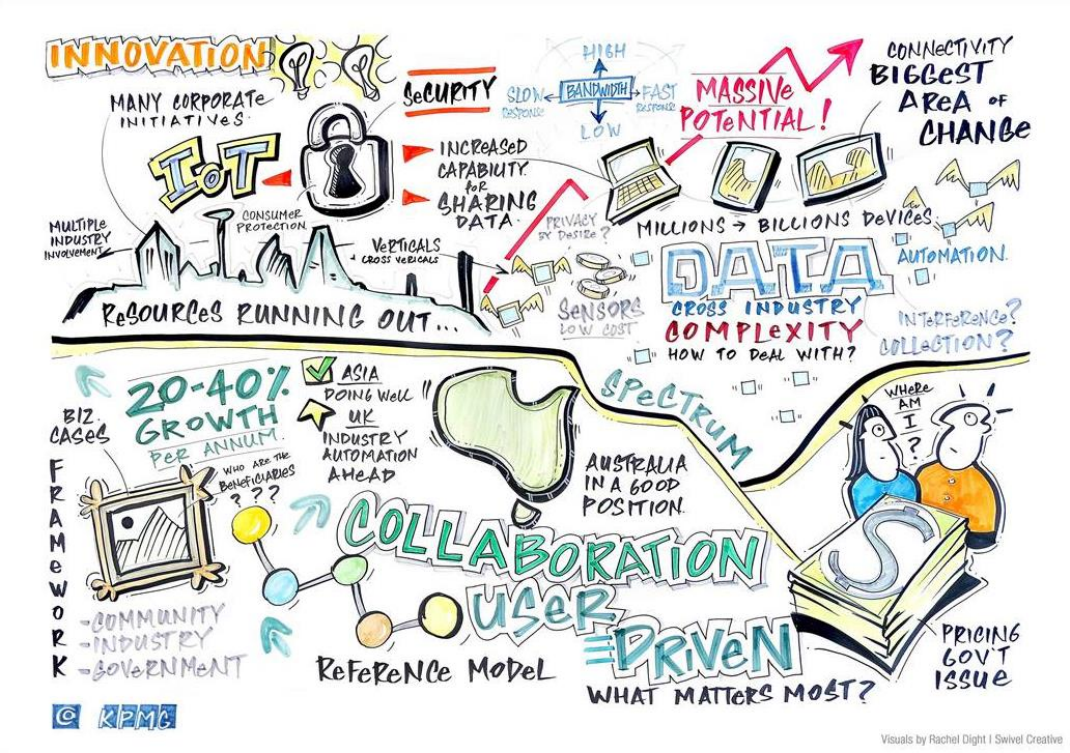
COMMUNICATIONS ALLIANCE LTD

Enabling the Internet of Things for Australia

Measure, Analyse, Connect, Act



Written by Geof Heydon and Frank Zeichner

October 2015

CreatorTech

Communications Alliance Internet of Things Think Tank

An Industry Report commissioned by the Communications Alliance Internet of Things Think Tank Executive Council

First published: October 2015

The Communications Alliance Internet of Things Think Tank was formed in May 2015.

The Think Tank's vision is to be a leading ICT industry initiative under a broad industry framework shaping the regulatory framework to harness for Australian industry the opportunities generated by the internet of Things. The Think Tank aims to define the IoT eco-system, inform and enable Australian companies to exploit the business opportunities afforded by IoT technology and services.

INTRODUCTORY STATEMENT

For the Australian economy and society, the rapid emergence of internet of Things (IoT) represents both a significant opportunity and a very real threat, depending on whether and how the nation adapts to and harnesses the power and potential of the IoT phenomenon. At stake is the opportunity for Australia and Australian companies to be early beneficiaries of industry renaissance and the emergence of new business models through IoT and the opportunity for Australia to become a significant exporter of business solutions enabled by IoT – if the policy and regulation setting can be optimised early to support business-led innovation.

The scale of IoT growth and the pervasiveness of its influence will mean that elements of our current telecommunications regulatory framework may be overwhelmed and/or might act as inhibitors to Australia's ability to reap fully the benefits of the changing environment. It will be imperative to address regulatory (and other) inhibitors early and to simultaneously create an environment that allows enablers of IoT services to be brought to its full potential.

Special Thanks

Undertaking a study of a subject as broad as IoT with the IoT Think Tank remit was exciting and a little daunting. It could only be accomplished with the special help and advice from many sources.

We would like to particularly thank: John Stanton and Christiane Gillespie-Jones, the IoT Think Tank Executive Council, our many interviewees and a few that went just a little further, including Mike Briers, Reg Coutts, Michael Cox, Warren Lemmens, Chris McLaren Helen Owens, Paul Paterson and Malcolm Shore.

TABLE OF CONTENTS

Table of Figures

1 EXECUTIVE SUMMARY

The internet of Things (IoT) promises major telecommunications/ICT infrastructure market innovation and will enable 'vertical' industry productivity, innovation and business opportunity. It offers Australia significant and transformational economic benefit through smarter use of infrastructure, efficiency gains and new business growth.

The McKinsey Global Institute (MGI) has published a comprehensive assessment of the potential for IoT called "The internet of Things: Mapping the Value Beyond the Hype", putting an upper limit on its potential global economic impact by 2025 of $US11.1 trillion, or about 11% of the World Bank's estimate of value of the world economy by that time. **This translates into an impact on the Australia economy of up to $116 billion by 2025.**

This Report is an industry-wide view of:

- Australian regulatory and policy enablers and inhibitors for Australian IoT industry success
- Australian industry readiness
- Recommendations for policy and industry initiatives
- Proposed collaborative work streams for the industry, Government and other stakeholders, facilitated by Communication Alliance (CA), to help drive the development of the IoT industry and community

The research and findings are drawn from core expertise, local interviews with key industry and Government players, public workshops, a survey, extensive desktop research and supported by the generous assistance of the members of the CA IoT Think Tank Executive Council, who have directed the strategic and operational aspects of this project throughout.

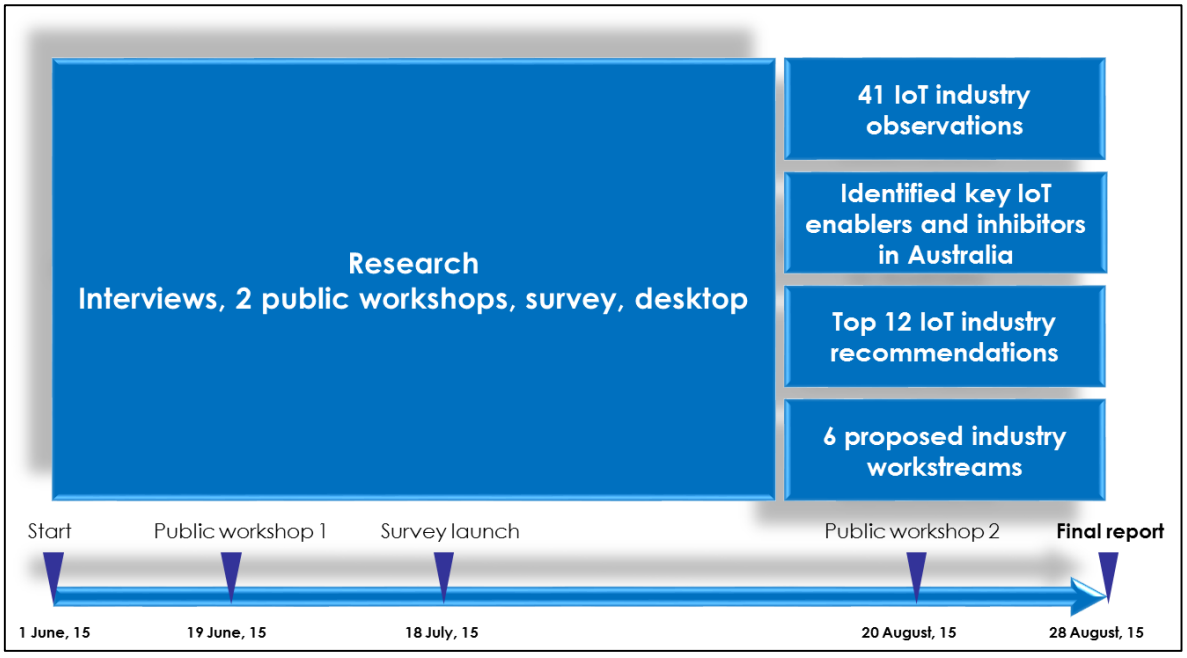


Figure 1: CA IoT Industry Report outcomes

A call to action – Australia's peers are active

The UK Government has acknowledged the role that the development of the IoT can play as part of its broader growth and innovation 'agenda2'. For example, in March 2014, the British Prime Minister announced a significant increase in Government funding for IoT projects, citing their potential to underpin a new 'industrial revolution'. In addition, the Government continues to fund the targeted development of IoT technologies and pilot studies through 'innovateUK3'.

The UK has also taken quite an aggressive view to opening Government data and this is proving to be a valuable contribution to innovation in that market and an enabler for IoT.

Similar national leadership is evident in Germany with its 'Industrie 4.0' program and in Singapore with the IDA smart city program, as well as the smart city programs underway in China and India, among other examples.

Accenture has developed a model for ranking countries and their readiness to embrace industrial IoT based on productive and innovative potential. Using Accenture's model, Australia currently ranks 11th behind the US, Switzerland, the Scandinavian countries, UK, Japan and Germany.

While Australia's fundamental capabilities are relatively good, given its high telecoms connectivity, educated workforce etc., we lack the IoT focus at industry and Government level of our peers in harnessing the opportunity IoT offers and we risk losing the opportunity for IoT competitive advantage and market leadership.

Focus on key market sectors

Applying IoT, by priority, to market sectors of greatest need or where competitive advantage may be gained makes good sense and follows observed overseas practice in our peer and customer countries. Refer, for example, to Germany's focus on industrial automation and China's and India's focus on smart cities.

A wide input of views have been received from many Australian ICT industry sources. We have seen a relatively consistent view that the most important market segments for Australia are mining and resources, transport and logistics, agriculture and the environment, as well as health, smart cities (infrastructure) and financial services.

As we consider Australia's traditional strengths and challenges, the opportunity for cost efficiencies and the barriers to entry, there a three sectors that stand out as most likely to transition to an IoT enabled global leadership position. The three sectors are mining and resources, food and agribusiness possibly including the environment, and transport and logistics.

In terms of greatest need and potential efficiency impact smart cities and health comes out strongly. While there are opportunities for significant transformation in these sectors, governance complexity bedevils both, as well as the issues surrounding data privacy for health.

IoT is both an industry vertical and a horizontal enabler

Characterising IoT is big and complex as it plays two distinct roles in the digital economy. It combines information technology, telecommunications, big data and analytics into a significant industry vertical as well as providing a horizontal enabler for every other sector. IoT becomes a significant infrastructure in its own right, enabling smarter, more efficient, more sophisticated, more innovative and more highly integrated sectors to prosper across the entire economy.

Key enablers and inhibitors

The key inhibitors and enablers for IoT success in Australia are drawn from the observations throughout the Report and are summarised in the following figure.

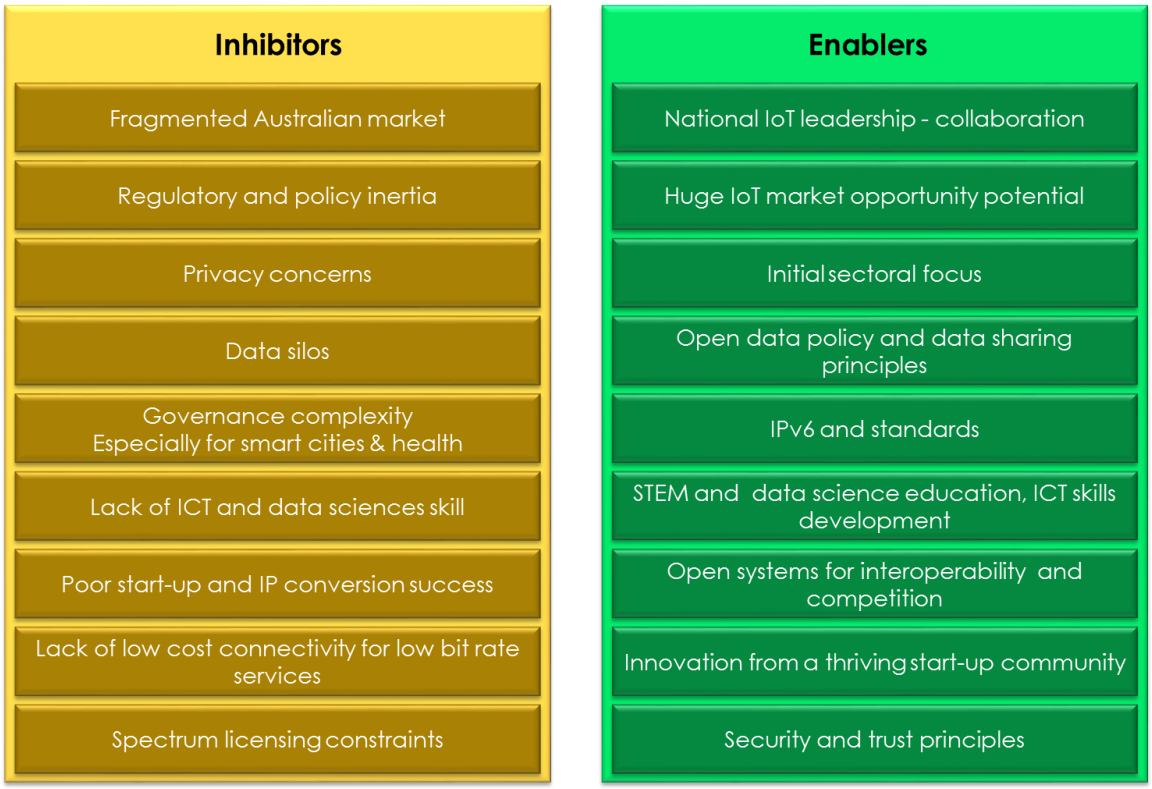


Figure 2: Key inhibitors and enablers

Through addressing the issues of the IoT inhibitors, opportunity, enablers and the IoT Think Tank's overarching aim to invigorate the Australian IoT industry and to help Australia become market leaders in some key focus areas, key recommendations are offered below for consideration:

It makes sense to align with key Government agency programs and strategies in the focus sectors of Department of Industry and Science (DIS) Growth Centre activities and Infrastructure Australia.

Recommendation 1: Develop and support a coherent and collaborative Australian IoT industry enabled by appropriate policy and regulation settings to drive productivity and innovation aligned with national economic objectives.

Recommendation 2: Choose leadership in a few key sectors where additional efforts are made at industry and Government level and collaboration is enhanced. Sectoral focus prospects where Australia may lead are in mining, agriculture, transport and telecommunications.

Recommendation 3: Develop a model and principles for IoT data sharing and opening of public data.

Recommendation 4: To build confidence and trust in IoT use, by addressing IoT privacy concerns with clear policy and guidelines for access to, consent and use of private data. Align with policies on open data and data sharing.

Recommendation 5: Develop minimum network/service security guidelines for the IoT service chain, from sensor/actuator, to network, to data. This needs to consider both security from attack and service resilience.

Recommendation 6: Encourage a thriving IoT start-up community through alignment, where sensible, with Industry Growth Centre activities, start-up incubators, focus industry sectors and collaboration to build eco-systems of innovation.

Recommendation 7: Review the adequacy of the current spectrum settings and licencing in accommodating new IoT wireless technologies and scale with particular focus on spectrum for low-bit rate services.

Recommendation 8: Encourage use of IPv6 by default on all platforms, including Government and internet Service Providers (ISPs).

Recommendation 9: Add weight to the drive for greater science, technology, engineering and mathematics (STEM) learning programs and develop IoT training programs, with particular emphasis on data engineering.

Recommendation 10: Review adequacy of Australian oversight and participation in the key IoT standards bodies with a view to having the capability to provide knowledgeable industry guidance on implications for trade impediments, data protection and local regulatory impact.

Recommendation 11: Consider reduction and simplification of governance in the development of smart cities in Australia.

Recommendation 12: More detailed economically sound, evidence-based research should be commissioned to confirm preliminary observations, recommendations, enablers, inhibitors and sectoral focus and which parties are best placed to drive initiatives and assume leadership roles.

These recommendations, and the report, are intended as input to Government policy makers and sectoral industry organisations to inform and influence thinking first and, hopefully, action next.

CA initiatives

CA, through its IoT Think Tank, will convene a powerful coalition of industry and broader stakeholders to carry forward the development of the IoT community in Australia. To that end, a proposed series of work streams supporting the above recommendations are being considered:

Workstream 1: Collaborative Australian IoT industry – Canvass support and develop a coherent, collaborative and globally-aware Australian IoT community with industry, Government and other key stakeholders to foster innovation and inform appropriate policy and regulatory settings.

Workstream 2: Sectoral engagement – Develop sectoral IoT advancement and alignment in key sectors, through Government Industry Growth Centre activities and key sectoral bodies with focus on mining, agriculture, transport and telecommunications.

Workstream 3: Open data – Develop IoT open data and data sharing principles and guidelines with possible sectoral focus. Data privacy – develop privacy guidelines for use of IoT data.

Workstream 4: Spectrum availability – Working party including the Australian Communications and Media Authority (ACMA) and broader stakeholders to address the spectrum settings and licencing needs for low bit rate wireless services, such as low power, wide area (LPWA).

Workstream 5: Security – Develop security guidelines for IoT services and service elements, including data protection.

Workstream 6: IoT start-up innovation – Develop policy and IoT eco-system frameworks in support of a national IoT program, which is linked to Industry Growth Centres.

2 THE INTERNET OF THINGS OPPORTUNITY

2.1 What is the IoT?

The OECD describes convergence between ICT and the economy on a grand scale, as the internet of Things[1]. The term implies the connection of most devices and objects over time to a network of networks.

The IoT is an environment that gathers information from multiple devices (computers, vehicles, smart phones, traffic lights, social media and anything with a sensor or actuator) and applications – anything from a social media app like Twitter to an e-commerce platform, from a manufacturing system to a traffic control system.

Where the IoT gets even more interesting is where information from devices and other systems is combined in novel ways, tapping into the huge processing capabilities available today to do the kinds of expansive analysis usually associated with the concept of big data – meaning analysis of data not necessarily designed to be analysed together to create beneficial outcomes.

The definition of the IoT by the ITU (International Telecommunications Union) is: "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies."(Recommendation ITU-T Y.2060)

IoT has sometimes been confused with machine to machine (M2M) communications which has been in use for a considerable period, albeit significantly increasing in the market through the use of mobile technologies. M2M is, in effect, a subset of IoT which is in the main restricted to specific bespoke solutions, within industries and indeed within companies, characterised by process specific sensors and devices.

The Machina Research chart below, shows the evolution from M2M to the IoT where the characteristics against scope and agility are represented.

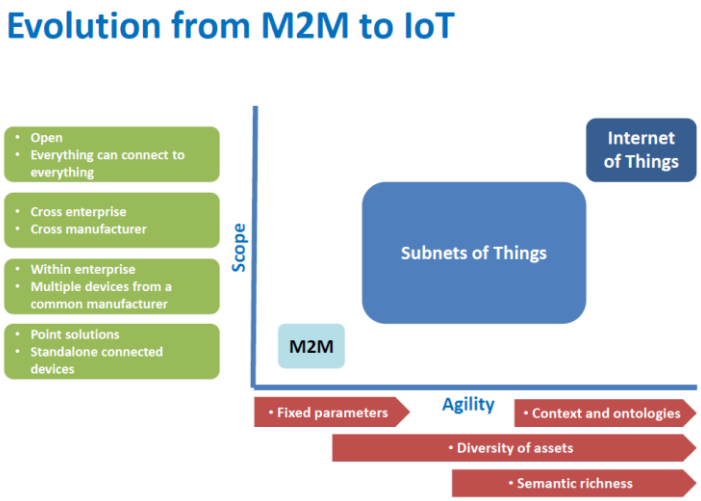


Figure 3: M2M towards IoT

[1] OECD Digital Economy Outlook 2015

2.2 Drivers of the IoT

While the basic technical elements that underpin IoT have existed for some time, a few key enablers in the availability, cost and sophistication of these elements are now opening, allowing IoT to be commercially viable, even today, in some sectors, and will allow, over time, a pervasive IoT environment.

Three key enablers for the IoT, illustrated below, are:

- The dramatic decrease in the cost of intelligent sensors (and actuators)
- The availability of near-ubiquitous connectivity; and at a progressively decreasing cost per bit
- Increasing sophistication in handing large volumes from disparate sources of data (big data analysis) which can uncover hitherto hidden value

Figure 4: IoT key enablers

Attempting to predict the future in any technology field is fraught with danger but it is possible to look at the rate of change over the recent past and extrapolate that forward. The figure below illustrates some important trends. This graph is not intended to be an accurate reflection of the past. It is intended to show a broad trend with a few proof points along the way. In 1965, Gordon Moore, co-founder of Intel, observed that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. This became known as Moore's Law and today is simply described as computer performance doubling every year.

Moore's Law has also underpinned the even more rapid increase in memory storage capability and at the same time has been behind the relentless cost reductions in electronics and computing. The following figure illustrates these trends.

