediate benefits—his day-to-day interactions with payment systems and government organisations became easier, with only the occasional lost bill.

At the same time, he was very aware of a resistance within his local community to the increasing censorship and sense of enforced conformity. He saw a resurgence of distrust in the technology that supported the systems.

When Anne had her stroke, Tom’s family were troubled by the lack of coordination between her various stages of treatment, despite all her medical history and requirements being stored in a centralised system. In the major hospitals, the majority of scheduling is done automatically, using an AI application. To make matters worse,

Appendix 1

the insurance company once refused payment because they could not accurately verify Anne's identity—her RFID had been temporarily erased.

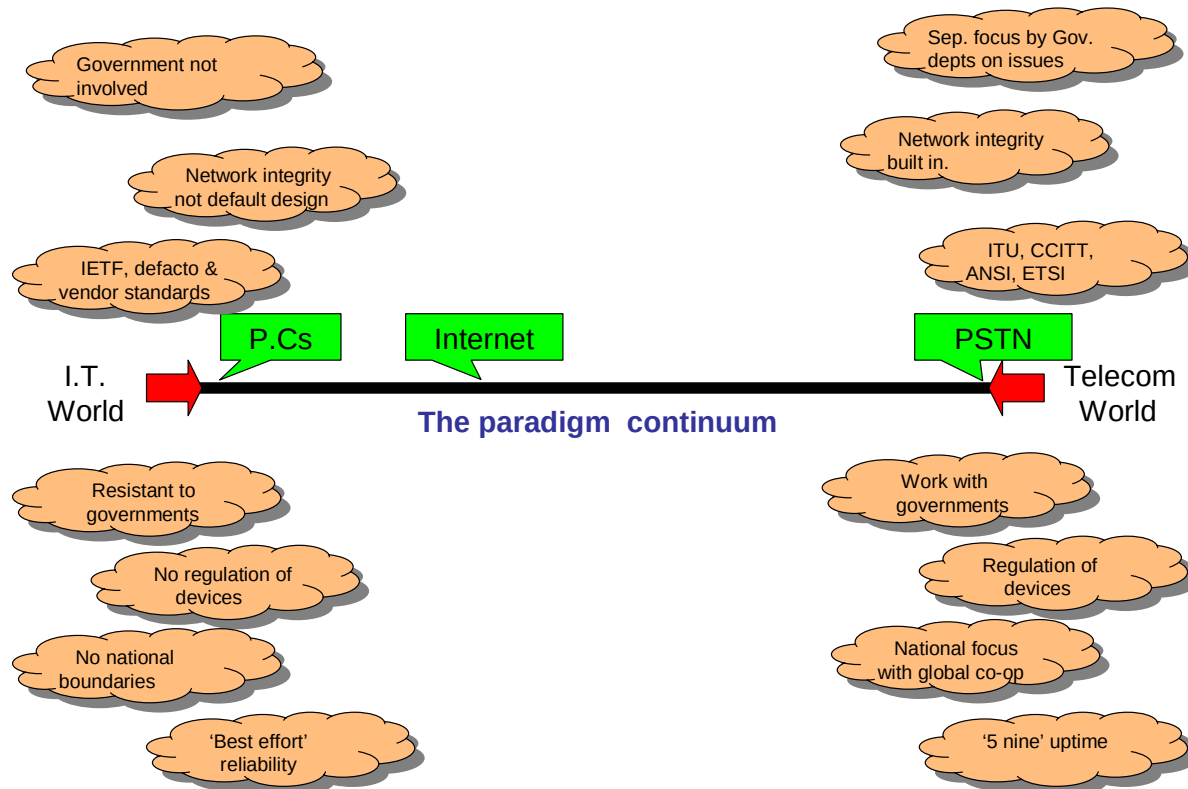
A national review of hospital procedures soon uncovered a systemic misuse of patient's genomic data. The findings of the independent inquiry resulted in a major overhaul of data management and transfer.

Tom still doesn't necessarily trust the system, or the technology that supports it. He has seen the worst and best outcomes through his mother's experiences. While the frameworks that surround the technologies have again been strengthened and have begun and keep pace with change, he is reassured by the fact that Anne's nursing home still has human nurses. He smiles as he walks into Anne's room.

Appendix 2: Clash of culture

While the understanding of culture is a non-trivial activity, it is worthwhile to give a brief analysis of why these differences occurred. As with most studies of culture, the answers are in the history of the players. By considering the history of the main groups (operators, Internet and IT) a basic understanding of why things are the way they are can be gleaned.

Figure 2 'The clash of cultures' – Internet verses Telecom



The Internet

- It was developed originally by the military as a closed trusted medium that needed to be resistant to nuclear attack and internal security was not an issue because everyone could be trusted (it was only military people talking to military). The Internet was designed not to be single point sensitive.
- It was adopted early by western academic Institutions because academia has a culture of allowing completely free and uncensored flow of information, which has flowed into current thinking with any form of censorship strongly opposed.
- For the Internet to expand could only be achieved by agreed cooperation and hence today, decisions such as within the IETF are still made by consensus, not by voting.
- The early Internet was seen as a peering agreement between institutions, with the power of the medium achieved through this peering concept. Today, it is still a collection of private networks that become valuable in their ability to connect to each other.
- The Internet was expanded by 'computer geeks' for 'computer geeks' and hence there is a focus on technology rather than political considerations.

IT

- PCs were not originally designed to be connected. The original concept of the 'The Network is the Computer' (motto of Sun Microsystems) led to a relatively late and heated

debate in the computer industry. As a consequence, the PC was not originally designed to handle the security issues associated with being online. Security is much easier to build in than design on, which is why today's computers are still struggling with security.