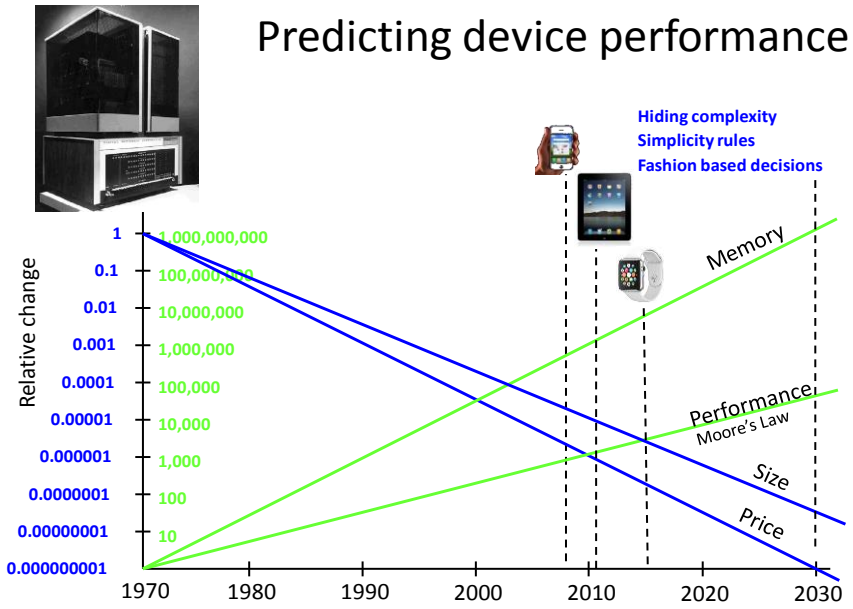


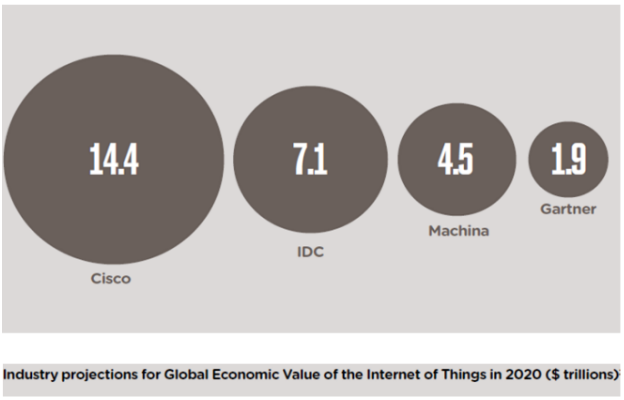
Figure 5: Predicting device performance

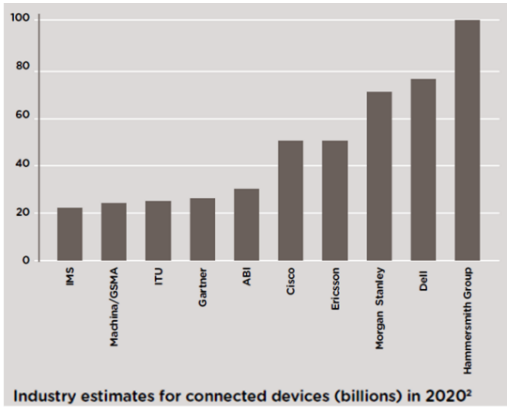
The relentless performance increase and cost decrease has made very low cost sensing, computing, communicating, storing and analysing capabilities possible. As these costs have come down and the performance has increased, cost effective solutions for complex problems have emerged and enabled a whole new range of capabilities.

Today it is cost effective to deploy an environmental sensor onto a single grape vine or on a single cow to gather information. At the same time the cost of sending this information to a database and processing it has also become very low. So what seemed impossible only a few years ago, today is becoming commonplace. And these trends will continue.

2.3 IoT Economic Potential

Estimates of the economic potential and value that IoT can bring have been made by numerous organisations. A chart below from the UK Government Office of Science includes a few well-known predictions.





Source: UK Government, Internet of Things Review January 2015

Figure 6: IoT Economic Impact

In addition, the same Office of Science report quotes a McKinsey report: "Disruptive Technologies: advances that will transform life, business, and the global economy", McKinsey Global Institute, 2013, predicting additional global value of $6.5 trillion by 2025, since upgraded to $4 trillion -$11.1 trillion in their recent "The internet of Things: Mapping the Value Beyond the Hype" report.

The industry projections for the potential value of the internet of Things for the global economy range in the region of $10 trillion by 2020, although there is considerable variation. Potential value is interpreted here as the potential value that could be realised.

Another common IoT growth measure is the number of predicted uniquely-identified internet connected devices. These range from very low cost sensors and industrial controllers to smart phones and large computer systems.

Figures for the number of internet devices are generally consistent over many sources (IDC, Gartner, ABI Research, BI Intelligence, Cisco, Ericsson etc.). The estimate for global internet connected devices in 2014 is 10 billion, with growth to up to 30-50 billion predicted by 2020. Figure 7 illustrates some of the market predictions of connected devices.

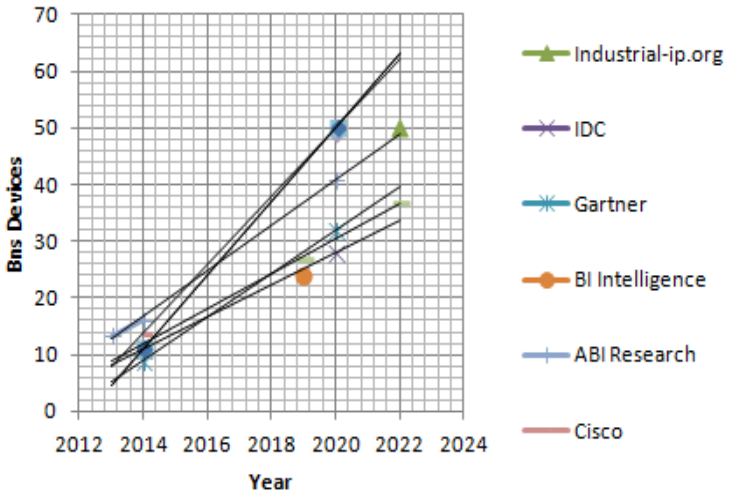


Figure 7: Predicted internet connected devices, billion

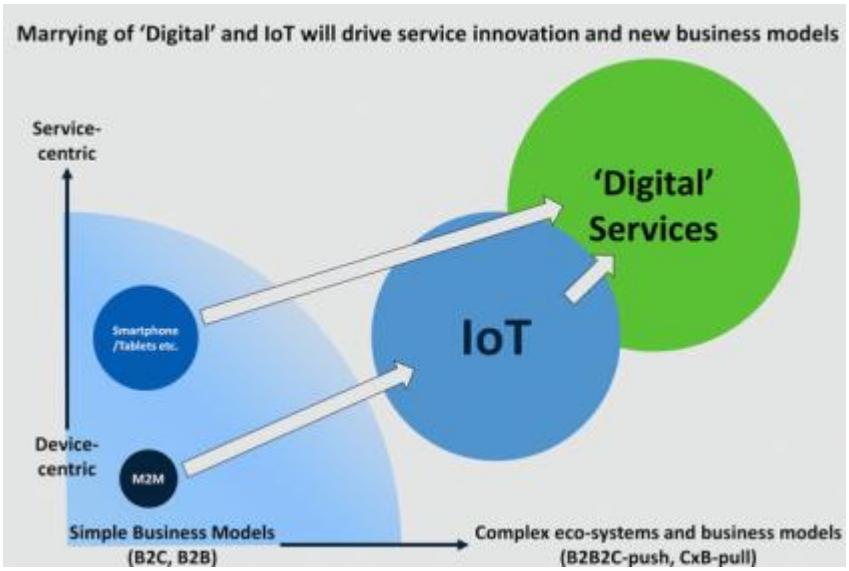
The above figures and also those quoted by the ITU, OECD, EU etc. all indicate significant growth in IoT opportunity for the ICT sector and also significant innovation opportunity across the entire economy.

Observation 1: There is a huge potential economic promise of productivity gain, business innovation and competitive advantage through the use of IoT.

2.4 IoT Market Impact

The capability of IoT to transform Government and business as well as business processes and models into new digital services will ultimately translate across the entire economy.

IoT will be an enabler to a wide range of new digital services across all market segments and business sectors.



Source: www.more-with-mobile.com

Figure 8: IoT digital services impact

IoT-driven digital services will impact Government, community, business, individuals and the home. The following figure positions IoT as an enabling infrastructure underpinning all other industry verticals. It is also practical to see the Telecommunications industry as a vertical as well as this horizontal enabler. Perhaps this is one of the reasons why it is difficult to paint a complete picture of the IoT impact.

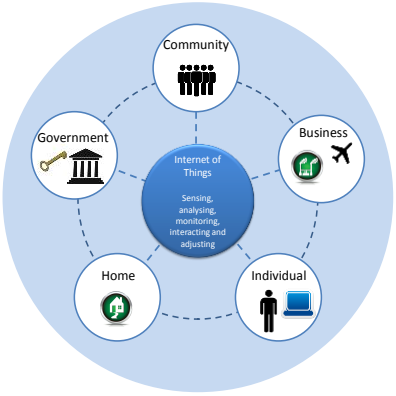


Figure 9: IoT has economy wide implications

Observation 2: IoT can be seen as both an industry vertical in its own right as well as a horizontal enabler for all other sectors within the ICT sector.

There are already endless examples of sensor networks and digital analytics creating new insights and innovative new digital services. Some diverse examples are:

The Commonwealth Scientific and Industrial Research Organisation (CSIRO) has made and deployed sensors to gather information from within an oyster, measuring the oyster's heartbeat to determine their state of health and growth performance within their environment. Sensors have been deployed on bees to measure swarm behaviours, Electrical current sensors have been used to remotely monitor and control electricity flowing into individual household electrical circuits. Digital sensors have been deployed

to monitor social media and analysed to show real time sentiment and wellness characteristics. Sensors have been used to monitor the activity and wellbeing of some elderly people who are monitored and supported by carers while continuing to live independently in the family home but with added security and protection.

While examples and trials are evident in almost all market sectors, of which a few are represented here, it seems evident that some sectors are more advanced in IoT development than others. Important indicators to which market sectors are likely to more advance in the use of IoT are:

- The level of sophistication and fit of existing communications infrastructure
- The level and access (availability) of existing data sources which can already be better mined and analysed (e.g. in retail or finance)
- The level of sectoral collaboration (e.g. in the automotive industry in the US)
- The level of Government leadership and support (e.g. Singapore smart city)

The table below from IoT Analytics shows a useful market sector segmentation than can be used to identify IoT opportunity segments.

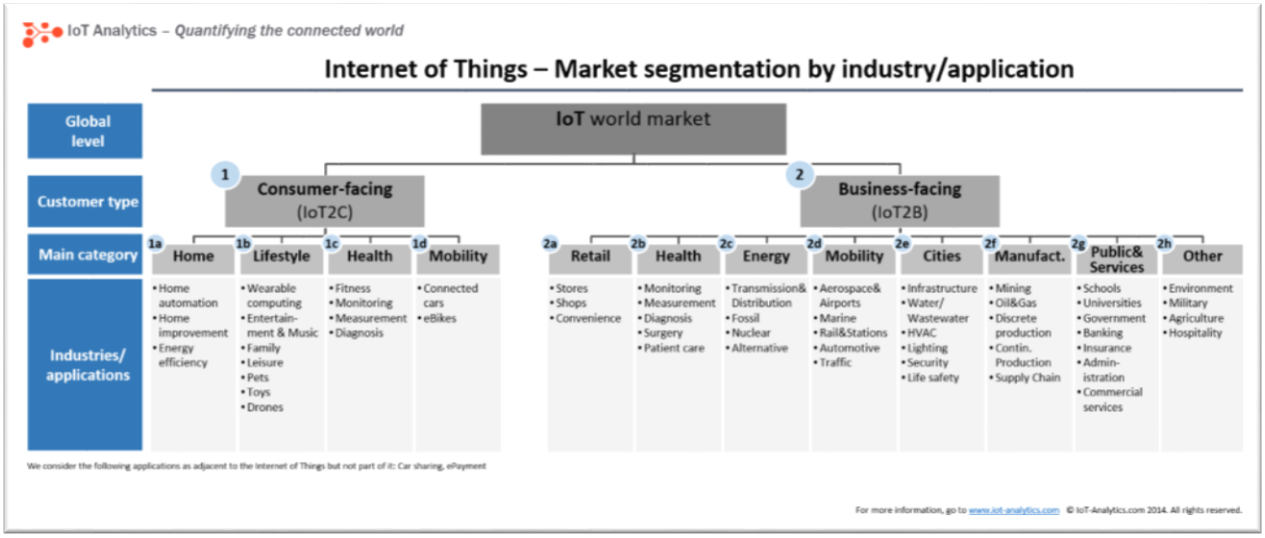


Figure 10: IoT impacts every segment

The leading countries are focussing on areas that make sense with respect to their existing strengths and aspirations. Germany and the US, for example, are leveraging their manufacturing strength to focus on the industrial and manufacturing dimensions of IoT. Germany is rallying around the Government's 'Industrie 4.0' initiative. South Korea and the US are targeting the automotive and transport sectors while Singapore, China and India see smart cities as a Government-led focus.

Observation 3: IoT innovation and deployment is more mature in some sectors than others. Those that are more advanced are characterised by strong collaboration within the sector in specific countries.

The UK Ofcom report of January 2015 predicts the growth in IoT will be driven by utilities, concluding that "Intelligent building and automation applications will also dominate the IoT market in 2022." However, the study also predicted significant growth over the coming ten years for categories of consumer electronics, utilities, healthcare and smart cities.

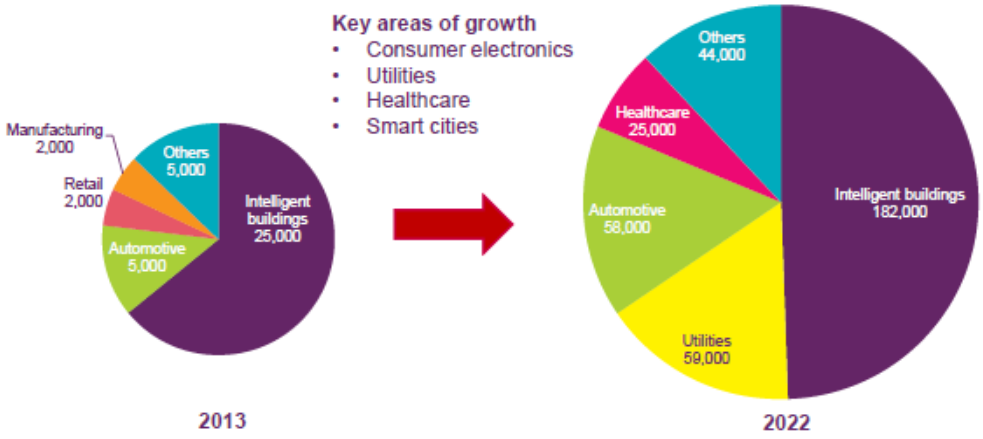


Figure 11: Ofcom IoT growth predictions

We have listed a few indicative examples of early IoT implementations across a range of market sectors.

The consumer home market – Already in today's market, consumers are connecting a wide range or devices to their home networks. This is extending well beyond the home computer, tablets and smart phones that are typically all connected using wifi or Ethernet. The home automation field is full of new remote monitoring and controlling sensors and actuators and increasingly hi-fi equipment, home theatre, white goods and appliances have network connectivity and sensors with internet access for remote control and monitoring. This trend is growing fast and in many ways today's consumer is more and more challenged to cope with achieving the value that all these solutions offer.

Google have recently launched their OnHub product described in Section 4.3.3 that, along with other Google initiatives, offers consumers a much better experience. Telcos are targeting this market but do not yet have the model right to attract broad consumer acceptance.

This raises the question of market structure. Is there an opportunity for a new player or players in the market to provide some form of aggregated home services management, by offering the consumer a service to resolve service problems or failures of any device connected in the home? How would these aggregators take ownership of risk when so many players may be providing fragments of an overall solution? These solutions will include local area networking, broadband connectivity, routing, wireless access points, sensors, actuators, smartphones, appliances, white goods, computers, software applications, data sharing, privacy etc. Some telcos think this is an opportunity for them and, indeed, this may be so, but the service layers above the basic network connectivity will be a challenge and the potential to understand many different vertical service models an even bigger challenge.

Observation 4: Innovation in the consumer IoT market is evident today with the growth of new home automation services. These are introducing a multi-dimensional, fragmented and complex service model for consumers.

Smart cities – There are developing smart city programs in place in Singapore, China and India today.

Smart Cities San Diego is a bold, multi-year collaboration combining the resources of the City of San Diego, San Diego Gas & Electric, GE, UC San Diego, and Cleantech San

Diego. Together, these leading organisations from Government, business, education, and non-profit are partnering to drive existing energy programs forward, identify new opportunities, embrace additional collaborators, and make the San Diego region a leader the smart cities movement.

Ericsson's Networked Society City Index provides an inspiring contribution to urban development around the world. The 2014 index examines and ranks 40 world cities, providing a framework for measuring ICT maturity in relation to social, economic and environmental progress. The City Index report and interactive tool is available at http://www.ericsson.com/thinkingahead/networked_society/city-life. Despite Sydney ranking 19 out of 40 indexed cities, there is no identifiable IoT program or smart city activity in action.

Agriculture – Monsanto, a global player, believes that the IoT potentially offers a leap forward in transforming agricultural efficiency and value through technology. Today these solutions are somewhat closed within the providers' analytics domain, with strong competition to lock into a single end-to-end solution provider. This will not be the model in the longer term. Open data and a competitive solutions market will prevail. Data will be shared across agricultural and meteorological domains and combined with transport data and retail market data etc. and this will be enabled through open data frameworks, not proprietary solutions.

"We expect the precision agriculture space to continue to group quickly as data becomes cheaper to store and easier to move from platform to platform. We are just beginning to explore all the value we can create for farmers with these tools." (Brett Begemann, Monsanto)

Field-based environmental sensors already measure soil. This data is already being combined with Bureau of Meteorology data and used by large farming operations to determine how much water to apply to crops and when to apply it. Sensors too are collecting data on temperature, light, soil acidity and fertiliser content. Animal tracking allows livestock to be monitored for disease and accidents as well as providing opportunities for better husbandry.

As with many other sectors, the IoT brings benefits in aggregate as well as to individuals. 'Smart farms' will share data with other farms, different parts of the supply chain, regulators and consumers. Maximising yield to sustain food production is a critical need now and in the future. And better managing the end-to-end food supply chain from farm to fridge will improve quality and value of the agricultural produce.

Early evidence suggests that controlled traffic farming – where machinery drives along repeatable tracks with greater accuracy – could reduce machinery and input costs by as much as 75%. Smallholdings contribute 70% of global food production. However, they have not been the target market for this level of precision agriculture to date. IoT will enable this market.

Sensors and analytics throughout the agriculture supply chain will yield higher quality crops and improved animal welfare, major productivity improvements and significant water utilisation improvement as well as reduced use of chemicals and improved environmental impact.

Smart parking – Siemens designed a solution that a modular, infrastructure-based sensor system that goes beyond the possibilities of ground sensors. The tool allows to form a clear picture of where available parking spaces can be found and how long each space has been occupied, while providing an overview of improper usage of any non-parking areas as well as nearby bicycle and emergency vehicle lanes. From routing and

enforcement applications to city dashboards, this detailed parking and violation information can then be accessed by various agencies and stakeholders, from commuters to designated law enforcement personnel. The solution does not only support parking services: from supporting traffic management to adaptive light management or retail-sponsored city services, multiple complementary applications can be linked on a single platform to make a city 'smart', innovative and easy to navigate.

Fleet management – Using five customer service vehicles (CSV) in New Zealand, Chorus (the NZ equivalent of Australia's NBN) leveraged an Alcatel-Lucent solution concept with several partners for a New Zealand market trial of an integrated platform intended to accelerate the installation of gigabit broadband nation-wide by increasing efficiencies and reducing costs. The CSVs minimized long trips to the warehouse, allowed for in-transit asset transfers and simplified work order processing. The two-month trial produced significant results, including time and cost savings in the areas of inventory management, installation, service provisioning, customer notification, tool and inventory tracking and electronically automated forms. These results can apply to any field service operation, not just that of a network provider. This IoT and network connected solution concept dramatically improves field service operations.

Medical instruments – Sensors are at the heart of almost every medical instrument, for example in equipment used in computerised axial tomography (CAT) scans, X-rays, retina scanning, ultra-scanning, magnetic resonance imaging (MRI) scans, even blood pressure, glucose level and temperature measurements. All medical instrument vendors are embracing IoT to add additional capability to their instruments and through the emergence of digital secure medical records, data archiving and sharing we will see massive changes in health care solutions and outcomes. Remote instruments can deliver scans and images to specialists anywhere. Aged care, tele-health and the entire preventative and treatment sectors are being transformed with IoT.

Mining – Modern mining practices are dependent on sensors for monitoring and measuring remote-controlled vehicles and equipment. The larger Australian mining operators including BHP, Rio Tinto, Woodside and others are very successfully deploying advanced networks to underpin advanced robotics and autonomous operations to dramatically lower the operational cost structure of the mining sector. It is worth observing that these complex solutions seem to emerge very well when a single player is in control of the entire eco-system, such as a remote mining infrastructure and the connecting transport infrastructure.

Supply chain- with radio-frequency identification (RFID) tags we are seeing sensors deployed on most goods as they are transported across the world, allowing us to accurately track progress end-to-end. Increasingly, these RFID tags are used to track lower and lower cost items as the tags themselves reduce in cost to a completely disposable item.

We see strong evidence that countries and major companies are focussing their early IoT efforts on specific market sectors. IoT is such a broad subject that spreading too thin is a real risk. Intel, for example, appear to be targeting smart building solutions, smart cities and transport. Cisco's focus appears to be different in different markets: manufacturing and transport in Europe, Government, utilities, and retail in the US, while in Australia they are focussing on mining and astronomy. Ericsson is focussed in Australia towards energy and transport while globally pushing harder into smart cities.

Observation 5: Long-term cross-sectoral opportunities are huge but initial success seems sector-focused overseas, due to a focus on common and achievable goals, trust, more easily identified mutual interest and fewer governance barriers.

2.5 A Model for Identifying IoT Opportunity and Challenge

In order to deal with the many elements that form IoT solutions, we have created a very simple general reference model:

Figure 12: IoT reference model

Figure 12 represents on overarching view of the IoT general architecture. From the outset it is important to illustrate that there is much more to this architecture than a technical model. The central section of this figure represents the technical framework but this must fit into the context of services models, the market segments as well as the affected users.

The following figure shows many of the main aspects across the IoT reference model that should be considered in the framework of a national IoT strategy.

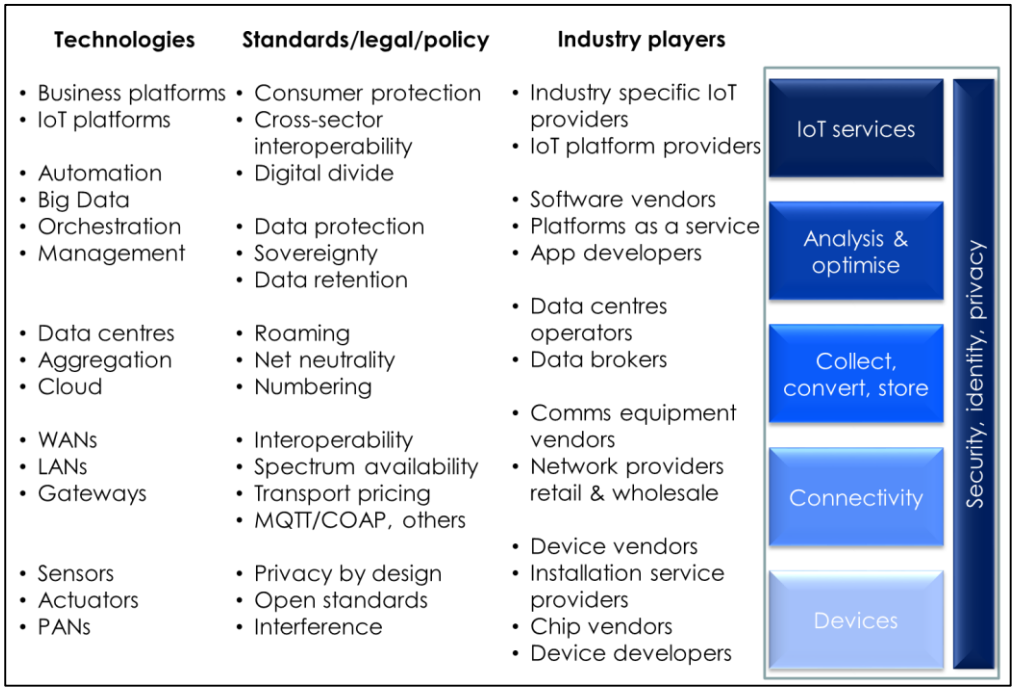


Figure 13: IoT considered dimensions

Devices or 'sensors and actuators' interface to the real world. Sensors convert physical characteristics such as temperature, humidity, motion, fire, location etc. into a digital form for other layers of the architecture to interpret and analyse. Actuators take action as a result of analytic outcomes and/or human interaction to switch on a pump, switch an electrical circuit, operate a hydraulic valve etc. Therefore, these devices must be connected regardless of where they are – in remote locations, in the home, in vehicles, in machines and appliances or even on farm animals and crops or in the ground or increasingly attached to people in the form of mobile smart phones and smart watches. This is far from an exhaustive list but it already serves to illustrate the challenge of the next layer. That of connectivity and communications. In fact the communications challenges exist throughout the IoT architecture and must be considered carefully at every point.

Device management, identity management and security are aspects that must be considered as the digital data is created, aggregated, stored and analysed. Understanding the context of sensor data is vital and so is protecting it from both a commercial and privacy perspective. The security and accuracy of data must be managed and protected while being available appropriately for use in many different use cases as business opportunities. How data is protected and shared is critical for a thriving eco-system.

Event processing and analytics contains much of the computing algorithms and intelligence that adds value and industry/sector context to the collected data.

The ability to create easy access to data and analytics is a key to the potential success of the IoT eco-system. Open application programming interfaces (APIs) are needed to enable application developers to easily create new innovative applications without having to spend time handling the underlying complex data sets. The quality of the APIs developed to support this model are fundamental to the success of the eco-system. The quality and administration/support of open APIs will play an important role in enabling a wholesale service model for retail service developers to build upon.

In summary, every element of the technical architecture plays a critical role in the end-to-end eco-system that underpins the IoT opportunity. These technical capabilities then drive opportunity into the end-user market through targeted industry/sector specific applications and business models. Throughout this document we will refer to all these architecture building blocks and use the names and definitions to establish a consistent language to address the issues when considering what is needed for a successful IoT eco-system that generates opportunities for Australian business.

3 THE GLOBAL CONTEXT

IDC predicts IoT will increasingly become a global phenomenon, led very visibly by countries in the G20. The opportunity calls for players in the IoT eco-system to first and foremost innovate and implement solutions that yield operational efficiencies in the top-tier countries. IDC's G20 ranking through the lens of the IoT puts forth the United States and South Korea as the number 1 and number 2 most-prepared countries for IoT, respectively. Japan, Britain and China ranked third, fourth, and fifth, respectively.

Some brief information on where the more evident IoT activity is at the national and regional level is given below:

3.1 European Commission

For the past six years, the Commission has cooperated actively with member states and third countries towards the development and future deployment of the IoT technology.

In March 2015 the European Commission initiated the creation of the Alliance for internet of Things Innovation (AIOTI). This alliance flags the intention of the European Commission to work closely with all stakeholders and actors of the IoT.

The Digital Single Market (DSM, http://ec.europa.eu/priorities/digital-single-market/), adopted in May 2015, leads Europe a step further in accelerating developments on IoT. The DSM consolidates initiatives on security and data protection, which are essential for the adoption of this technology. Most importantly, it announced an initiative on the data economy (free flow of data, allocation of liability, ownership, interoperability, usability and access) and promises to tackle interoperability and standardisation.

3.2 United Kingdom

The UK Government has acknowledged the role that the development of the IoT can play as part of its broader growth and innovation agenda. For example, in March 2014 the Prime Minister announced a significant increase in Government funding for IoT projects, citing their potential to underpin a new 'industrial revolution'. In addition, the Government continues to fund the targeted development of IoT technologies and pilot studies through 'InnovateUK3'.

The Prime Minister commissioned the Government Chief Scientific Adviser to review how the UK can exploit the potential of the IoT. "The internet of Things: making the most of the Second Digital Revolution" was published in December 2014. It includes nine recommendations for Government policy to better enable IoT for the betterment of the UK economy and competitiveness.

Ofcom, the UK communications regulator, released its report: "Promoting investment and innovation in the internet of Things: Summary of responses and next steps" in January 2015. Ofcom has identified several priority areas to help support the growth of the IoT. Following feedback from stakeholders in 2014, these areas include spectrum availability, data privacy, network security and resilience, and network addresses.

The UK Government has also earmarked £73m for IoT projects in 2015. Initiatives include "Hypercat", a streamlined IoT interoperability profile driven by the UK Technology Strategy Board.

3.3 Germany

'Industrie 4.0' is the German vision for the future of manufacturing; a vision where smart factories use information and communications technologies to digitise their processes and reap huge benefits in the form of improved quality, lower costs, and increased efficiency.

'Industrie 4.0' is a favourite theme for Chancellor Angela Merkel who brings it up in almost every speech about business or the economy. Most recently, she urged all of Europe to embrace 'Industrie 4.0' when addressing the World Economic Forum in Davos in January 2015.

Germany's 'Industrie 4.0' strategic initiative, in its High-Tech Strategy 2020 Action Plan, establishes the framework to enable the country to take a leadership role in the manufacturing engineering sector, including in IoT.

3.4 Singapore

The IDA Smart Nation Platform (SNP) is a key infrastructure initiative to support Singapore's vision to be a smart nation. SNP is aimed at bringing together a nationwide sensor network and data analytics abilities, providing better situational awareness through data collection, and efficient sharing of sensor data.

The IDA initiative was launched in October 2014 with its first report published in April 2015. The recommendations provide technical and policy direction in the development of the Singapore smart nation (smart city) infrastructure.

3.5 China

In late 2009, then Chinese Premier, Wen Jiabao, identified IoT as an "emerging strategic industry" in an interview on state media. Beijing has focused on developing technology by which devices can communicate via infrared sensor, RFID and other M2M technology.

China's Ministry of Industry and Information Technology released its 12th Five-Year Development Plan in 2012, with the goal of scaling the IoT market to RMB1,000 billion ($163 billion) by 2020. The midterm Information and Communications Technology Development Report of the 18th Central Committee of the Communist Party of China (CPC) Congress significantly expanded the focus on new sectors such as cloud computing and the IoT. Specifically, the Circular 181 and Circular 42 provide preferential tax policies for the software and integrated circuits industries, including interpretation to include IoT manufacturers. The Government and private sectors have been tasked with setting communication and security standards, demonstrating practical applications, nurturing new businesses, and planning the regional distribution of the IoT industry. In addition, the IoT Special Fund promotes IoT research and development, applications and services. Grants are offered to self-funded projects, and loan subsidies support enterprises with bank-loan funding.

One of the first applications in which the Government is looking to the IoT for help is to deal with food safety issues and healthcare in remote areas. The Government has established state-owned enterprise zones such as the Chengdu IoT Technology Institute in Sichuan province, which is developing a health care system in which rural villagers can step into a telephone booth-sized 'health capsule' to get a diagnosis and prescription from a doctor in a distant hospital.

According to a report released by Groupe Special Mobile Association (GSMA) over the summer of 2015 "In China, the IoT is benefiting from both Government support and productive partnerships between companies from different sectors. … As it has done in other it sectors, China's central Government is leading the development of standards, supporting the establishment of an IoT standards association and promoting Chinese-developed standards internationally. The central Government also selected 202 cities in 2014 to pilot smart city projects. … The Government is mandating the use of smart meters to improve energy efficiency in homes."

3.6 South Korea

The South Korean Government has set aside KRW50 billion (US$48.87m) over the next five years, from 2015, to seek out new revenue opportunities from the IoT market.

The country's Ministry of Science, ICT and Future Planning and Ministry of Trade, Industry and Energy will invest KRW37 billion from 2015 in the development of core technologies in IoT, reported Yonhap News Agency. The investment will also look at the development of micro-electromechanical system (MEMS) sensor chips as well as broadband sensing devices.

Another KRW12.3 billion will come from Korea's private sector, giving an overall investment of KRW50 billion. The Government also has plans to groom specialists in IoT technologies.

The South Korean Government in May 2014 came up with a master plan for developing IoT services and products through setting up an open IoT eco-system consisting of service, platform, network, device, and IT security sectors. South Korea aims to increase its domestic market for the IoT from KRW2.3 trillion in 2013 to KRW30 trillion ($28.9 billion) by 2020.The plan aims to increase the domestic IoT market fourteen-fold over the seven years to 2020, with a 30%increase in productivity and efficiency in user companies.

The Government also has plans to increase the technical labour pool in IoT technologies.

3.7 USA

In early 2014, the Federal Communications Commission's (FCC) Technology Advisory Council created an IoT working group to look at the future of the IoT. In June 2014, a group of senators wrote a letter to the Government Accountability Office (GAO) asking them to conduct research on IoT including strategies that Government agencies might be able to use in the future of IoT; any regulation currently in place; spectrum viability; and whether the Government has any experience with the technology. They also asked for implementation of a set standards for Government agencies, as well as uniform equipment across the country.

"Given the growth in IoT as well as the way new technologies are being embedded in millions of everyday products, a more robust analysis of the challenges and opportunities associated with the IoT is needed," the lawmakers wrote in the letter.

The United States Senate also passed an IoT resolution in March 2015 to create a national strategy on the best ways to implement the IoT in the US.

In the US significant industry investment into the IoT is a major driver. For example:

- IBM announced on 31 March 2015 that it will invest $3 billion over four years to establish a new IoT unit, and that it is building a cloud-based open platform designed to help clients and eco-system partners build IoT solutions.

- Google, Apple and Microsoft have launched IoT consumer lifestyle and health platforms.
- The agricultural sector with companies such as Monsanto and farmers are developing IoT data sharing protocols and IoT solutions.
- The automotive industry through the major manufactures are driving IoT intelligent transport solutions
- Major US IoT industry bodies promoting IoT in various sectors are highly active. These include:
    - Industrial internet Consortium (IIC)
    - Open Interconnect Consortium

3.8 Netherlands

In July 2015, an entrepreneur announced that Amsterdam was to become a 'connected city,' with the launch of a new IoT wireless network that will allow objects to transmit data between each other. The 'Things Network' is a first-of-its-kind system that uses low-power, low-bandwidth LoRa Wider Area Network (WAN) technology to cover the city with a wireless signal that allows objects like boats, trash cans and street lights to become tools for developers. Unlike other smart city projects, this one is entirely crowd-sourced by citizens and was put together in just six weeks.

A pilot project to demonstrate the 'Things Network's' potential will see boat owners in the city (there are many, thanks to its network of canals) able to place a small bowl in the base of their vessel. If the boat develops a leak and starts taking on water, the bowl will use the network to send an SMS alert to a boat maintenance company that will come and fix the problem.

The 'Things Network' concept was put together in just six weeks, starting with a LoRaWAN gateway device and the knowledge that with ten such devices the whole of Amsterdam could be covered. The idea was pitched at an IoT meet-up in the city and received a positive response.

The initiative has now created a community-owned data network that developers can build on top of without any proprietary restrictions. Companies including The Next Web and accountancy giant KPMG have agreed to host gateway devices at their premises, and the City of Amsterdam local authority is enthusiastic about the idea.

The City of Amsterdam's Chief Technology Officer (CTO), says the network's strength is its crowd sourced nature. "Amsterdammers invest in it themselves and the community is the owner of the network. I do not think this has happened before and it is interesting to see how traditional telcos will cope with this disruptive new idea of building networks."

The 'Things Network' may also be used for bike location systems, security installations and beyond, and the port of Amsterdam is also interested in using the network. The following figure shows the network nodes and their hosts highlighting that with a small number of LoRaWAN nodes, most of the city can be covered for sensor connectivity.

Figure 14: The Amsterdam 'Things Network'

3.9 India

The Department of Electronics and Information Technology, (DeiTY) has issued a draft IoT policy document which focuses on the following objectives:

- To create an IoT industry in India of US$15 billion by 2020. It has been assumed that India would have a share of 5-6% of the global IoT industry.
- To undertake capacity development (human and technology) for IoT specific skill-sets for domestic and international markets.
- To undertake research and development for all the assisting technologies.
- To develop IoT products specific to Indian needs in all possible domains.

The policy framework of the IoT policy has been proposed to be implemented via a multi-pillar approach. The approach comprises of five vertical pillars (Demonstration Centres, Capacity Building & Incubation, R&D and Innovation, Incentives and Engagements, Human Resource Development) and 2 horizontal supports (Standards & Governance Structure).

In July 2014, the Indian Prime Minister announced plans and funding (£710m) for development of 100 smart cities, to revolutionise urban living and city efficiency in India.

3.10 Spain

Telefonica sows the seeds for agro-technology growth. According to Telefonica, investment in technology for agriculture is expected to reach $4.3 billion in the US alone this year, making it the sector with the greatest investment ahead of technology applied to the financial and medical sectors.

The telco has just announced that Brazilian agro-technology firm SAA is one of the first two companies (the other being Chinese online games developer Xcloud Game) to benefit from the partnership between China Unicom, Tsinghua Holdings Technology and Innovation, and Telefonica Open Future. The partnership is designed to promote mutually beneficial entrepreneurial initiatives within their respective accelerators, and has seen SAA entering the Chinese market, with Xcloud Game expanding into Brazil.

SAA has evolved to become the first online market to connect agricultural technology companies around the world with distributors from emerging markets such as China and Brazil. The next step for SAA is to move into Binggo, the acceleration space co-sponsored by Telefonica Open Future and China Unicom, which it will use as its base for the launch of its 'Smart Ag' platform.

VisualNACert is another start-up working in the agro-technology, having developed a tool for managing information and making decisions in farming ventures. Clicking on a map interface maximises the efficiency of planting through geo-positioning and visualisation of plots and applying criteria such as quality, health, sowing periods and productivity. The company was an investee of Telefonica's 'Wayra' programme last year and is on track to report revenues of €1m this year with operations in Spain, Australia, the US and Latin America.

Telefonica Open Future is a global, open program designed to connect entrepreneurs, start-ups, investors and public and private organisations from around the world. The program already has investments in over 550 start-ups worldwide, has invested €647m with a further €733m pledged.

3.10.1 Growth in Spain's Agro-Technology

A report from the CleanTech Group at the end of last year revealed that equity investment in agriculture and food technology reached $269m across 41 deals in the third quarter of 2014, an increase of 48% year-on-year (14Q3 was the most recent report available) in terms of value. In November 2014, Eric Schmidt's Innovation Endeavours and Flextronics Lab IX launched 'Farm2050', a collective to support agro-technology start-ups with a focus on solutions designed to boost global food production.

A report by Beecham Research released earlier this year suggested that IoT could be the key to the farming industry meeting the challenge of increasing food production by 70% to feed the 9.6 billion global population expected by 2050.

"In Europe, the move towards smart farming is being encouraged through various projects and programmes funded by public and private money," said Saverio Romeo, principal analyst at Beecham Research. "While the M2M agricultural sector is still emerging, M2M and IoT technologies will be key enablers for transforming the agricultural sector and creating the smart farming vision."

Romeo says the US market is leading the way in smart farming, particularly in areas such as arable farming. Europe, meanwhile, is increasingly looking into small-sized field farming, precision livestock farming and smart fish farming; and this trend will soon expand into other important agricultural economies.

"In terms of time scale, the next two years will be exploratory for smart farming, but the pace of change will intensify from 2017 to 2020," said Romero. "While the M2M/IoT industries will not see the light from the agricultural sector immediately, they need to be prepared, because it will be soon strong and bright."

3.11 Ranking Country IoT Capability

Once the technologies behind the Industrial internet of Things combine with a number of broader social, economic and political enabling factors, countries can make the most of their productive and innovative potential.

Accenture terms these enabling factors that explain the extent to which countries have woven the IoT into their economic fabric as a country's 'national absorptive capacity'

(NAC). Their ranking of major economies on this metric is intended to spur policy makers into action. This NAC is based on four pillars:

Business commons

- Communications infrastructure
- Human capital
- Quality of governance and institutions
- Access to capital
- Economic openness

Take-off factors

- Government support and spending on research and development
- STEM talent
- Quality of scientific research institutions
- Standards setting
- Urbanization
- Expanding middle class

Transfer factors

- Formal and informal knowledge transfers
- Organisations' ability to embrace new technologies within organisations
- Consumer willingness to adopt new technologies
- Data privacy and security concerns

Innovation dynamo

- Entrepreneurial culture
- 'Maker-ism' movement
- University-industry collaboration in research and development
- Development of technology clusters
- Organisations' focus on customer needs

Below is a table comparing NAC scores between countries. The results indicate a country with a NAC score of 100 would be the top performer on each of the 55 indicators compared to the other study countries. Overall, the results show that no one country has achieved this level of NAC. In other words, every country has work to do.

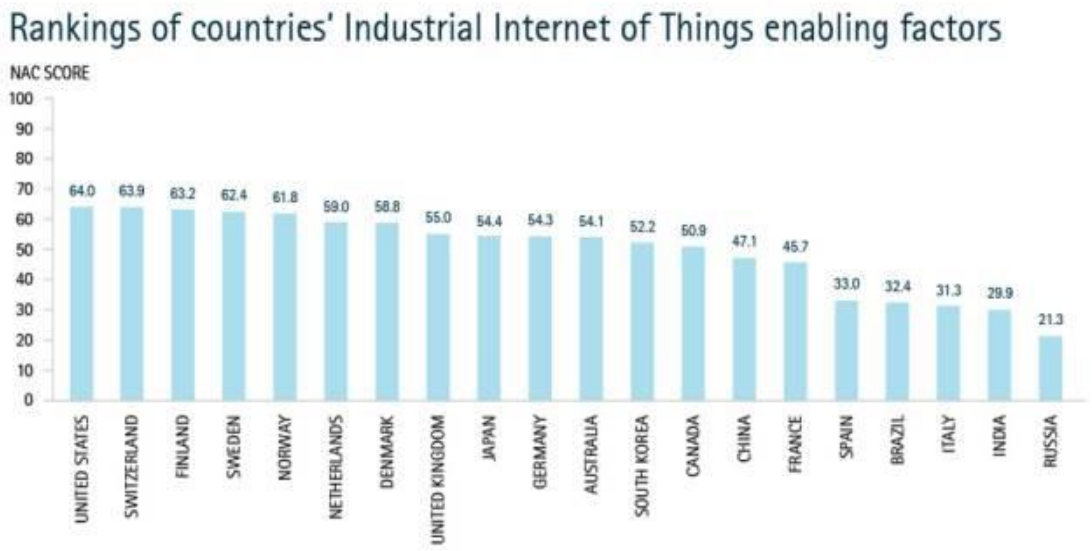


Figure 15: IoT country rankings

Observation 6: Australia's peer countries and customers are further advanced in articulating and encouraging IoT industry benefits.

Observation 7: A key factor in IoT success and leadership is collaboration at many levels. Collaboration is required between Government, industry, research and education, within and between industry sectors, between 'eco-system' partners.

4 ENABLING TECHNOLOGIES AND THE CONFUSION OF CHOICE

IoT involves all 'layers' of ICT technologies from devices to service presentation, and everything in between. Our model introduced in Section 2.5 illustrates this and the following figure overlays the opportunity for vendors and service providers at all layers, but also introduces complexity around open data sharing and standards.

Understanding and navigating through the complexity of technology choice, and leveraging of interoperable technology "eco-systems" will be crucial in IoT success. It will help to avoid technology "dead-ends", vendor lock-in, and help achieve competitive advantage. The technologies are highlighted in the following figure.