- PCs were originally designed to be non-critical, discrete devices. If one computer stopped working, this did not affect other users. This culture of non-criticality has permeated the industry and is only now evolving.
- Because computers were generally not networked, maintenance methodologies developed along very different lines.
- Most of the dominant companies are relatively young and American based.

Telecommunications

- Operators are traditionally made up of quasi-government organisations.
- Unlike the IT industry, many of the major vendors are not American.
- The operators are used to running very big, interconnected systems.
- The major vendors are large and maintain strong market dominance.

Appendix 3: Spam – a case study

How the current activities associated with spam provide insight into future problems & opportunities.

In itself, spam and the international attempts to stop it appear relatively mundane. However, the challenges associated with spam regulation provide an interesting insight into more holistic problems that will affect all facets of communication regulation. By comparing and contrasting the experiences of dealing with spam today, we can anticipate many of the problems that will face regulation in the future.

Buy-in

In many ways, 'spam regulation' should be the easiest to manage because it has huge public 'buy-in', or support. With the exception of the actual spammers, of which there are probably fewer than 100 'hard core' operators, no one likes spam. Therefore spam regulation appears to set the extreme end of positive commitment to a solution. Despite this positive energy, experience has shown that it is still difficult to get consensus about the best way forward to stop or reduce spam.

This highlights the difficulty in reaching an agreed way forward for more controversial areas where not everyone agrees. The challenges faced by spam regulation can provide some guidance for future telecommunications regulation.

Technical solutions abound

There are technical solutions that could solve the spam problem—technology in itself is not the problem. 'Band aid' fixes such as spam filters and blocking lists only fix symptoms, not the root cause. They are popular because of the lack of a system to effectively roll out systemic solutions for the global network. There is no way of globally mandating changes to the network. Temporary fixes are used because they can be deployed individually and do not require coordination.

This problem should not be considered lightly. In general, communications engineers consider problems from a technical rather than a social perspective. In any network environment, such as communications, railways or language, it is the coordination of 'standards'—be they technical protocols or human language—that is the challenge.

This will be a critical issue for communication networks because there are a large number of technical 'solutions', but an integrated method must be found to successfully change them as the environment changes. This type of failure is evident with the current email standard/protocol/technology. When the email protocol was developed in the 1970s, it was never expected to have to deal with the current environment, where there are potentially millions of non-trusted or malicious users.

Philosophical differences

One person's spam is another person's valuable product information. There are also cultural differences in attitudes to censorship and free speech, which affect national spam laws. For example, the USA has opt-out legislation because they believe the right of free speech overrides the right of people not to receive email they do not want. This challenge with spam is minor when compared with more common telecommunications differences over standards such as for GSM and CDMA, W-CDMA and UMTS.

The approach taken to international cooperation

While organisations such as the ITU and the IETF have been very supportive of anti-spam initiatives, they do not have the power or authority to do anything by themselves because of the nature of these organisations. It is left to groups and organisations that 'own' the various parts of the Internet to take action.

Summary of why spam is such a problem

- Technical solutions are hard to deploy globally.

- Spam is generally sent from one country to another, crossing legal jurisdictions.
- There is a lack of global standardisation of spam laws.
- There is a lack of operational coordination between law enforcement agencies against spammers.
- The design of the existing email interface was based on the assumption that all users could be trusted, which is one of the reasons why there is no sender authentication.
- It essentially costs nothing to send an email and the cost-benefit for spammers is high.
- Most PCs in the world are insecure and can be used illegally as 'hosts' to send out spam.
- The number of PCs in the world is growing every day, they are becoming more powerful and have faster internet connections.
- There is no global coordination body that can make changes to the Internet mandatory.

Summary of learning from spam into the future

- Technical 'solutions' abound, but the solutions to network problems are rarely technical.
- Rolling out technical solutions into the network is difficult if the 'network' is owned by many separate parties, as is the case with the Internet, that have no formal agreement to cooperate or coordinate their activities.
- The network becomes inherently insecure as a result of 'device intelligence at the network edge'. Because of the sheer number of devices involved, technical and procedural systems need to be in place within the network to minimise the damage individual network elements can cause.
- Getting effective global agreement from regulators and government is difficult to achieve. 'Organic regulation'—where a 'standard' method is implemented in one discrete domain or jurisdiction and is distributed gradually through one-to-one agreement—seems to be effective.
- It is difficult to achieve high-level government strategic agreements that are timely and effective. However, low-level operational agreements can be achieved relatively quickly and can facilitate the creation of high-level agreements over time.
- A key reason that spam is so hard to combat is that it crosses multiple boundaries—networks, governments and jurisdictions—that do not have effective or timely interfaces. With communication becoming global in nature, significant emphasis must be placed on developing effective interfaces between the various parties involved.
- Most regulators struggled with the challenges spam creates because they had to develop new skills and knowledge, since few regulators had a good understanding of how the Internet works, and new relationships with ISPs and the Internet industry.

How this case study relates to the Vision 20/20 project and its recommendations

While the aim of the Vision 20/20 project report was to consider the next 15 years of regulation, it is clear that the issues already highlighted by spam will be systemic. The immediate challenges posed by regulating spam may help 'bridge the paradigm gap' between current and future regulation.

Specific recommendations in the Vision 20/20 project report directly correlating with insights gained from spam regulation include:

- a) Section 4.2.3. Develop a total 'communications systems' approach to regulation
- b) Section 4.2.4. Promote cooperation and collaboration
- c) Section 4.2.5. Promote network integrity and agreed e-government and e-commerce frameworks
- d) Section 4.2.6. New challenges in digital content
- e) Section 4.2.8. Develop new skills and abilities.