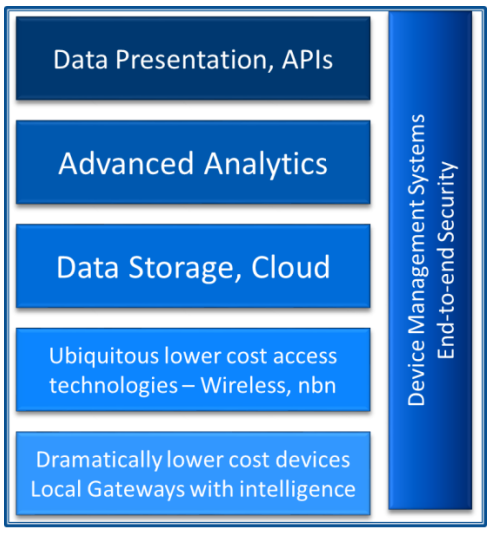


Figure 16: IoT technology enablers

4.1 IoT Open Systems and Interoperability

Open architectures, protocols, data standards and interoperability are all key to the future success of IoT. The Open Interconnection Consortium (OIC) was established to address these issues and Appendix D below describes this and other standards bodies all working to achieve interoperability in one form or another. The OIC said it well when it explained:

"We want to connect the next 25 billion devices for the internet of Things. We want to provide secure and reliable device discovery and connectivity across multiple OSs and platforms. There are multiple proposals and forums driving different approaches... but no single solution addresses the majority of key requirements. We need industry consolidation around a common, interoperable approach. We need a broad industry consortium of companies to create a scalable solution.

We are defining the specification, certification& branding to deliver reliable interoperability -- a connectivity framework that abstracts complexity. This standard will be an open specification that anyone can implement and is easy for developers to use.

It will include IP protection & branding for certified devices (via compliance testing) and service-level interoperability. There will also be an Open Source implementation of the standard. This Open Source implementation will be designed to enable application developers and device manufacturers to deliver interoperable products across Android, iOS, Windows, Linux, Tizen, and more.

Consumers, Enterprise, Industrial, Automotive, Health, etc. who want smart devices to easily interconnect and communicate with appliances, embedded devices, etc. all need this. Developers of operating systems, platforms, and applications who want their products to interoperate seamlessly across many brands and eco-systems. End users who want consistent levels of security and identity across smart devices down to the smallest connected appliance.

Our goal is to define a comprehensive communications framework to enable emerging applications in all key vertical markets. The framework must enable multiple new modes of communication, such as Peer-to-Peer, Mesh & Bridging, Reporting & Control, etc.

The framework should include a consistent implementation of identity, authentication and security across the modes of User ID, Enterprise / Industrial ID & Credentials. It should include a sense of proximity for the internet of Things and Wearable devices and include support for On-boarding and Provisioning. And the framework must support a "building block" architecture and provide an Open Source implementation."

Observation 8: Interoperability is a key enabler for IoT systems, for which open systems are essential.

4.2 Many Open Architectures and Standards for IoT

There is a host of standards and industry bodies working on frameworks for IoT at the global, regional, national and even sectoral levels. These frameworks further incorporate many more standards at each layer of their frameworks. Anecdotally, and frequently mentioned in news articles and company pronouncements, the plethora of frameworks is to some extent causing confusion across the industry sectors.

As IoT is relatively new, the competitive market has not yet resolved which frameworks will persist and which will be successfully commercially adopted.

A sample of some of the more high profile standards and industry bodies with IoT frameworks is listed below, and described in further detail, in Appendix D.

- International Telecommunication Union (ITU)
- Open Interconnect Consortium (OIC)
- Allseen Alliance
- European Telecommunications Standards Institute (ETSI)
- Industrial Interconnect Consortium
- OneM2M
- ISO/IEC JTC1 – IT (International Organization for Standardization, ISO; International Electrotechnical Commission, IEC)
- IEEE P243 (Institute of Electrical and Electronics Engineers, IEEE)
- World IoT Forum

Within each framework are choices of standards and profiles for interconnection. While many of these are common across the various frameworks above, design, commercial and partnering considerations will influence choices.

Observation 9: There are many open architectures with corresponding standards choices – each fit for certain purposes. Choosing the right one will be important depending on each industry, application or service level.

The figure below extracted from an ITU paper dealing with IoT serves to illustrate that a healthy range of business models can co-exist across the IoT architecture and this is underpinned by standards and sharing frameworks at every level. The figure shows three different cases that result in three different commercial boundary cases. Operators choosing to provide a part of a solution can do so because there would be agreed boundaries enabling a straight forward technical and commercial hand-over for other partnering providers. There are many other possible combinations that lead to different business models and openness, and standards must support them all.

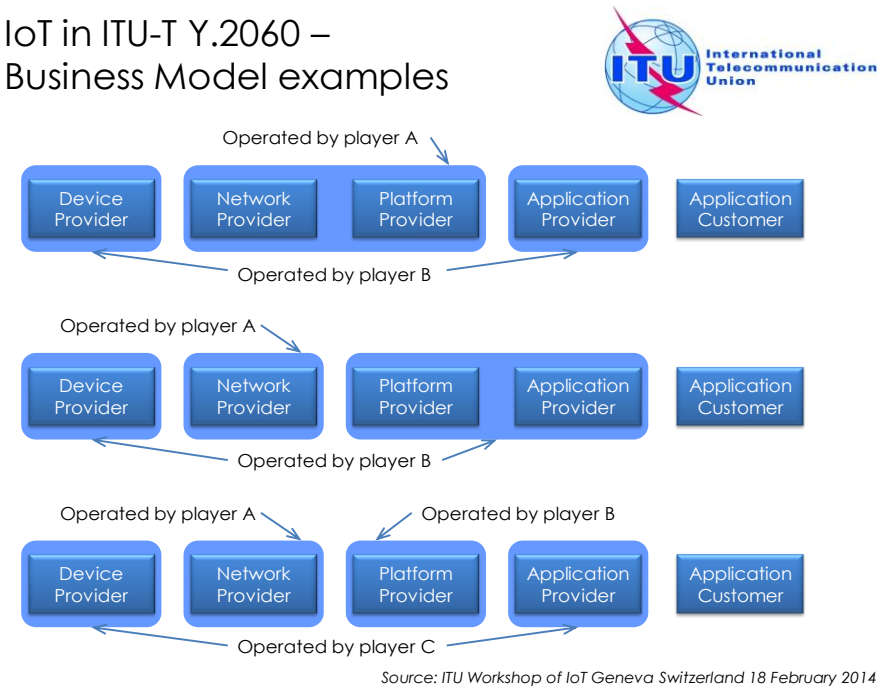


Figure 17: IoT business model examples from ITU

This figure shows that at each provider layer there is the potential for a technical and commercial boundary depending on the business model. Of course, at the device layer, network layer and platform layer there is a need for telecommunications standards, and at the device to network point there are already well over 100 different standards supporting just as many protocols. The need for standards at this layer is rich with choices and considering the creation of another standard would serve no purpose. From this wide range of existing choices, there is, however, a need to understand which standards are best suited to specific situations.

Refer to Appendix F for furhter information on standards.

Observation 10: Australia should not try to establish new IoT standards. There are already more than the average engineer can cope with and enough to serve our needs well.

4.3 Low-Cost Devices – Device Technologies, Local Area Networks (LAN), Personal Area Networks (PAN)

The figure below illustrates the sensor price versus expected volumes of the IoT device market and also the indicative standards that may typically apply. It is this wide range of sensors and applications and scenarios that make market size predictions so difficult to narrow down.

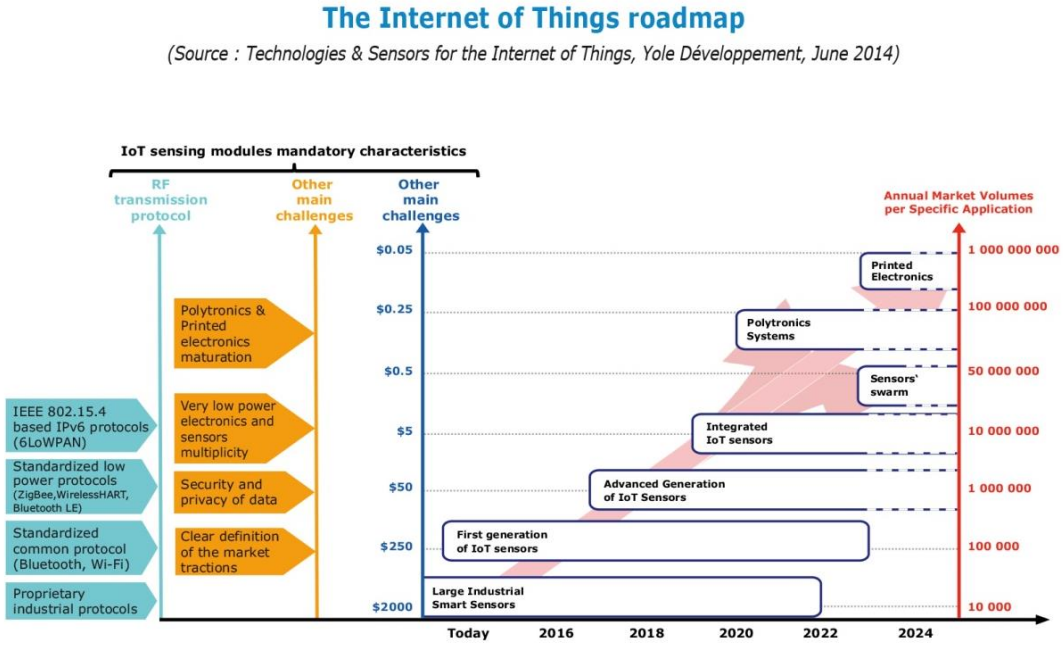


Figure 18: Yole development's view of IoT technology volumes

4.3.1 Which Technology, the Optimum Cost Model

M2M communication services refer to connectivity services that link IoT 'things' to central or back-end systems, without human input. Operational technology (OT) is enterprise technology used to monitor and/or control physical devices, assets and processes. Gartner's M2M and IoT context is captured in the following figure.

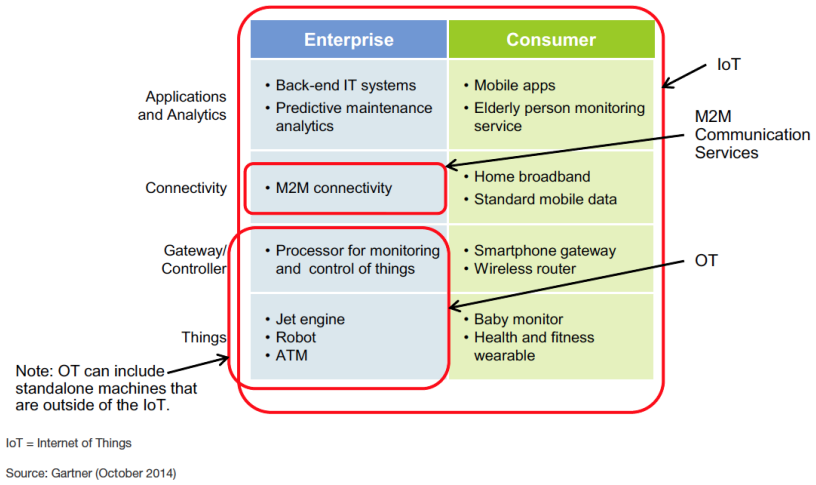


Figure 19: Gartner's M2M and IoT context

A 'thing' categorized within the 'low-end scenario' could, for example, generate $2 per month with a temperature sensor in a carton/container, generating $24 per year (e.g. tallying the goods moved from Asia to the US via boat freight). The 'high-end scenario' could generate $100 per month via, for example, a monitor in a critical care unit, generating $1,200 per year (e.g. providing prescriptive capabilities around sepsis – which is the most expensive condition treated in hospitals, accounting for over $20 billion in annual costs to the US healthcare system alone).

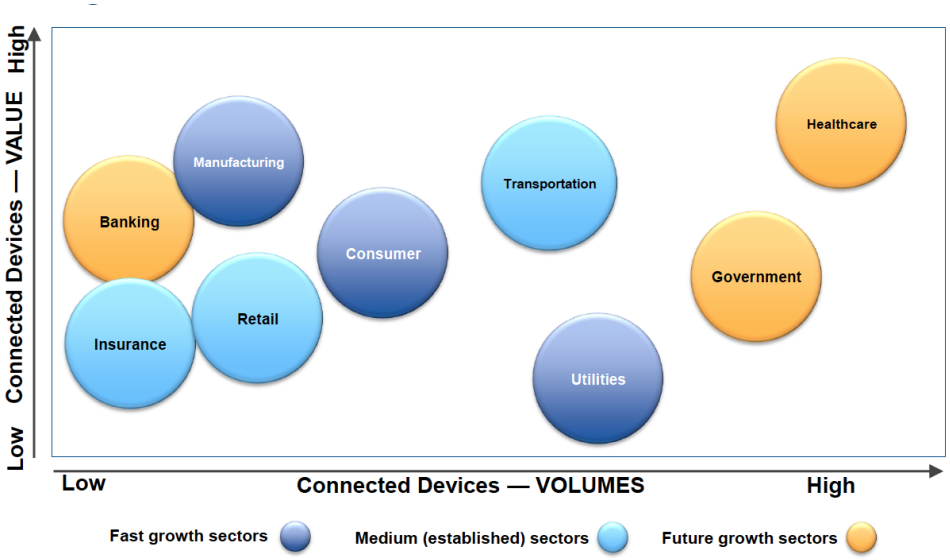


Figure 20: IDC's connected device value versus volume

At Directions 2014, IDC's Carrie MacGillivray, talked about which industries were leading the charge with IoT based on the value vs. volume of the devices in their connected device networks, illustrated in the above figure. Insurance, retail, and transportation are considered the established IoT sectors, while manufacturing, consumer, and utilities are the most promising in terms of growth.

Observation 11: IoT is very sensitive to connectivity costs and today tariffs are set from the perspective of a person accessing the internet – either fixed or mobile. New lower cost and lower tariff models will be required that support very low data volumes for a few cents per month.

The IoT relies upon connectivity between devices. The different types of connectivity can be described based on the geographic dispersion and geographic mobility they support. The higher the geographic dispersion and mobility the application demands, the greater the energy use needed to sustain the application, and the larger the antenna required (if the device is wireless). Energy use and antenna size, in turn, define the form factor (i.e. the size, configuration or physical arrangement of a computer hardware object) and device applications. The smallest sensors and actuators are those that either harvest electromagnetic energy through their wireless circuitry, such as RFID tags, or are connected with a wire to a power source and communications network. Developments in battery technology are, unfortunately, linear compared to the exponential advancements in integrated circuits, where increasingly smaller sizes and advances in capabilities are traded off against greater energy use. The following figure represents this comparison.

Geographically dispersed	**Application**: Smart grid, smart meter, smart city and remote monitoring **Technology required**: PSTN, broadband, 2G/3G/4G, power line communication	**Application**: Car automation, eHealth, logistics, personal devices **Technology required**: 2G/3G/4G, satellite
Geographically concentrated	**Application**: Smart home, factory automation, eHealth **Technology required**: Wireless personal area networks (WPAN), wired networks, indoor electrical wiring, Wi-Fi, RFID, Near Field Communication	**Application**: On-site logistics **Technology required**: Wi-Fi, WPAN
	Geographically Fixed	Geographically Mobile

Figure 21: M2M apps and technologies by dispersion and mobility

4.3.2 Gateway Architectures – Intelligence at the Edge

Gateway architectures or 'fog computing' or 'fog networking' is an architecture that uses one or a multitude of end-user clients or near-user edge devices such as residential gateway/modems to carry out a substantial amount of storage (rather than data being stored primarily in cloud data centres) and local communication (rather than always routed over the internet). Fog computing, a term coined by Professor Salvatore J. Stolfo, can be perceived both in large cloud systems and big data structures.

"Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives, dense geographical distribution and local resource pooling, latency reduction for quality of service (QoS) and edge analytics/stream mining, resulting in improved user-experience and better redundancy in case of failure.

In other words, the concept of fog computing has been introduced as a bridge between IoT devices in the field and remote data centres via gateways. IoT devices can produce huge data sets that need to be processed. With fog computing some of that processing load can be handled by computing resources at the edge – in the gateway, by filtering and summarising the data to reduce volume and increase value and relevance.

The success of fog computing hinges directly on the resilience of those smart gateways directing countless tasks on an internet teeming with IoT devices. IT resilience will be a necessity for the business continuity of IoT operations, with redundancy, security, monitoring of power and cooling and failover solutions in place to ensure maximum uptime."

Source: http://www.datacenterknowledge.com/archives/2015/04/08/fog-computing-for-internet-of-things-needs-smarter-gateways/

4.3.3 Google's OnHub

In August 2015 Google announced its new Wi-Fi router called OnHub, developed in partnership with manufacturer TP-Link. Following is some text extracted from Google's press release and resulting article https://www.linkedin.com/pulse/telcos-need-wake-up-take-long-hard-look-googles-home-iot-guy-daniels:

Key features announced include:

- Google OnHub supports IEEE 802.15.4 standards
- Future hub for Thread, ZigBee and Bluetooth 4.0
- The IoT platform for the home
- Full control via Smartphone app, and automatic software updates

Figure 22: Google's OnHub device

"Google's OnHub is a home IoT gateway. As well as a wifi router. It supports IEEE 802.11b/g/n at 2.4GHz and 802.11a/n/ac at 5GHz, and has some nifty congestion sensing radio and antenna technology to optimise the use of its 12 internal wifi antennas. That alone would be worthy of the price tag of US$199. But it also supports Bluetooth 4.0, IEEE 802.15.4 (as used by ZigBee and Google Thread) and Android Weave. These technologies are central to home IoT deployments.

So do we have a new answer to the question: "how will home IoT appliances and services be managed"? OnHub may be a leading contender for that role. It comes with 4GB of flash memory and a dual-core 1.4GHz processor, so it has plenty of processing power and capacity for future software enhancements. And it is fully controlled from a companion app on Android and iOS devices.

It is far too early to say Google has won this in-home IoT market, but with this launch it has stolen a march on the telcos and its direct competitors such as Apple.

Under this model, telcos would not be central to the emerging home IoT eco-system, and would again be forced to play the role of connectivity provider. Devices are going to be created by a multitude of companies, and they'll eventually be powered by one or two dedicated operating systems – of which Google's Brillo will almost certainly be one. They will communicate via a couple of dedicated protocols – Google's Thread amongst them, and also ZigBee and Bluetooth 4.0 – and don't forget the promise of Google Weave to tie this all together."

4.4 Short Range and Home Networks

Both wired and wireless networks are essential for the IoT. Wired networks provide capacity, but are inflexible in their location. Wireless networks allow for flexibility in location and motion, but are often limited by bandwidth and energy. Wired networks use standard networking technologies such as Ethernet (for in-company and fibre networks), gigabit passive optical network (GPON) (for fibre access networks), digital subscriber line (DSL) (for public copper networks) and Docsis (for cable Hybrid Fibre Coax networks). Although some standards exist for power-line communication, and power over Ethernet is

commonly used in businesses for Voice over IP (VoIP) phones and other equipment, there has been little development in wired protocols for the IoT. Existing standards are often applicable for situations where a wired connection can be used.

The least mature and, therefore, the most rapidly changing area is short-range wireless standards in the home and factory. Technologies such as RFID, near field communication (NFC), Zigbee, 6LowPan, Bluetooth and Wi-Fi, in order of complexity, have all been advanced as global standards, and each has its own niche. RFID technology is a one-way communication protocol that allows small chips (tags) to broadcast their location. In 2003, when Walmart announced that it would require its top suppliers to use RFID for all pallets and cases, it appeared that RFID was set for a big future in retailing. Many analysts predicted that every milk carton would soon carry an RFID tag and a refrigerator would be able to scan and provide an inventory of its contents. Some analysts predicted that within a decade100 billion tags would be used each year. This has not become a reality, in part because the price of tags has not decreased sufficiently, but also because radio frequencies do not easily penetrate packaging made from tin foil or products that consist (partially) of liquids. Therefore, RFIDs have found only limited use in high-volume, low-margin and fast-moving consumables.

By 2014, the RFID market had matured with RFID tags used increasingly in clothing and apparel stores. The benefit of RFID here lies in the ability to scan a stack of clothing and know whether particular sizes are still available or need to be replenished from storage. This reduces the time spent by customers waiting for employees to locate particular sizes in a stack. In addition, RFID is used in aerospace and manufacturing to track the location of parts and tools, and to ascertain whether the correct part has been used and its exact age.

In health care, RFID is used to track goods, medicine and patients as well as hand-washing hygiene by staff. The use of RFID-controlled soap dispensers has increased the use of soap in hospitals and decreased the amount of infections. In transport single-use or multiday tickets are embedded with RFID tags. RFIDs are also used in livestock identification to comply with Government requirements regarding the traceability of animals throughout their lives. One analyst company estimates that 5.8 billion tags were sold in 2013 and predicted a rise to 6.9 billion in 2014 (Das and Harrop, 2014).

NFC is a two-way technology developed for interaction, for example, when making payments or entering a facility. Operation requires two NFC-equipped devices to be in very close proximity to each other. NFC is integrated into swipe cards for building access and public transport (e.g. the Parisian Navigo, London's Oyster card and Japan's Suicacard). Its use is currently being expanded to contactless payments, with more and more banks introducing credit and debit cards with NFC. With the introduction of Apple's iPhone 6, all major smartphone platforms now support NFC. At the same time, some public transport cards, such as Seoul's T-card and Japan's Suicacard, can be used for payments of groceries, snacks, taxis and other purchases.

The main challenges of NFC concern standardisation. Most systems that use NFC are so-called closed-loop systems. This means that only cards issued by the organisation can be used for the types of transactions it authorises. This limits usage. For example, a public transport authority will only accept transport cards it has issued, but not cards from neighbouring regions or bank cards (the Parisian Navigo system cannot be used outside central France). An open-loop system allows customers to use cards issued by other organisations, such as other public transport authorities, banks and mobile phone vendors.

The main obstacle to standardisation is willingness among organisations to open access to what they see as their customers. It is difficult to introduce a system that works only when a customer uses bank Q, public transport organisation X and smartphone brand Y provided by mobile operator Z. Such an overlap covers only a small demographic. Many early NFC trials failed because they were limited to one bank and one mobile operator. Interest in open-loop systems is now increasing. Starting from September 2014, Transport for London began supporting payments through smartphones via 'Cash on Tap' from EE and Vodafone Smartpass. The use of a prepaid debit or credit card means that only the co-operation of the bank/credit card company is needed. The Transport for London system has proven popular with 5% of trips being paid through the open-loop card system within the first week of launch. One problem with open-loop systems, however, is the potential for 'card clash', which can occur when multiple cards may be used to perform actions such as transport payments. If a user's wallet touches a gate, the system may deduct payment from each card it detects.

Smartphones have also brought NFC technology to other applications. For example, pairing a smartphone with a wireless speaker can be achieved by tapping the phone on the speaker. This functionality is integrated into many Android phones and most Bluetooth wireless speakers and headphones, and is now expanding to keyboards, printers, televisions and other devices. It allows the user to pair devices without needing to know or understand the underlying wireless technologies (Wi-Fi/Bluetooth), and to establish authentication without knowing the keys for the devices. NFC stickers allow users to enable their phones to change configuration automatically when the sticker is tapped, for example, when the phone is docked in a vehicle.

Bluetooth was initially designed as a wireless personal area network (WPAN) to connect peripheral devices, such as headsets and keyboards, at short range to mobile phones and computers. Over 90% of phones, tablets and laptops have Bluetooth capabilities, and some vehicles. Compared to NFC it is a higher bandwidth, longer range technology, working up to10-20 metres in a star topology with a central controller where all devices connect to each other.

The latest version is Bluetooth 4.0; however ongoing development for Bluetooth 4.1 is expected to introduce mesh-networking and IPv6. This would allow devices to connect directly to each other and via IPv6 to the internet, instead of via a central controller. This would make Bluetooth a direct competitor to IEEE 802.15.4-based networks (discussed below). Bluetooth 4.0 has expanded its IoT capabilities through support for low-energy profiles. This has sparked innovation around a number of low-energy sensors and tags, such as Apple's iBeacon and competing standards. A number of uses have been identified in the home, including sensors that combine temperature, movement, position and other capabilities. These can be used to locate objects such as car keys, but also to signal whether a (liquor or gun) cupboard or window has been opened.

Bluetooth has also found uses outside the home, for example, in shops and malls. In the airports of Amsterdam and Miami, Bluetooth beacons guide smartphone owners to the correct gate via a dedicated app. SITA (an organisation specializing in IT and communications solutions for airports) maintains an open index which allows airports to register their beacons and app-makers to interact and develop services. In a few years it may be commonplace for airlines to use beacons to locate passengers and for travellers to find their plane using tags.

Beacons with relevant information can be placed at any location, such as a bus stop, and accessed via a smartphone. On a similar note, Microsoft has designed a headset that conveys information vocally for use by the visually impaired among other users. IEEE 802.15.4 (Low Rate Wireless Personal Area Network) is a networking standard that

distinguishes itself by supporting both star topology and mesh topology networking for low power applications. It is designed to use very little power enabling it to work for years in battery-operated situations, even when a device is in sleep mode. It is limited to 250kbit/s, which makes it ideal for IoT applications in the home and industrial settings. IEEE 802.15.4 specifies how devices broadcast and connect, but not some of their higher level interactions which are necessary to allow devices to interact in a meaningful way.

A number of other standards both open and proprietary are built on top of IEEE 802.15.4, including Wireless Hart, MiWi, ISA100.11A, Zigbee and Thread, each of which addresses different use cases. IEEE 802.15.4, however, does not work well with a standard IP stack, which has prompted the internet Engineering Task Force (IETF) to develop the 6LowPanstandard to enable native IPv6. The difficulty lies in the packet size, which for IEEE 802.15.4is too small to hold a standard IP packet, and the energy consumption associated with the internet's always-on assumption. Unlike Bluetooth, however, 802.15.4 is rarely supported on mobile phones, tablets and laptops, and therefore needs a dedicated gateway to function.

Zigbee is the most well-known standard to make use of IEEE 802.15.4. However, a number of incompatible implementations of Zigbee exist on the market, which has slowed adoption. Zigbee can be found in light bulbs by GE and Philips and Comcast's new set-top box. Most variants of Zigbee do not support IP-based networking natively although some do. One reason for lack of native support for IP is the power requirements. For example, Zigbee Green Power allows the use of Zigbee networking in devices that have no permanent power source, such as a battery or other electrical connection. Instead, these devices can harvest energy from motion, such as by pressing a light switch.

In 2014, Google Nest, Samsung, ARM and a number of other companies announced Thread, a standard for in and around the home, launched as an alternative to Zigbee. Thread makes use of 802.15.4 and comes with native 6LowPan support. While incompatible with Zigbee, it is designed in such a way that the same chips and radios can be used. Whether it will be successful remains to be seen. A number of alternative proprietary technologies to IEEE 802.15.4-based technologies exist, such as ANT, Peanut and Z-Wave. Of these, Z-Wave is the most widely implemented.

GE, for example, offers a wide range of Z-Wave-based products. As proprietary technologies, they are controlled by a company or group of companies, unlike open standards which allow everyone to make use of the standard (under certain conditions). A limited number of vendors provide the chips and radios, although more vendors may be building packages around the technology.

Wi-Fi (IEEE 802.11x) is the final networking protocol in this quadrant that deserves attention. It forms the basis for a great many IoT devices in and around a home, with almost every ISP supplying its customers with a modem/switch with Wi-Fi on board. Despite using unlicensed spectrum, Wi-Fi has become the preferred way for many consumers to connect to the internet. It was optimised for use by computers in local area networks and as a result can attain speeds of up to 1Gbit/s, instead of prioritising energy efficiency, as does IEEE 802.15.4. This makes Wi-Fi the technology of choice for higher bandwidth and low latency applications, such as voice and video applications. As a result, Wi-Fi requires more energy and does not support battery-operated technologies well. Wi-Fi is therefore used to connect all kinds of devices that are (regularly) connected to the mains supply.

Short-range networking technologies are the most contentious area for networking the IoT, as the conflicting requirements of technologies make it hard to predict a winner. Where a technology needs to work for years on a single charge, IEEE 802.15.4 or

Bluetooth-based technologies win out. Where high speeds are needed, Wi-Fi is a likely choice. However, no matter what technology is chosen, a trade-off needs to be made. A possible solution is for some manufacturers to put multiple networking technologies in some of their chipsets aimed at IoT solutions. This might increase the costs of the chipsets, but also increase the flexibility with which they can be deployed, and potentially avoid lock-in.

4.4.1 Thread Group

Following is an extract from http://threadgroup.org/.

"In response to the difficulties associated with getting consumer devices to talk to one another. And once they do, the connection is often spotty and power hungry. The Thread Group was established in 2014 to change that. The foundation members are ARM, Bigass Fans, Freescale semiconductor, Nest, Samsung, Silicon Labs and Yale, based in San Ramon California.

It is a low power mesh network designed to securely and reliably connect hundreds of consumer products around the home – without blowing through battery life.

- Designed specifically for the home
- Robust self-healing mesh network
- No single point of failure
- Interoperable by design using proven, open standards and IPv6 technology with 6LoWPAN as the foundation
- Requires just a software enhancement for today's 802.15.4 products

Designed to support a wide variety of products for the home: appliances, access control, climate control, energy management, lighting, safety, and security. The positioning of Thread is shown in the following figure.

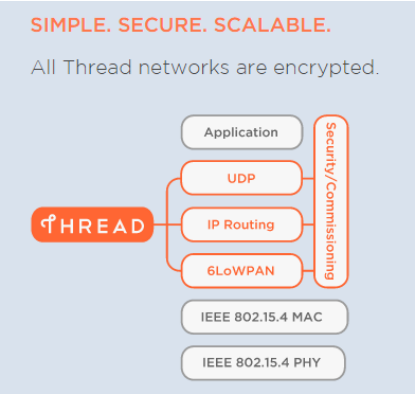


Figure 23: The Thread model

All Thread networks are easy to set up and secure to use. They use a smartphone-era authentication scheme and AES encryption to close security holes that exist in other wireless protocols.

- Simple installation using a smartphone, tablet or computer
- Scalable to connect 250+ devices into a single network supporting multiple hops
- Provides security at network and application layers
- Product install codes are used to ensure only authorized devices can join the network
- Supported by banking-class, public-key cryptography

Designed from the ground up to have extremely low power consumption. Devices efficiently communicate to deliver a great user experience, yet still run for years on the smallest of batteries.

- Extensive support for sleepy nodes allows for years of operation, even on a single AA battery
- Based on the power efficient IEEE 802.15.4 MAC/PHY
- Short messaging conserves bandwidth and power
- Streamlined routing protocol reduces network overhead and latency
- Designed to run on readily available, low power wireless system-on-chips"

4.5 Wide Area Connectivity

Mobile/wireless carrier networks traditionally end at a modem or personal device. This boundary is shifting and the choices are becoming numerous. The carrier network is being extended with Wi-Fi LAN technologies etc. and this is in some cases being provided by the fixed or mobile carrier and in some cases offered by over-the-top players. When considering this, the notion of a level playing field for public networks gets more complicated as the boundary of the playing field may vary from provider to provider.

One carrier service may terminate at a home router/modem while another may extend to include LoRaWAN or 802.11ah for extended range sensor connectivity. And the nbn provided the wholesale access only which means that there could be as many as four or even five providers in an end-to-end 'sensor to actuator and analytics' service.

In other cases a service provider may offer only this wider area connectivity in unlicensed spectrum while another offers similar service but in licensed spectrum.

Moreover, with the advent of electronic subscriber identity modules (eSIMs) or 'soft' SIMs there will be models where the eSIM provider may not be the licenced carrier provider, which brings into question service responsibilities and licencing conditions.

Observation 12: The advent of IoT will introduce the possibility of increasing fragmentation of the service components across potentially many sub-component service providers. For example, access, core network, data storage and distribution etc. Similarly, with the advent of eSIMS, consideration will need to be given to what service obligations and licencing conditions should apply to the 'service provider' to ensure customer service obligations are met and a level-playing field exists between service provision at the appropriate layers and segments.

4.5.1 Long-Range and Mobile Networks

This sub-section borrows heavily from "Ofcom Statement 27 January 2015; Promoting investment and innovation in the internet of Things Summary of responses and next steps".

For geographically dispersed networks wired options are only viable in locations where wired connectivity is already present, or for certain organisations such as those managing roads, railroads and other infrastructures as part of an overall smart infrastructure. For others, the costs associated with the civil works necessary often make wiring remote locations too expensive. For this reason the use of wireless networks is essential to the IoT for geographically dispersed IoT applications. Whether used to control traffic lights or remotely monitoring pumps or vehicles, the only cost-effective way to

connect them is through wireless networks. In many cases, the combination of fixed network supplemented by wireless will be appropriate.

The choices of wide-area connectivity, as well as local area connectivity are driven by some fundamental constraints, as shown in the Ofcom sourced figure below:

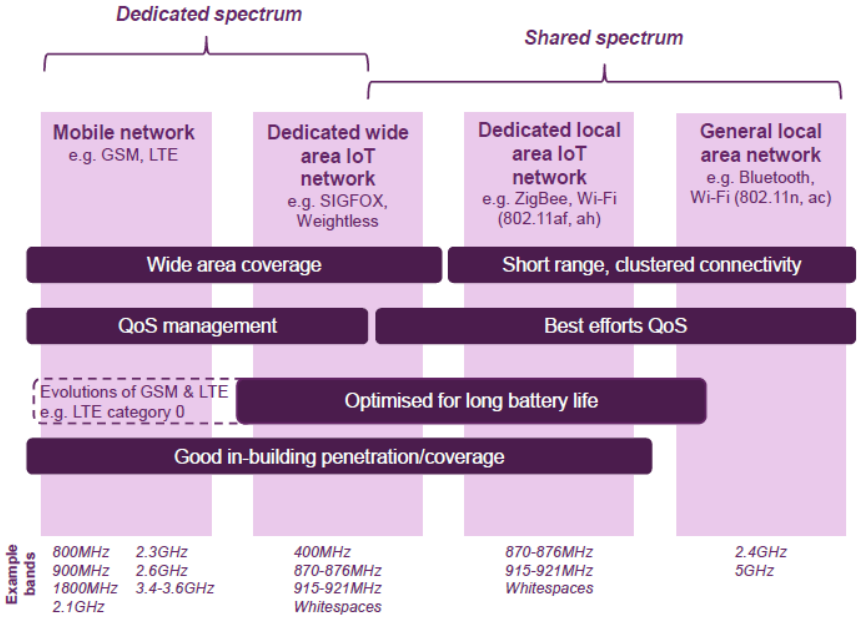


Figure 24: The wide range of wireless choices for IoT

Mobile networks offer great flexibility but with this flexibility comes high service connectivity tariffs today and networks dimensioned for device numbers consistent with the population of people. The IoT dramatically alters these connectivity and tariff models so these is much to consider here.

"2G/3G/4G networks, as developed by the 3rd Generation Partnership Project 2 (3GPP2), are the primary networks for the deployment of the IoT:

- 2G (GSM) networks offer near-worldwide coverage, both indoors and outdoors, and as such are considered future proof. Some mobile operators plan to retire their 2G networks (e.g. AT&T in 2017 and Telstra and Optus in similar timeframes), but their coverage can be superior to that of 3G and 4G networks and the installed GSM base is so large, particularly in Europe, that retirement will prove challenging.
- 3G (UMTS/HSDPA) is considered by some in the industry to be less useful because it makes use primarily of the 2,100 MHz band, which does not offer good indoor coverage. Nevertheless, some countries use 3G in other bands and some M2M modules support 3G.
- 4G networks are increasingly prized because of their potential for use in a wide range of frequencies, including below 1 GHz, and their high throughput and low latency. 4G networks can also work in bands that currently support 2G and 3G. 4G IoT modules are still considered expensive, although prices are decreasing. Analysts predict that by 2022, 70% of M2M modules for M2M applications will use 4G. However, this would still leave 30% of the market based on 2G modules. Given the 10 to 20-year lifespan of M2M, this effectively means that 2G networks would need to remain operational well after 2030 (Connected World, 2014).

There are, however, drawbacks to using 2G/3G/4G networks for large-scale IoT roll outs. The primary obstacle is SIM card lock-in. It is difficult if not impossible to switch mobile operators during the lifetime of the device, as any change in operator requires the physical replacement of the SIM card, which locks the device to a single operator. This hinders competition. One way to overcome or minimise this concern is with the use of the electronic SIM or eSIM that allows the SIM functions to be reprogramed without physically changing a SIM card.

In addition, it creates difficulties in achieving coverage because even in dense cities no one network can claim full (indoor) coverage. If competitors' networks cover a location, then large-scale users may opt to use multiple networks at the same time. Moreover, mobile networks are not static and change their operating characteristics based on demands from network load and operations such as maintenance.

Research in Norway has shown that up to 20% of devices are offline for at least 10 minutes a day, even in dense cities, without counting major network failures. In addition, some sites may face congestion during busy hours. This may not be a problem for smart electricity meters which can reschedule data transmission, but it does pose a problem for recharging an electric vehicle, traffic lights and payment terminals that require direct interaction. Some have suggested that additional quality-of-service mechanisms are necessary to deal with the best-effort nature of the internet, in order to support critical IoT applications such as autonomous vehicles or eHealth.

However, others argue that the inherent unreliability of the underlying network and the inability of higher networking protocols, such as IP, to effect change, calls for a more fundamental approach. This would involve making applications more resilient and allowing the fast switching of the underlying network using operator-independent SIM cards or 'soft' SIMs. In addition, international mobile roaming, though well supported, is expensive and no mobile network operator or alliance of operators has a wide enough footprint to offer good coverage and rates for some customer requirements.

One option is for Governments to change regulations to allow private companies (not public telecommunication networks) to hold the numbers necessary for use in mobile networks, such as international mobile subscriber identities (IMSIs) for SIM cards, telephone numbers and mobile network codes. This would make the market for 2G/3G/4G connectivity competitive without long-term lock-in to a single network. Instead, customers could choose one or more networks per territory, based on their needs. They might even opt to use alternative networks, such as wifi networks, and employ their SIM card as an authentication mechanism.

In the Netherlands, the Government has changed the existing regulations, in part at the request of its energy sector, for the roll-out of smart meters. Enexis, a regulated utility managing an energy network, is the first private virtual network operator in the country to use its own SIM cards. It chose this solution to avoid lock-in and ensure flexibility in the future.

The Governments of Belgium and Germany are also consulting on a possible rule change. The European Conference of Postal and Telecommunications Administrations (CEPT/ECC) working group on naming and numbering concluded in a report on IMSI numbers for SIM cards that:

"CEPT countries should review the assignment criteria for E.212 Mobile Network Codes (MNCs) and consider introducing more flexibility regarding the assignment of MNCs for:

a. Traditional market players such as MVNOs, MVNEs and Resellers; and

b. Emerging business models such as M2M service providers and SMS Service Providers (ECC, 2014)."

Some Governments are of the opinion that changes to the relevant ITU recommendations are necessary to grant private networks access to IMSI numbers and related numbers. In2015, the ITU Study Group 2 will discuss proposed changes to the relevant regulation. As a result of potential lock-in with mobile networks and the challenges in achieving coverage, large-scale suppliers and users of the IoT have been looking at alternative networking options. It is instructive to examine various solutions used for automatic meter reading/smart grids. Telefonica together with Connode from Sweden won a15-year contract to supply smart metering solutions in the United Kingdom, using a combination of 802.15.4 IPv6-based mesh networking and cellular connectivity. The mesh networking allows smart meters to use other smart meters to reach a hub that has cellular connectivity. If coverage is lost on one node, another node can act as a hub.

In the Netherlands, Alliander (a regulated utility managing an energy network) purchased a code division multiple access (CDMA) 450 license from an existing licensee to offer network services to its own operating companies for smart grid purposes, but also to third parties. CDMA450 offers better coverage than higher frequency networks and is used by some companies to deploy wireless telephony in rural areas. The technology has limited capacity for voice calls; however, CDMA450 or long term evolution (LTE) 450 may deliver data communication with better coverage than existing wireless technologies. In other countries, energy companies have opted to use power-line communication, which can take up to a day to relay messages. While too slow for real-time services, this option often proves reliable and falls under the control of the energy company. In some cases, metering companies have opted for a short-range drive-by system, where the meter is not permanently connected but communicates when a meter company vehicle passes nearby.

In the United Kingdom, a company called Neul (recently purchased by Huawei) advocates the use of whitespace spectrum – unused frequencies in the television bands. Its technology works on spectrum between 470 MHz to 790 MHz. In France, SIGFOX aims to use unlicensed industrial, scientific and medical (ISM) bands (868 MHz in Europe and 902 MHz in the United States) with Ultra Narrow Band networks. A device can send up to 140 messages per day of 12 bytes payload. Although currently available in only a few countries, it received US$115 million in funding in 2015 to expand locations. Another French company, Semtech, and others are promoting LoRa for long-range (up to 15 km) communication at low bit-rates with IoT devices.

These developments underline the need on the part of many users for communication over a widely dispersed area with large coverage. Alternative solutions to 2G/3G/4G are being developed, however only a few can make use of globally standardised spectrum bands and the available spectrum bandwidths are narrow, limiting their use." (Ofcom Statement 27 January 2015; Promoting investment and innovation in the internet of Things Summary of responses and next steps)

4.5.2 LTE-M or LTE for M2M

"With the IoT and M2M communications becoming more widespread, there has been a growing need for a version of LTE that meets the needs of lower power, lower data rate and longer battery life.

LTE, the long term evolution cellular system, is well placed to carry a lot of the traffic for machine to machine communications. The issue is that LTE is a complex system capable

of carrying high data rates and this is not always suitable for M2M.To overcome this issue a 'variant' of LTE, often referred to as LTE-M has been developed for LTE M2M communications. There are several requirements for LTE M2M applications if the cellular system is to be viable in these scenarios:

- **Wide spectrum of devices:** Any LTE machine to machine system must be able to support a wide variety of different types of devices. These may range from smart meters to vending machines and automotive fleet management to security and medical devices. These different devices have many differing requirements, so any LTE-M system needs to be able to be flexible.
- **Low cost of devices:** Most M2M devices need to be small and fit into equipment that is very cost sensitive. With many low cost M2M systems already available, LTE-M needs to provide the benefits of a cellular system, but at low cost.
- **Long battery life:** Many M2M devices will need to be left unattended for long periods of time in areas where there may be no power supply. Maintaining batteries is a costly business and therefore any devices should be able to have a time between battery changes of up to ten years. This means that the LTE-M system must be capable of draining very little battery power.
- **Enhanced coverage:** LTE-M applications will need to operate within a variety of locations – not just where reception is good. They will need to operate within buildings, often in positions where there is little access and where reception may be poor. Accordingly LTE-M must be able to operate under all these conditions.
- **Large volumes – low data rates:** As it is anticipated that volumes of remote devices will be enormous, the LTE-M must be structured so that the networks are be able to accommodate vast numbers of connected devices that may only require small amounts of data to be carried, often in short peaks but with low data rates.

A number of updates have been introduced in 3GPP Rel 12 to accommodate LTE-M requirements. These updates mean that the cost of a low end M2M modem could be about half that of a regular LTE devices, making them comparable with (enhanced general packet radio service) EGPRS ones.

To accommodate these requirements a new (user equipment) UE category has been implemented – LTE Category 0. These categories define the broad capabilities of the device so that the base station is able to communicate properly. These low cost LTE-M, M2M modems have limited capability, including relating to:

- **Antennas:** There is the capability for only one receive antenna compared to two receive antennas for other device categories.
- **Transport Block Size:** There is a restriction on the transport block size. These low cost LTE-M devices are allowed to send or receive up to 1000 bits of unicast data per sub-frame. This reduces the maximum data rate to 1 Mbit/s in both the uplink and the downlink.
- **Duplex:** Half duplex (frequency division duplex) FDD devices are supported as an optional feature – this provides cost savings because it enables (radio frequency) RF switches and duplexers that are needed for the full performance modems to be removed. It also means there is no need for a second phase locked loop for the frequency conversion, although having only one (phase locked loop) PLL means that switching times between receive and transmit are longer.

There are several features that are being proposed and prepared for the next release of the 3GPP standards in terms of LTE M2M capabilities. These include some of the following capabilities:

- Reduce bandwidth to 1.4 MHz for uplink and downlink
- Reduce transmit power to 20dBm
- Reduce support for downlink transmission modes
- Relax the requirements that require high levels of processing, e.g. downlink modulation scheme, reduce downlink (hybrid automatic repeat request) HARQ timeline

It should be stated that these last points for Rel 13 are currently only proposals and are not yet implemented.

With a number of cellular style M2M wireless communication systems like LoRa(described in Section 5.2 of this document) and Sigfox (described in Section 5.3 of this document) being deployed, LTE needs its own M2M capability to ensure that it is able to compete with these growing standards. Otherwise LTE may not be suitable for carrying this form of low data rate date from devices that require long battery life, etc. LTE-M is the cellular operators' attempt to respond to this."

(Source: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/lte-m-m2m-machine-to-machine.php)

4.5.3 Constrained Application Protocol (CoAP) or Message Queuing Telemetry Transport (MQTT)

The following text is sourced from: http://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php

"Two of the most promising protocols for small, low cost sensor devices are MQTT and CoAP. Both MQTT and CoAP:

- Are open standards
- Are better suited to constrained environments than HTTP
- Provide mechanisms for asynchronous communication
- Run on IP
- Have a range of implementations

MQTT gives flexibility in communication patterns and acts purely as a pipe for binary data. CoAP is designed for interoperability with the web."

Both have their place and it is possible that both will be supported in many low cost sensors to enable large volume manufacturing cost reductions.

4.5.4 Constrained Application Protocol (CoAP)

Following is the Wikipedia definition of CoAP: "Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronics devices that allows them to communicate interactively over the internet. It is particularly targeted for small low power sensors, switches, valves and similar components that need to be controlled or supervised remotely, through standard internet networks. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Multicast, low overhead, and simplicity are extremely important for internet of Things (IoT) and Machine-to-Machine (M2M) devices, which tend to be deeply embedded and have much less memory and power supply than traditional internet

devices have. Therefore, efficiency is very important. CoAP can run on most devices that support UDP or a UDP analogue.

The internet Engineering Task Force (IETF) Constrained RESTful environments (CoRE) Working Group has done the major standardization work for this protocol. In order to make the protocol suitable to IoT and M2M applications, various new functionalities have been added. The core of the protocol is specified in RFC 7252, important extensions are in various stages of the standardization process."

4.5.5 Message Queue Telemetry Transport (MQTT)

The following text is sourced from: http://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php

"MQTT is a "publish/subscribe" messaging protocol designed for lightweight M2M communications. It was originally developed by IBM and is now an open standard. MQTT has a client/server model, where every sensor is a client and connects to a server, known as a broker, over TCP. It is message-oriented. Every message is a discrete chunk of data, opaque to the broker. Every message is published to an address, known as a topic. Clients may subscribe to multiple topics. Every client subscribed to a topic receives every message published to the topic.

MQTT supports three quality of service levels, "Fire and forget", "delivered at least once" and "delivered exactly once".

Even though MQTT is designed to be lightweight, it has two drawbacks for very constrained devices. Every MQTT client must support TCP and will typically hold a connection open to the broker at all times. For some environments where packet loss is high or computing resources are scarce, this is a problem."

4.5.6 Wireless Technology Choice – Spectrum and Licence Limited

Wireless technology design decisions that need to be made for optimum IoT connectivity are based on a number of criteria including, latency, cost and bandwidth as well as the availabilty of precious Government controlled spectrum.

In many cases, the 'right' technology may simply not be able to be used, due to local country regulations and licensing rules. It is critical for a nation's economy that the management of spectrum, and thereby the appropriate technology choice can flexibly accommodated within the very fast changing IoT market environment.

Difficult areas include the use of LAN wireless technologies in shared unlicensed spectrum which is increasingly cluttered and noisy which results in unreliable sensor connectivity. This problem is getting worse as more devices are connected.

Furthermore, as new standards emerge to extend these LANs such as used by Taggle, LoRa, SIGFOX, IEEE's 802.11ah and others, the spectrum is either open and congestible or spectrum prices can be prohibitive for entry of innovation by smaller players and potentially too risky in the short term to attract the big players. The 'sole use' spectrum is not really appropriate for low cost sensors. Therefore looking closely at a new model of spectrum management for IoT may be appropriate.

As new IoT services grow and use wireless spectrum to support business models with millions and billions of sensors/actuators, the business value per Hz will change within the various bands used for connectivity. This will force a rethink in the licencing of IoT connectivity bands – much as old terrestrial analogue services made way for more efficient digital alternatives.

Observation 13: IoT will force a re-evaluation in the value of wireless spectrum for connectivity, accessibility, sharing and licencing across existing and new bands. National regulators of spectrum are recognising this and providing focus on preparing for a more pervasive IoT future.

4.5.7 Massive IoT Numbering – IPv6 and the IoT

IPv6 and the IoT are often perceived to be strongly aligned, to the extent that they are mutually reliant. The IoT needs the massively expanded protocol address space that only IPv6 can provide, while IPv6 needs to provide a substantive foundation to justify the additional expenditures associated with widespread deployment of this new protocol. Some argue that the use of IPv6 would also alleviate shortages in telephone numbers and IMSI numbers. However, these are still necessary for the moment, to identify a device in a mobile network over which IPv6 is run.

However, the evidence to date on device deployments does not provide a compelling justification. Existing deployment of sensor networks, mobile devices and other forms of microware all use the IPv4 network. This is viewed as a pragmatic choice, dictated by availability. While estimates vary, the consensus indicates that between 8 billion and 10 billion devices were connected to the internet in 2012. At that time the internet comprised about 2.5 billion addresses, indicating that the majority of these devices were located behind conventional network address translation (NAT) units that allow one IPv4 address to be shared across multiple devices simultaneously.

This raises the question of whether the IoT requires IPv6 as an essential precondition, or whether an ever-expanding population of micro devices can continue to be deployed on the present address-sharing framework on IPv4, or a mix of IPv4 and IPv6 with translation between parts of the same network.

Given the large volume of devices contemplated in the IoT, the 'polled model' would require the greater volume of addresses supplied by IPv6, and could not be sustained on IPv4. An alternate sensor-reporting model is the 'report to base' model, in which the device collects data and periodically initiates a connection to its controller to pass the data back.

This second model functions adequately in an environment of IPv4 and NATs, as the device initiates connection requests and is assigned the use of a public address only for the duration of the connection. At the same time, this model essentially 'hides' the sensor device from the external internet, as the NAT function effectively prevents external agents from initiating any form of communication with the device.

Much of the work to date in sensor networks and similar application environments for embedded automated devices uses this 'report to base' model of connection, which permits the devices to be located behind NATs and use the existing IPv4 network. Such devices do not add to the impetus for broad IPv6 deployment. However, when continuous sensor models (e.g. video streams or continuous environmental sensors) are considered, as well as forms of 'just in time' opportunistic data collection, then the ability to poll sensors as and when needed becomes a significant asset and NATs become an impediment.

In this case, using IPv6 is generally thought to be a necessary precondition. However, not using a NAT will expose unattended micro devices to the internet. This has attendant issues relating to security and abuse, including the risk of such addressable devices being co-opted into various forms of high-volume distributed denial of service (DOS) attacks. The question of whether the larger address space of IPv6 effectively prevents the opportunistic discovery of sensor devices, or whether operational prudence requires that

such exposed sensors be equipped with robust security and continual monitoring and maintenance, is at present an open issue for the sensor industry. It should be noted however that one of the critical elements of a successful IoT market is that of simplicity and security and IPv6 definitely offers improvements in both these key areas.

Observation 14: IPv6 is the universally agreed, preferred communications protocol for IoT for scalability, security by design and simplicity.

Source: CommsWire No: 150507, Thursday 7th May 2015 (reprinted with permission)

VINT CERF TELLS INTERNET USERS TO ASK ISPS FOR IPV6 CITING INTERNET OF THINGS

At the US National Press Club, 'Father of the internet' Vint Cerf and Chief internet Evangelist at Google says IPv6 will be essential for the 'internet of things'.

The world has run out of IPv4 addresses, which only number at 4.3 billion, with IPv6 promising 340 trillion trillion trillion addresses.

With Cisco predicting 50 billion devices to be connected to the internet by 2020, IPv4 clearly won't handle it, while for IPv6 it is just a drop in the bucket.

At the US National Press Club earlier this week, Vint Cerf explained to the audience that 'the world needs more internet addresses'. Cerf's 59 minute speech to the Press Club can be watched in full, embedded below, while the YouTube link is here. USA Today quoted Cerf stating: "The next wave of stuff is the internet of Things.

"Every appliance you can possibly imagine, you're shifting from electromechanical controls to programmable controls. And once you put a computer inside of anything, there's an opportunity to put it on the Net."

"I think ultimately when we finally get (IPv6) everywhere, people will have the flexibility to run end-to-end security and safety.

"They'll be able to cluster things together and have hubs that manage access to them which we're going to need for the internet of Things." Cerf called for internet users to switch to IPv6 and call their ISPs to get switched over.

However a check for 'IPv6 Telstra' on Google uncovered a Crowd support Telstra forum Thursday 7 May 2015 iTWire Pty Ltd www.itwire.com page 11 where a Telstra technical support representative stated in answer to a question in July 2014 about IPv6 that: "While the IPv6 is clearly visible to you, it is not currently accessible/available/configurable for Bigpond customers. There is no official word on when this will be officially supported by Bigpond and is currently it is only available to business grade services."

Another Crowd support Telstra forum page has a user called 'Disstopic' asking about IPv6 for Bigpond DSL customers back in October 2013.

The same technical support agent from the other Crowd support thread answered back in 2013 with a similar message, that IPv6 was available for business customers only.

The thread ends with user 'Disstopic' stating on 12 March 2015: "It is been over a year now since my original post in this thread. Surely IPv6 can't be too far away now. "Every router being sold seems to support IPv6, and my home network is ready to go. Just need Telstra to flick the switch.

"I kind of get that with the NBN rolling out Telstra may not see the ADSL network as a priority, but surely given IPv6 is a proven technology there is no harm in letting those who want it have it. "Has anyone got any insider information as to when IPv6 may be available for home ADSL customers?" The question remains unanswered.

Optus also appears to only offer IPv6 for business customers and not consumers. According to Google IPv6 rankings, Australia only has a 1.21% IPv6 adoption rate.

While countries such as the US have a 14.96% adoption rate, Germany 14.86% and Peru a 13.49% adoption rate, many countries around the world are also low adopters of IPv6, with China at 1.2% and the UK at 0.33%, for example. Meanwhile, apnic.net only puts Australia at 0.78% adoption.

Google itself reports only about 6% of its users access IPv6 over IPv6, with Cerf saying only about 3 to 4% of internet users have IPv6.

According to WorldIPv6Launch.org, AT&T is the world's most IPv6 deployed telco, with 46.08% deployment. A search for Telstra or Optus didn't find them listed in the database of 240 telcos and organisations.

By Alex Zaharov-Reutt

4.6 Massive Data Storage

4.6.1 Cloud and Local Storage

Large data volumes from IoT will drive radical changes within today's data centres and will require new 'big data' strategies within enterprises. Due to a skills shortage and the need to constantly procure infrastructure to keep up with the amounts of incoming data, enterprises will increasingly move away from the in-house models towards platform-as-a-service (PaaS), managed, and orchestrated solutions. The value of IoT is in the data, the quicker enterprises can start analysing their data the more business value they can derive.

Data was getting seriously 'big' even before IoT devices entered the picture. EMC and IDC have been tracking the size of the 'digital universe' (DU), since 2007. The DU is all the digital data created, replicated and consumed in a single year. In 2012 EMC and IDC estimated that the DU would double every two years to reach 40 zettabytes (ZB) by 2020 – a number since revised upwards to 44ZB (that is 44 trillion gigabytes). Astronomical numbers perhaps need astronomical illustrations, which may be why EMC/IDC pictured 44ZB as 6.6 stacks of 128GB iPad Air tablets reaching from earth to the moon. The DU estimate for 2013 was 4.4ZB (or one stack of iPads reaching two-thirds of the way to the moon).

Observation 15: There are profound implications and opportunities, in how, where and by whom data is captured and stored for IoT.

Amazon, one of the biggest cloud service providers, describes cloud as follows:

"Whether you are running applications that share photos to millions of mobile users or you're supporting the critical operations of your business, the 'cloud' provides rapid access to flexible and low cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use.

Cloud Computing provides a simple way to access servers, storage, databases and a broad set of application services over the internet. Cloud Computing providers own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application.

Instead of having to invest heavily in data centres and servers before you know how you're going to use them, you can pay only when you consume computing resources, and only pay for how much you consume.

By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers are aggregated in the cloud, Web Services providers can achieve higher economies of scale which translates into lower pay-as-you-go prices.

The idea is to eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With Cloud Computing, these problems go away. You can access as much or as little as you need, and scale up and down as required with only a few minute's notice.

In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

Cloud computing has three main types that are commonly referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)."

In the context of IoT, cloud offers a real cost enabler. Combined with low cost sensing and ubiquitous low cost communications, low cost scalable computing resources add up to maturing and successful business models for IoT.

There is a number of cloud architectures that range from public to private and a hybrid model that combines aspects of public and private cloud.

Simple IoT solutions deploy sensors, gather and store data and then analyse it so it can be presented to the user in a meaningful way that adds value in one form or another. More complex solutions combine data sources. It is not practical to copy all the complex data sets into a single data base so that analysis can be performed. Instead the model now is to federate data. In other words, access data wherever it happens to be stored and use it without making a local copy of that data. Cloud based solutions can facilitate this open data model. Data sets are already too numerous to describe but recognising the wide variety of data sets helps to illustrate the scale and scope of the challenge. Date can come from environmental sensors, Government data sources like the Bureau of Meteorology, social media like Twitter and Facebook as well as any number of business applications and smartphone apps. The range is wide indeed and they may have all

been captured and stored for a specific single reason, only to be used by others later for completely unforeseen new business models.

This represents the breadth of choices for finding and accessing data as well as capturing specific data. Data centres emerge that solve these sorts of challenges. Different data centre approaches for different scenarios abound. There is no single right way, and there may be several different ways to address the data storage requirement of any IoT project.

4.7 Advanced Data Analytics

It is a somewhat axiomatic assumption that large amounts of data with advanced analytics offers significant potential for operational and market insight.

Big data, meanwhile, is characterised by 'five Vs': volume, variety, velocity, veracity and ultimately value. That is, big data comes in large amounts (volume), is a mixture of structured and unstructured information (variety), arrives at (often real-time) speed (velocity) and can be of uncertain provenance (veracity). Such information is unsuitable for processing using traditional structured query language (SQL) relational database management systems (RDBMSs), which is why a constellation of alternative tools, notably Apache's open-source Hadoop distributed data processing system, plus various NoSQL databases and a range of business intelligence platforms – has evolved to service this market. The five V's are summarised below.

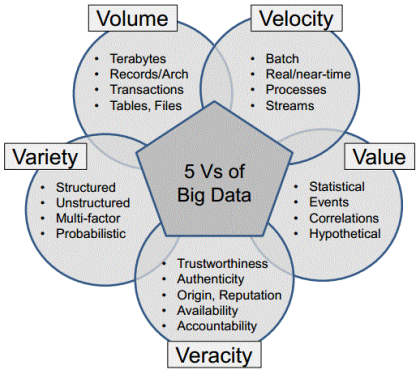


Figure 25: The five V's of big data

The IoT and big data are clearly intimately connected: billions of internet-connected 'things' will, by definition, generate massive amounts of data. However, that in itself would not usher in another industrial revolution, transform day-to-day digital living, or deliver a planet-saving early warning system.

As EMC and IDC point out in their latest Digital Universe Report, organisations need to identify high-value, 'target-rich' data that is:

- easy to access;
- available in real time;
- has a large footprint (affecting major parts of the organisation or its customer base); and/or
- Can effect meaningful change, given the appropriate analysis and follow-up action.

To deliver on these opportunities, a new generation of advanced data analytics within IoT applications will be required to address specific business needs such as: predictive maintenance; loss prevention; asset utilisation; inventory tracking; disaster planning and recovery; downtime minimisation; energy usage optimisation; device performance effectiveness; network performance management; capacity utilisation; capacity planning; demand forecasting; pricing optimisation; yield management; load balancing optimisation and many more.

Further, advanced data analytics needs to be able, insightful and applicable within sectoral domains.

The opportunity and success in the analysis of the volumes of data generated from IoT sensors will determine the value of the data and ultimately the benefit to the business and service provider.

Recently the Big Data Value Association (BDVA) was established under Belgian law. The BDVA is an industry-led association representing the big data value stakeholder community with a presence in Europe. Its principles are openness, transparency and inclusiveness. Refer to www.bdva.eu which is the source of much of the material in this sub-section. This group represents the view that data is a key asset and the following figure illustrates the scale of the European value chain for data.

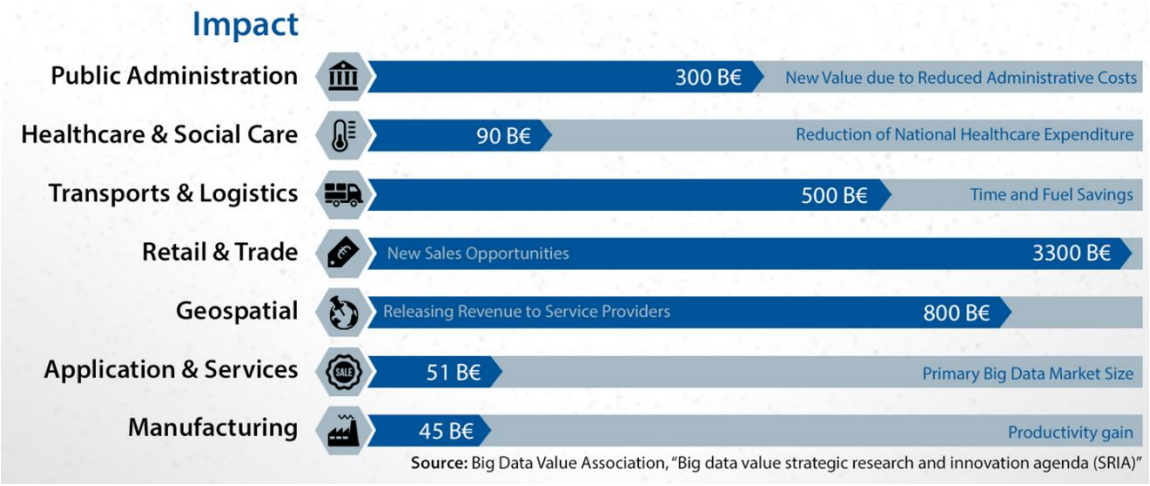


Figure 26: The financial impact of big data

Note that this summary is derived from existing industry verticals with existing data sets. The absence of agriculture and the environment is a reflection of the lack of sensor data today rather than the lack of importance of this sector.

Examples are emerging of businesses that manage the sale of information derived from big data analytics. One such example is Big Data Exchange (BDEX) who buy and sell data mostly around the retail goods sales experience. Refer to www.bigdataexchange.com.

Observation 16: The development of IoT advanced analytics is in its early days. There is opportunity for developers and service providers who can specialise and demonstrate insightful capability within analysis domains.

4.7.1 The Jasper Example

The following sub-section borrows heavily from the Jasper Technologies Inc White Paper "Best Practices for Implementing Global IoT Initiatives. Key Considerations for Launching a Connected Devices Service".

Jasper describes itself as "a global internet of Things (IoT) platform leader but today it is probably more accurate to describe it as a leader in M2M data gathering, sharing and analysis. Jasper has designed its software-as-a-service (SaaS) IoT platform to enable companies of all sizes to rapidly and cost-effectively launch, manage and monetize IoT services on a global scale. When companies do this, they become much more than product businesses. They become service businesses, capable of automatically managing their customers' entire IoT service lifecycle, delivering increased customer value and unlocking new sources of revenue.

More than 2,000 companies in over 20 vertical markets, including many of the world's top telcos and brands, choose Jasper to fast-track their IoT services. Jasper currently partners with 24 mobile operator groups, representing more than 100 mobile operator networks worldwide. Several of the major telcos in the Australian market use Jasper services.

The Jasper Control Centre optimizes and automates every stage of a carrier's IoT service lifecycle, enabling them to get the most out of devices, networks and applications. As telco's develop new data sets across more than just mobile devices, there will be a need to federate or integrate data with Jasper. Many telco's have mobile device data sets open already for third party developments leveraging the Jasper platform and this open data open API model is gaining support with telcos."

4.8 Collaboration Through Data Visualisation and APIs

Providing IoT services in an open and usable fashion will be fundamental for successful collaboration with partners and customers and will be a differentiator in ease of use and market take-up. To accomplish this open APIs and data visualisation technologies are essential. The following was sourced from http://www.sas.com/en_us/insights/big-data/data-visualization.html.

"Data visualization is the presentation of data in a pictorial or graphical format. For centuries, people have depended on visual representations such as charts and maps to understand information more easily and quickly.

As more and more data is collected and analysed, decision makers at all levels welcome data visualization software that enables them to see analytical results presented visually, find relevance among the millions of variables, communicate concepts and hypotheses to others, and even predict the future.

Because of the way the human brain processes information, it is faster for people to grasp the meaning of many data points when they are displayed in charts and graphs rather than poring over piles of spreadsheets or reading pages and pages of reports.

Interactive data visualization goes a step further – moving beyond the display of static graphics and spreadsheets to using computers and mobile devices to drill down into charts and graphs for more details, and interactively (and immediately) changing what data you see and how it is processed.

Visualizations help people see things that were not obvious to them before. Even when data volumes are very large, patterns can be spotted quickly and easily. Visualizations convey information in a universal manner and make it simple to share ideas with others. It

lets people ask others, “Do you see what I see?” And it can even answer questions like “What would happen if we made an adjustment to that area?”

There are a few basic concepts that can help you generate the best visuals for displaying your data:

- Understand the data you are trying to visualize, including its size and cardinality (the uniqueness of data values in a column).
- Determine what you are trying to visualize and what kind of information you want to communicate.
- Know your audience and understand how it processes visual information.
- Use a visual that conveys the information in the best and simplest form for your audience.

Data visualization is an art and a science unto itself, and there are many graphical techniques that can be used to help people understand the story their data is telling.”

Observation 17: Data visualisation and open service APIs are key for unlocking big data insights and proving usable, insightful IoT services and collaborating with partners and customers.

4.9 Security

IoT devices have embedded network, computing and other information processing capabilities, which allow these devices to be interconnected. The number and types of devices that are being manufactured with these built-in IoT features are increasing rapidly. It is imperative that assurance, security and governance professionals take notice of the IoT trend because it has the potential to redefine the risk equation within many enterprises and for individuals.

According to IDC, "Within two years, 90% of all IT networks will have an IoT-based security breach, although many will be considered 'inconveniences'...Chief Information Security Officers (CISOs) will be forced to adopt new IoT policies". Progress on data standards will help, but there is no doubt that security and privacy is a concern with the IoT particularly when it comes to areas like healthcare or critical national infrastructure.

The IoT was certainly prominent in the security predictions for 2015 issued by analysts and other pundits at the beginning of the year. Here is a selection (courtesy of ZDNet):

- Your refrigerator is not an IT security threat. Industrial sensors are. (Websense)
- Attacks on the internet of Things will focus on smart home automation. (Symantec)
- Internet of Things attacks move from proof-of-concept to mainstream risks. (Sophos)
- The gap between ICS/SCADA and real world security only grows bigger. (Sophos)
- Technological diversity will save IoE/IoT devices from mass attacks but the same will not be true for the data they process. (Trend Micro)
- A wearables health data breach will spur FTC action. (Forrester)

No one single control is going to adequately protect a device. A multi-layered approach to security is likely to be needed. Security cannot be thought of as an add-on to a device, but rather as integral to the device’s reliable functioning. At the protocol layer this is achievable leveraging the security features of IPv6. Software security controls need to be used at the operating system level, taking advantage of the hardware security capabilities now entering the market, and extend up through the device stack to

continuously maintain the trusted computing base. Building security in at the operating system level takes the onus off device designers and developers to configure systems to mitigate threats and ensure their platforms are safe.

Security at both the device and network levels is critical to the operation of IoT. The same intelligence that enables devices to perform their tasks must also enable them to recognise and counteract threats. Fortunately, this does not require a revolutionary approach, but rather an evolution of measures that have proven successful in IT networks, adapted to the challenges of IoT and to the constraints of connected devices.

4.9.1 Privacy by Design

In October 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing privacy by design as an essential component of fundamental privacy protection.

This was followed by the US Federal Trade Commission's recognition of privacy by design in 2012 as one of its three recommended practices for protecting online privacy in its report entitled "Protecting Consumer Privacy in an Era of Rapid Change – a major validation of its significance".

More recently, data protection by design has been incorporated into the European Commission plans to unify data protection within the European Union with a single law the General Data Protection Regulation.

Privacy by design's foundational principles are described by Intel as follows:

"Privacy by Design (PbD) is an approach that takes privacy into account and builds in protections at each phase of the product or service development process. It promotes the dual goals of enhancing privacy and personal control over individuals' information and enabling organizations to sustain a competitive advantage through innovation and robust data use. PbD incorporates seven privacy principles:

- Privacy should be built in at the beginning of product or service development. It should be proactive and not reactive, preventive and not remedial.
- Privacy should be implemented as the default setting.
- Privacy should be embedded into the product or service design.
- PbD encourages both privacy and robust innovation, with privacy as a positive-sum; not a zero-sum game.
- PbD involves implementation of end-to-end security that provides full lifecycle protection.
- PbD promotes openness, visibility, and transparency.
- PbD is about respect for user privacy and must be user-centric in its orientation."

4.9.2 Data protection

Data protection is tightly coupled with the subject of 'open data' discussed in Section 5 of this document. This also calls into play the quality of data and data provenance. For example if data containing information is collected from a group of environmental sensors and one isolated measurement is clearly faulty – perhaps reporting 100 Celsius when every other sensor in close proximity is reporting 5 Celsius. The analytics at play may choose to correct this fault and take some statistically acceptable way of extrapolating a 'better' value. How is this correction recorded, how is it accounted for in the analytics, who is trusted to make the correction and under what circumstances? The example used

is trivial but the principles applied will have impact across financial records, health records etc.

4.9.3 Work on IoT Security

Sachin Babar of Aalborg University has proposed a security model and threat taxonomy for the IoT[2]. This model is based on nine high level security requirements for IoT, and proposes a cube with dimensions of security, trust, and privacy. Xin Huang[3] has also proposed a security model called SecIoT. Helen Brumfitt[4] has proposed a novel IoT security framework which can be applied to mobile devices which connect back to the home IoT network.

The European Commission has published its research into the IoT architecture[5], which includes a section on security. This, however, provides a lot of information on security weaknesses but little in the way of security architecture. Malisa Vucinic has proposed an object security architecture for IoT called OSCAR[6] which leverages concepts from both content and connection centric approaches. David Lake published a paper on an eHealth IoT architectural framework[7], providing a sector specific perspective of how security could be architected. This leverages industry standards and security for connected health technologies as established by Continua Alliance. This could usefully form an initial deep dive investigation for the security focused workstream suggested to be founded in Section 8 of this study. Ricardo Niesse has published a paper on security policies for the IoT[8] as applied within a smart city context.

The Online Trust Alliance has published a discussion paper on an IoT trust framework[9], and is seeking feedback. The Cloud Security Alliance has also provided security guidance for early adopters of the IoT[10].

Testing

A key part of cybersecurity for IoT will be establishing a testing regime to ensure that any IoT deployment is cyber-secure. The Open Web Application Security Project (OWASP) has for a decade or more been the standard by which cybersecurity of web portals is judged with its OWASP Top 10 for the web. It has also produced an OWASP Mobile Top 10, and more recently an OWASP IoT Top 10. This provides a list of the top ten most significant attack surface areas for IoT.

Observation 18: Security technology and processes at design, management and service delivery will be critical for certain market sectors and applications. These will need to be consistent with any Government/industry regulations and guidelines regarding data privacy, security and network resilience.

---

[2] Babar S et al, Proposed Security Model and Threat Taxonomy for the internet of Things (IoT) CNSA 2010, CCIS89, pp 420-429 2010

[3] Huang X et al, SecIoT: A Security Framework for the internet of Things, Security and Communications Networks, May 2015

[4] Brumfitt HA, A Framework for Device Security in the internet of Things, 2014

[5] internet of Things Architecture (IoT-A) dated 4/3/2011

[6] Vucinic M et al, OSCAR: Object Security Architecture for the internet of Things, April 2014

[7] Lake D et al, internet of Things: Architectural Framework for eHealth Security, Journal of ICT, Vol 3 & 4, 2014

[8] Niesse R et al, SecKit: A Model-Based Security Toolkit for the internet of Things, Computers & Security, 2015

[9] Online Trust Alliance, IoT Trust Framework – Discussion Draft release August 11, 2015

[10] Cloud Security Alliance, Security Guidance for Early Adopters of the internet of Things (IoT), April 2015

4.10 Industry Platforms –Vertical and Horizontal

There is a host of new and nascent industry players introducing 'platform' solutions, whether at IoT horizontal levels (e.g. cloud storage or device as a service), or at the vertical level such as physical fitness as a service.

Some examples are shown below.

4.10.1 General Electric's Industrial Internet and Predix Platform

GE's position has been taken from www.ge.com and is "that the Industrial Revolution radically changed the way we use energy and make things. The internet Revolution altered how we communicate, consume information, and spend money. A combination of these two transformations, called the Industrial internet, now links networks, data and machines. It promises to remake global industry, boost productivity, and launch an entirely new age of prosperity and robust growth.

The opportunity is staggering. Estimates in the US alone are the Industrial internet could boost average incomes by 25 to 40% over the next 20 years and lift growth back to levels not seen since the late 1990s. If the rest of the world achieved half of the US productivity gains, the Industrial internet could add from $10 to $15 trillion to global GDP – the size of today's US economy – over the same period.

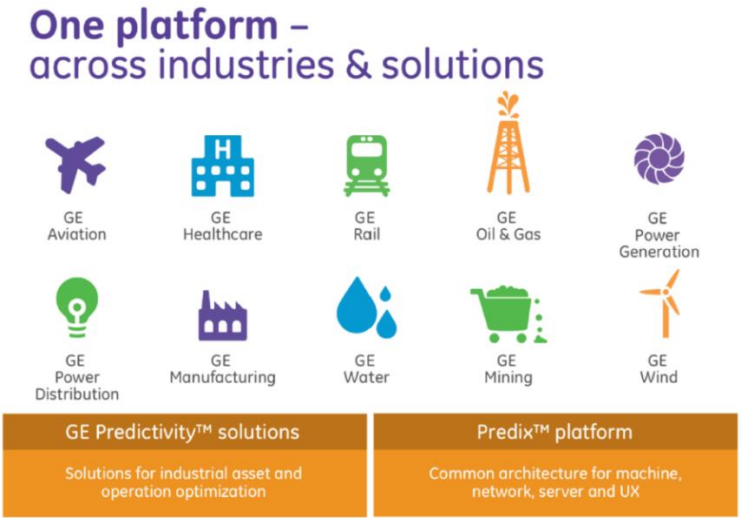


Figure 27: The GE Predix Platform

Predix is global Industrial IoT platform able to connect a wide variety of machines, sensors, control systems, data sources, and devices. These can include building infrastructure, mining equipment, aircraft engines, healthcare devices, and even Government systems. Some of these "things" are modern, while others might still need to be digitized. Predix can securely connect with multiple machines, old and new, from different vendors on very large industrial scales using a heterogeneous mix of data and communication protocols to aggregate data from these devices.

Predix provides services that enable developers and data scientists to deploy effective analytics. Pre-packaged services for machine learning, heuristic analysis, and physics- and engineering-based modelling will drive faster, more accurate insight and foresight. Predix incorporates years of insights building advanced machines and leverages expertise from the GE businesses and partners to enable mission-critical IoT applications.

Predix integrates cloud and mobile technology so that you can focus on innovation. Applications built on Predix can be delivered in several different models. The platform supports building responsive web applications that scale gracefully from smart phone to big glass in a traditional app development model or in a more contemporary cross-platform browser application. Predix allows developers to simplify the delivery and consumption of applications by using the automation and elasticity of cloud computing for faster time to market, improved agility, and reduced operating and capital expenses."

4.10.2 IBM Bluemix

IBM Bluemix is the cloud platform that helps developers build, manage and run web and mobile applications. At www.IBM.com Bluemix is being described as follows:

"Bluemix originally began with public cloud, our hosted deployment of the open source project Cloud Foundry. Since that time it has evolved into a much broader cloud platform, supporting an ever increasing variety of apps, workloads, and services across a combination of public and private cloud.

Following is a list of some of the tools IBM has made available to the development community. A selection of analytics, database management, cloud etc. all play an important part of this open platform for innovation."

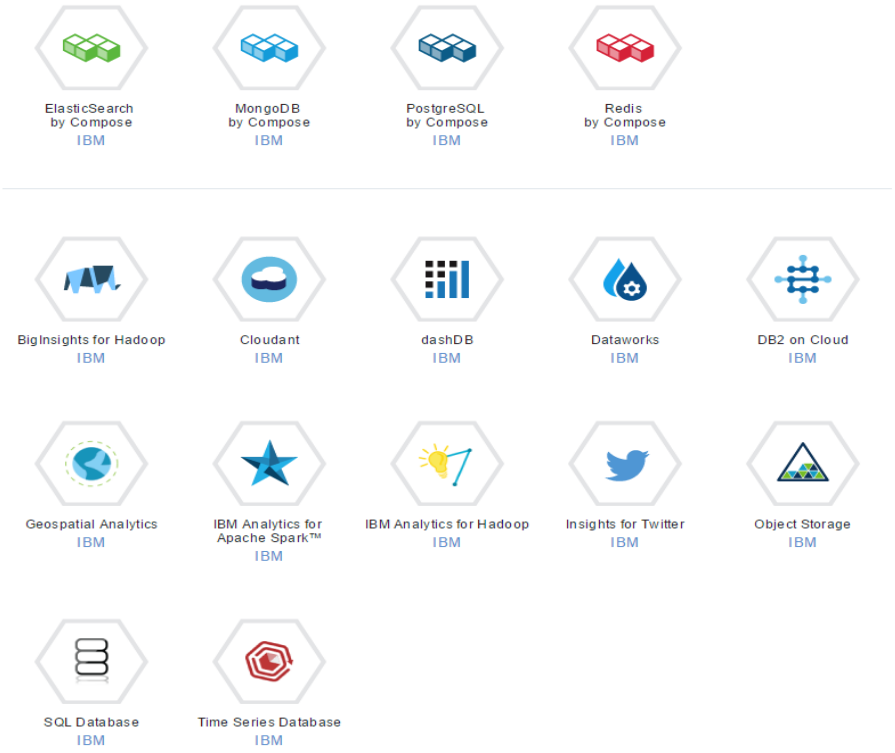


Figure 28: The IBM IoT Bluemix tools

IBM run Bluemix "Meetup groups" and "Bluemix Garage" events all over the world and involve about 20,000 developer members. Garage events are like collaboration hackathons and have been conducted in San Francisco, London, Toronto, and Nice. An event is in planning for Melbourne.

4.10.3 Google

Brillo is Google's new platform for IoT, which has been developed on the back of its acquisition of Nest in 2014. It is likely to change the IoT scenario for the personal device domain. For personal devices like smartphones and tablets, Google's website describes it as follows:

"IoT's growth will be platform and OS based. The Mobile era proved to us that no single player can build the eco-system themselves. Innovations are often crowd-sourced."

Brillo will have some commonalities and overlaps with Android and this is likely to help developers, who are already familiar with Android to adapt to Brillo. Back in 2008-09, developers used to swear by Microsoft Windows, now they swear by Android. Google has built a wide range of tools for developers and some of these learnings will seep into Brillo. With the kind of numbers that Android has in the smartphone market, Google can play a big role there, by integrating Brillo with Android.

Brillo is an Android-derived operating system for IoT devices. Brillo is smaller and slimmer than Android, providing a kernel, hardware abstraction, connectivity, and security infrastructure. The company does not talk technical details yet, so the range of systems-on-chips supported and specific hardware requirements are currently unknown; previous rumours estimated that it would go as low as 32 or 64 MB of RAM, making it a lot smaller than regular Android.

A preview of Brillo should be available in the third quarter of 2015.

Google has also announced Weave. Weave was described as a communications layer for IoT devices. Weave provides a common language and vocabulary so that IoT devices can advertise their capabilities to other devices on the same network and expose the different functions that they offer.

As such, it appears to be broadly comparable to Apple's HomeKit system for device discovery, configuration, and communication, being the glue that turns a bunch of disparate networked devices into a rich system for automation and interoperability.

Google said that it would be publishing documentation over the course of the rest of 2015, with a full stack available by the end of the year."

4.10.4 Apple

Within Apple's controlled iTunes and App Store model, they have launched a range of 'kits' that support developers in the IoT based on Apple products. The Apple Watch offers some new IoT possibilities and Apple is strongly supporting the app community to develop new ideas on this emerging platform. HomeKit is described at www.apple.com as follows:

"HomeKit is Apple's framework for communicating with and controlling connected accessories in a user's home and is based from iOS 8 onwards. You can enable users to discover HomeKit accessories in their home and configure them, or you can create actions to control those devices. Users can group actions together and trigger them using Siri.

If a developer builds an iOS app primarily designed to provide home configuration or home automation services such as turning on a light or opening a garage door then the HomeKit APIs used for communicating with HomeKit accessories is appropriate.

Apple also are supporting the development of accessories and sensors that sit within the HomeKit framework.

With the new features and capabilities that watchOS 2 brings to WatchKit, your apps can integrate even more closely with Apple Watch. Take advantage of the Digital Crown, microphone, Taptic engine, and health sensors to take your Apple Watch app to the next level. And with ClockKit, you can extend your app to the clock face with Complications."

4.10.5 Samsung

SmartThings is an Application acquired by Samsung that provides a dashboard letting you see what is happening at home when you're on the go: "See what's happening at home now and what's happened recently by looking at different category groups. Easily control your lights, locks, electronics, appliances and other connected devices in your home from anywhere. Set your connected devices to work in new ways when your needs change. This app supports Apple, Android and Microsoft devices.

The Things screen lets you control, name, and organize your connected devices and create custom images to identify them. As developers add new and creative use cases to the Platform. The "Activity Feed" lets you see up-to-the-minute information about what is happening in different parts of your home, and what has happened recently.

By selecting the area around your home on a map, you can trigger things to automatically happen; like doors locking or unlocking, and lights turning on or off; when your smartphone comes in and out of this prese range.

This app supports well over a hundred sensing devices across most home related parameters interfacing with Z-Wave, ZigBee and LAN protocols."

The full list can be found at: http://www.smartthings.com/compatible-products/

5 OPEN DATA AND DATA SHARING

A fundamental requirement and key enabler for IoT is the ability to access data and to share data.

Observation 19: So-called data silos within Asia-Pacific organisations – including many in Australia – are limiting the ability of major organisations to make insight-based decisions, and resulting in increased IT costs.

The above is a major finding from market researcher IDC in a report commissioned by cloud services provider Commvault.

Data silos are seen as repositories of fixed data that an organisation does not regularly use in its day-to-day operation, or make easily available to other systems in the organisation.

Commvault commissioned IDC to survey 600 IT decision makers across Asia-Pacific and India on how they can leverage data as a strategic asset, while minimising costs and risks.

One problem was identified as the continuing spread of data across different departments and locations – not only on-premises but also in various silos, third-party datacentres, and in highly virtualised environments – and in various formats.

In summary, open data solutions that are consistent across sectors will be increasingly important and vehicles for sharing data across sectors is a critical enabler for innovation in the digital economy.

5.1 The Value of Data

www.Opendatahandbook.org provides a simple explanation of open data as follows:

"Open data, especially open Government data, is a tremendous resource that is as yet largely untapped. Many individuals and organisations collect a broad range of different types of data in order to perform their tasks. Government is particularly significant in this respect, both because of the quantity and centrality of the data it collects, but also because most of that Government data is public data by law, and therefore could be made open and made available for others to use. Why is that of interest?

There are many areas where we can expect open data to be of value, and where examples of how it has been used already exist. There are also many different groups of people and organisations who can benefit from the availability of open data, including Government itself. At the same time it is impossible to predict precisely how and where value will be created in the future. The nature of innovation is that developments often comes from unlikely places.

It is already possible to point to a large number of areas where open Government data is creating value. Some of these areas include:

- Transparency and democratic control
- Participation
- Self-empowerment
- Improved or new private products and services
- Innovation
- Improved efficiency of Government services

- Improved effectiveness of Government services
- Impact measurement of policies
- New knowledge from combined data sources and patterns in large data volumes

Economically, open data is of great importance as well. Several studies have estimated the economic value of open data at several tens of billions of Euros annually in the EU alone. New products and companies are re-using open data. The Danish husetsweb.dk helps you to find ways of improving the energy efficiency of your home, including financial planning and finding builders who can do the work. It is based on re-using cadastral information and information about Government subsidies, as well as the local trade register. Google Translate uses the enormous volume of EU documents that appear in all European languages to train the translation algorithms, thus improving its quality of service.

Open data is also of value for Government itself. For example, it can increase Government efficiency. The Dutch Ministry of Education has published all of their education-related data online for re-use. Since then, the number of questions they receive has dropped, reducing work-load and costs, and the remaining questions are now also easier for civil servants to answer, because it is clear where the relevant data can be found. Open data is also making Government more effective, which ultimately also reduces costs. The Dutch Department for Cultural Heritage is actively releasing its data and collaborating with amateur historical societies and groups such as the Wikimedia Foundation in order to execute its own tasks more effectively. This not only results in improvements to the quality of its data, but will also ultimately make the department smaller.

While there are numerous instances of the ways in which open data is already creating both social and economic value, we don't yet know what new things will become possible. New combinations of data can create new knowledge and insights, which can lead to whole new fields of application. We have seen this in the past, for example when Dr. Snow discovered the relationship between drinking water pollution and cholera in London in the 19th century, by combining data about cholera deaths with the location of water wells. This led to the building of London's sewage systems, and hugely improved the general health of the population. We are likely to see such developments happening again as unexpected insights flow from the combination of different open data sets.

This untapped potential can be unleashed if we turn public Government data into open data. This will only happen, however, if it is really open, i.e. if there are no restrictions (legal, financial or technological) to its re-use by others. Every restriction will exclude people from re-using the public data, and make it harder to find valuable ways of doing that. For the potential to be realized, public data needs to be open data."

The following is an extract for a new report from Deloitte Access Economics titled "Assessment of the economic benefits of open Government data" for the Bureau of Communications Research. This extract highlights some of the views from:

- United Kingdom
- United States
- New Zealand
- Canada

United Kingdom

Increasing the economic value of open data in the UK has been a Government priority for some time resulting in more rigorous evaluation, both in Government commissioned reports and academic literature. This focus on open Government data is in part due to a commitment by the UK Government since the establishment of the Power of Information Taskforce in 2008 to not only study the economic and social gains that can be made through better use of Government data but also to capitalise on the opportunities (Vickery 2011). As part of this the National Archives, one of the main agencies implementing the 'Open Government' initiatives, produces an annual report outlining developments and the future agenda.

Relatively recent estimates put the overall economic value of Government open data in the UK at £1.8 billion (2011 prices) but when a measure of societal value is included, the figure jumps to between £6.2 billion and £7.2 billion (Deloitte, 2013). These estimates come from the UK-wide market assessment of public sector information (in this literature review referred to as Government open data), conducted by Deloitte for the UK Department for Business Innovation and Skills. As previously mentioned, this report built on the methodology of the DotEcon (2006) report, which placed the then current value of open Government data to the UK economy at approximately £590 million. The report found that this value could double to generate around £1.1 billion per year (DotEcon, 2006). In contrast, the PIRA (2000) report placed the then current value of open Government data in the UK at €11.2 billion per annum. Although the figure specific to the UK from the MEPSIR (2006) study is not available, as noted previously the MEPSIR (2006) study returned much lower figures for the EU than PIRA (2000) and as a result, it is likely that the €11.2 billion per annum figure is too high.

As well as the Government commissioned reports, there are a range of economic papers (Newberry, Bently and Pollock (2008) and Pollock (2009, 2011a, 2011b)) that estimate the welfare gains to UK society from opening up access to open Government data under specific restrictions. Pollock (2009) specifically estimates that the welfare gain could be £1.6 to £2 billion per year. From a UK Government perspective, this means that the estimates for potential gains from opening access to open Government data have ranged between £1.1 and £2 billion per year (from estimates made between 2006 and 2009).

Finally, there are a number of sector specific studies to come out of the UK. A 2013 study found that Ordnance Survey's (OS), Britain's mapping agency, open data initiative would deliver a net £13.0 million to £28.5 million increase in gross domestic product (GDP) in 2016. This comprises an increase in net productivity gains (£8.1 million to £18.2 million) and additional real tax revenues (£4.4 million to £8.3 million) (Carpenter & Watts, 2013). Comparing this to an Australian study using data from PWC (2010), Houghton (2011) found that the net welfare benefits from providing free access over cost recovery to Geosciences Australia topographical data would be around $25 million per annum. Assessment of the economic benefits of open Government data

United States

Of the US$3 trillion annual economic surplus that was estimated as potential global value to be unlocked through open data, the McKinsey (2013) study calculated that the US proportion of this figure would be approximately US$1.1 trillion. The global McKinsey study heavily relied on a previous report on the health care sector in the US, which again calculated the benefit of open data including private sources as well as Government ones, at US$350 to $400 billion. Like the global report, the exact methodology used in this study is ambiguous (Groves, Kayyali, Knott, & Van Kuiken, 2013).

Looking at the then current value of the open Government data in the US in order to provide a comparison point with the EU, PIRA (2000) estimated the annual economic value of the information sector, which is built on open Government information, at US$750 billion. As noted by teVelde (2009), this is a very optimistic estimate given that US$750 billion was almost 8% of US GDP in that year. The MEPSIR (2006) study, despite collecting data from the US in order to make comparisons with the EU, did not allow for an estimate of the overall market size. However the overall MEPSIR (2006) study found a figure substantially lower for the whole of Europe than PIRA (2000) and as a result it is possible that the €22 billion figure mentioned above for the size of the market in the US is an overestimate.

New Zealand

The major piece of work that has been completed for the New Zealand economy is the ACIL Tasman (2009) report into spatial information using similar methodology as the report by the same group on the Australian economy (ACIL Tasman, 2008). The report estimates that in 2008, the use and re-use of spatial information added NZ$1.2 billion in productivity-related benefits to the New Zealand economy. Further, they predict that "had key barriers been removed it is estimated that New Zealand could have benefited from an additional NZ$481 million in productivity-related benefits in 2008, generating at least $100 million in Government revenue". These figures align with the results of the Australian study, which found that Australia could have benefited from an additional $500 million in productivity-related benefits without constraints on access to data.

Canada

A 2014 report "*Open data: the way of the future*" by the Canadian Standing Committee on Government Operations and Estimates noted that there are few studies that have been conducted to measure the economic impact of having ready access to more information. To provide a sense of the value of open data to the Canadian economy, the committee heard from an author of the McKinsey Global Institute report, Michael Chui, who acknowledged that a rough estimation of the potential impact of releasing open data in Canada (from Government at all levels and from the private sector) would be close to $100 billion, based on the ratio of Canada's GDP to the US' GDP.

Although no studies quantifying the economic benefit of open data in Canada have been identified, Castro and Korte (2015) and Klinkenberg (2003) provide significant discussion of the policy context of open data in Canada. Assessment of the economic benefits of open Government data.

Concluding comments

Consultations with industry experts indicate that the US$3 trillion figure by McKinsey (2013) that could be unlocked globally through open data, is a 'heroic figure' or likely an overestimate, but a worthy starting point for quantifying the global economic impacts of open data.

5.2 Sectoral Advances in Data Sharing

While general data sharing principles across all sectors seem not to exist, there have been useful sectoral initiatives that serve as a basis for sharing between parties. Some examples are shown below:

Automotive industry

The Association of Global Automakers and its member companies recently unveiled auto industry consumer privacy protection principles for vehicle technologies and services (Principles). The Principles acknowledge that the connected car, and the associated technologies and services, involves the collection of data to enhance vehicle safety, improve vehicle performance, comply with environmental requirements, and augment the driving experience. However, with increasing connectivity, automakers maintain that customer privacy must still be a priority. The Principles commit automakers to take certain steps to protect the personal data generated by their vehicles, including the precise geo-location of vehicles or how drivers operate their vehicles.

Agricultural sector

A framework for sharing data covering privacy and security principles of farm data was agreed on November13, 2014. This is the starting point for joint sectoral agreement and opening of data to mutually benefit the agricultural sector.

The recent evolution of precision agriculture and farm data is providing farmers with tools, which can help to increase productivity and profitability. As that technology continues to evolve, the undersigned organisations and companies believe the following data principles should be adopted by each agriculture technology provider (ATP).

It is imperative that an ATP's principles, policies, and practices be consistent with each company's contracts with farmers. The undersigned organisations are committed to ongoing engagement and dialogue regarding this rapidly developing technology.

ATP members include: American Farm Bureau Federation, American Soy Bean Association, Beck's Hybrids Dow, Agro Sciences, LLC, DuPont, Pioneer, John Deere, National Association of Wheat Growers, National Corn Growers Association, National Farmers Union, Raven Industries, The Climate Corporation– a division of Monsanto USA, Rice Federation.

Observation 20: Frameworks for sharing data are proving to be useful in opening usage and value. This is occurring in some sectors and in are in discussion and development at Government level in many countries.

6 REGULATORY AND POLICY

It is evident that significant work on policy and regulation is occurring at the regional level (US and Europe) and at the country level. This is to some extent consistent with the level of Government and industry country and regional activity, see Section 3.

There are a number of consistent profile themes across the active jurisdictions which are summarised in a non-exhaustive list in the table further below.

Below are samples of activities in play:

European Union

The European Union has made the IoT an essential part of its Digital Agenda for Europe 2020, which focuses on applications, research and innovation, and the policy environment.

The European Union has been particularly active in promoting research and innovation:

The Internet of Things European Research Cluster groups together the IoT projects funded by the European research framework programmes, as well as national IoT initiatives.

The requirements of IoT will also be fed into the research on empowering network technologies, like 5G Mobiles. The Future Internet Public Private partnership will develop building blocks useful for IoT applications, while Cloud Computing will provide objects with service and storage resources. On the application side, initiatives like Sensing Enterprise and Factory of the Future help companies use the technology to innovate, while experimental facilities like Future Internet and Research Experimentation (FIRE) are available for large scale testing.

The Digital Single Market (DSM, http://ec.europa.eu/priorities/digital-single-market), adopted in May 2015, leads Europe a step further in accelerating developments on IoT. The DSM consolidates initiatives on security and data protection, which are essential for the adoption of this technology. Most importantly, it announced an initiative on the data economy (free flow of data, allocation of liability, ownership, interoperability, usability and access) and promises to tackle interoperability and standardisation.

United Kingdom

In late 2014, the UK Government chief scientific adviser Sir Mark Walport made several policy recommendations for the UK Government to consider:

The report called for the Government to foster and promote a clear aspiration and vision around the IoT, with the goal of making the UK a world leader in the field, enabling goods to be produced more imaginatively, services to be provided more effectively, and scarce resources to be used more efficiently. Walport said the Government will need to take a leading role in delivering this vision.

The Government should be prepared to take risks and be a lead customer for early-stage IoT projects, and should use its buying power to help define best practice and commission open standards-based, interoperable and secure solutions.

Currently, IoT applications and devices tend to use relatively small amounts of bandwidth, but as more come on-stream this may change. Walport called for the Government to take note that existing networks may not be suitable for millions of sensors

	Policy/Regulatory Context	US	UK	Germany	EU	ITU	Singapore
1.	Spectrum management Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands. Flexible licencing arrangements		Ofcom priority area		Studies for the European Commission have suggested that a licence exempt model is most effective for IoT development, since it avoids the need for contractual negotiations before devices are manufactured and used, allowing the production of large numbers of cheap devices		
2.	Interoperability and Open systems	Numerous Industy bodies – OIC, IIC, SMLC, World IoT Forum					
3.	Network Resilience and Security	The FCC should define its role within the context of an overall cybersecurity framework, dedicating resources and participating in IoT security activities with other government stakeholders	Ofcom priority arrea				
4.	Security and Privacy of Data Security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles. Personal Data privacy and protection	To protect individuals' privacy, the FTC has suggested a set of guidelines covering: 1. Security by Design 2. Data Minimisation 3. Notice and Choice for unexpected uses	Ofcom, priority area. studying how 105A-D of the Communications Act applies to IoT		Article 13a of the European Framework EU rules require organisations processing personal data from IoT systems to carry out security assessments, and make use of relevant security certifications and standards. The EU has a detailed legal framework regulating the public and private sector's use of personal data, with a general Data Protection Directive (95/46/EC) relevant to IoT device manufacturers, social media platforms and app developers that access IoT data; and an e-Privacy Directive (2002/58/EC) also relevant to IoT device manufacturers ARTICLE 29 DATA PROTECTION WORKING PARTY - THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA		

	Policy/Regulatory Context	US	UK	Germany	EU	ITU	Korea	Singapore
5.	Numbering/Roaming Very large address space needed for globally addressable things. – Ipv6 – an IoT enabler	The US government set up a Federal IPv6 Task Force to move all federal agencies from IPv4 to IPv6, with one aim being to encourage the private sector to do the same	Ofcom priority area					
6.	Data Sharing, in particular open government data		Ofcom resnet study Jan, 15 concluded that a common framework that allows consumers easily and transparently to authorise the conditions under which data collected by their devices is used and shared by others will be critical to future development of IoT					
7.	Government/Industry industry sectors leadership	Significant Automotive, Industrial and Agricultural industry focus	Significant IoT investment incentives	Industrie 4.0, leadership in industrial automation		The Alliance for Internet of Things Innovation (AIOTI) was recently initiated by the European Commission in order to develop and support the dialogue and interaction among the Internet of Things (IoT) various players. The overall goal of the establishment of the AIOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT. The AIOTI will assist the European Commission in the preparation of future IoT research as well as innovation and standardisation policies.	Korean Telecommunications Strategy Council has been given responsibility to adapt existing laws and regulations to ensure a liberal and competitive industrial environment for IoT.	IDA – smart cities initiative

requiring low power to communicate a lot of very small data packets, and suggested the creation of a national lower-power wide area network (WAN) to supplement existing and future fibre networks. With this in mind, Walport said the Government would need to develop a roadmap for IoT infrastructure with the aim of avoiding independent, fragmented and partial networks, damaging connectivity and resilience, and could consider selling licensed spectrum space to accommodate it.

If the IoT is to flourish, interoperability and open standards must be key considerations, said Walport, to guard against cybercrime and other security threats, and support

energy efficiency. The Government should take a proactive role in driving this development.

Walport said the Government should foster a greater range of skills to support the development of the IoT, from well-trained installers to system architects and research scientists. Walport urged the Government to implement more study of algorithms in the computer-programming curriculum, and to adjust the maths curriculum to build an emphasis on using calculation to solve problems.

It recommended the Government:

- mandate that public bodies and regulated industries publish reliable machine-readable data through open-application programming interfaces, subject to data protection safeguards to foster more innovation.
- address the need for legislative change to address new challenges that may arise, such as the protection of personal data, or who is at fault in a car crash involving driverless, connected vehicles.
- work hard from the outset along with the Centre for Protection of National Infrastructure (CPNI) and the Communications and Electronics Security Group (CESG) to establish 'security-by-default' on the IoT, and must play a lead role in the inevitable public debate over trust and security. It should also expand digital inclusion programmes to ensure the IoT does not widen the digital divide in the UK.
- create an IoT advisory board made up of private and public sector organisations, including bodies such as Tech City and the Digital Catapult, to foster a deeper culture of collaboration between Government and industry and 'maximise the efficiency and effectiveness' of the IoT.

Different types of IoT applications are likely to have different spectrum requirements. "We have a duty to ensure the optimal use of radio spectrum. The appropriate management of scarce resource that underpins the wireless and mobile services on which many citizens depend is critical for promoting investment and innovation in the IoT business. This includes exploring new sources of spectrum demand and how to best meet this demand to deliver benefits to citizens.

The IoT was identified as a priority area in our recently published Spectrum Management Strategy. In addition, our recent statement on spectrum sharing for mobile and wireless data services noted the views of many stakeholders that making additional spectrum available on a shared basis might benefit the development of the IoT."[11]

US – Federal Trade Commission

The Federal Trade Commission (FTC) held a workshop in November 2014 to explore consumer privacy and security issues posed by IoT. The FTC has made it a priority to bring enforcement cases against deceptive business practices in the IoT.

US – Federal Communications Commission

At the Federal Communications Commission, the Technological Advisory Council (a group of academic and industry experts appointed by the FCC Chairman) is studying issues surrounding how the IoT will affect communications networks in the next 10 to 20

[11]Ofcom – Promoting Innovation and Investment in Internet of Things – Oct 2014

years. In December 2014, the IoT Working Group made the following recommendations to the Technological Advisory Council (TAC):

- The FCC should programmatically monitor consumer IoT network traffic impact on WLAN and WWAN with a focus on new high bandwidth consuming applications.
- The FCC should focus on availability of unlicensed spectrum suitable to a range of PAN/WLAN services without making spectrum allocations unique to IoT, and ensure there is enough short-range spectrum to meet growth in PAN/WLAN requirements and sufficient network capacity upstream from IoT devices and proxies.
- The FCC should define its role within the context of an overall cyber security framework, dedicating resources and participating in IoT security activities with other Government stakeholders.
- The FCC (in collaboration with other agencies) should conduct a consumer awareness campaign related to IoT security and privacy.
- The FCC should conduct internal periodic scenario exercises to determine appropriate response to widespread consumer events related to the IoT.

Observation 21: IoT policy areas under review or development coalesce around a few areas, which are: spectrum management, personal privacy, use of IPv6, network resilience and security, open Government data, interoperability and national innovation and competitiveness.

7 AUSTRALIAN POLICY AND REGULATION CHALLENGES

7.1 Potential Economic Impact of IoT in Australia

The McKinsey Global Institute (MGI) has published a comprehensive assessment of the potential for IoT called "The internet of Things: Mapping the Value Beyond the Hype", putting an upper limit on its potential global economic impact by 2025 of $US11.1 trillion, or about 11% of the World Bank's estimate of value of the world economy by that time.

It examines the impact of IoT across nine environments: homes, offices, factories, worksites (mining, oil and gas, and construction), retail environments, cities, vehicles, and the outdoors and includes a 'human' setting for systems that attach to the human body and enable such health and wellness applications as monitoring chronic disease or exercise, and productivity-enhancing applications such as use of augmented-reality technology to guide workers in performing complex physical tasks.

The study does not give any estimate of the economic impact of IoT today, but if it is to achieve an impact even at the lower end of MGI's estimates ($3.9T) in just 10 years, its impact will be enormous and the disruption created will be widespread.

The figure below has taken the MGI global diagram and estimated the impact on Australia based on our global contribution to GDP of about 1.15% and then some juggling to align to our relative strengths and weaknesses. This by its nature cannot be very accurate but it serves to show an order of magnitude. Noteworthy also is the absence of agriculture in this diagram and we have included this into 'factories' as we feel this will be a significant contributor by 2025.

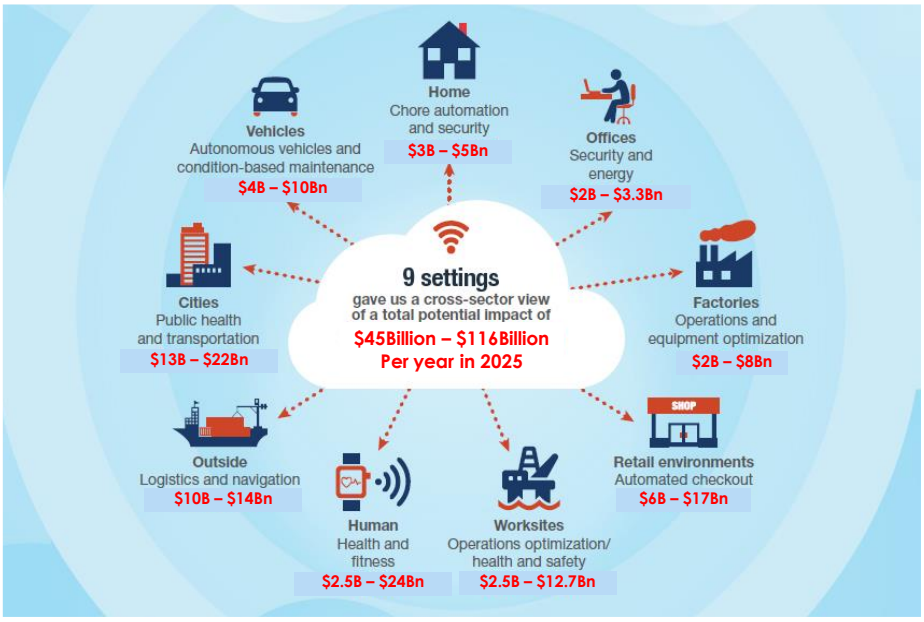


Figure 29: High level estimate of Australian economic impact of IoT

Consumers may have the most to gain; perhaps years of life from IoT enabled preventative health applications and safer transportation, greater convenience and time savings, and less costly goods and services as well as healthier food and environment. These are even harder to quantify but nonetheless significant.

Cisco describes a global contribution from the Internet of Everything (IoE) by 2022 as about $14.4Trillion. This translates to an Australian impact of about $165 billion. Although different from the MGI view it is of the same order of magnitude and in either case the impact is very significant indeed.

Observation 22: A potentially realisable $100 billion economic impact of the IoT on the Australian economy by 2025 is worthy of a considered national IoT strategy and focus.

7.2 Industry View – Key Australian IoT Themes and Challenges

Key themes and challenges that have come out of the IoT Think Tank public workshops, interviews with over 30 companies and Government departments are summarised in the following figure.

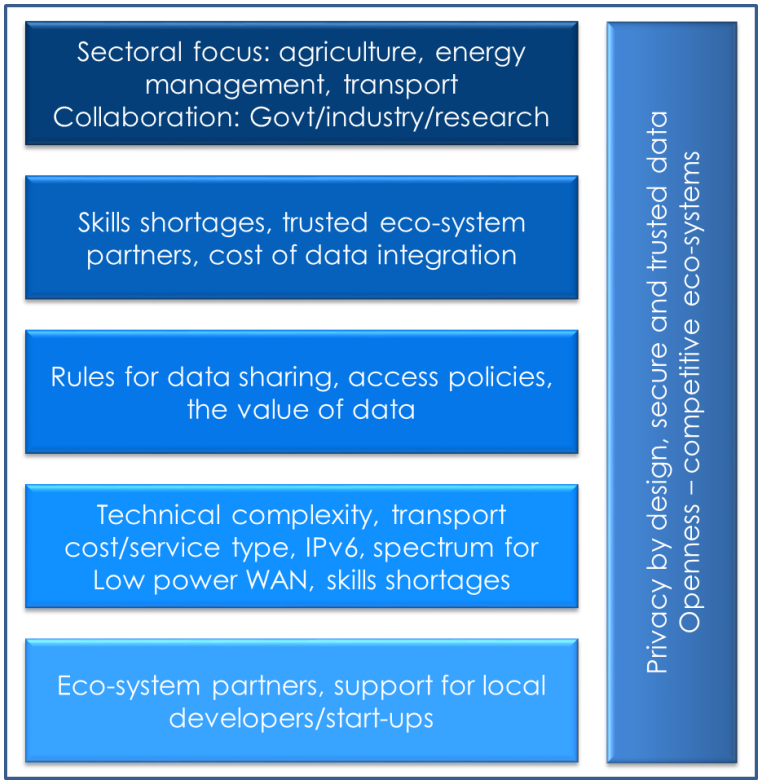


Figure 30: Emerging key themes in an Australian context

The issues summarised here are captured in our observations and recommendations throughout the document.

7.3 Australian Capability and Potential IoT Eco-System Players

Australia has many important building blocks and pockets of excellence that can contribute and even lead in key industry and market sectors.

These include:

- An increasingly ubiquitous national broadband network
- High penetration of 2G/3G and 4G mobile network coverage
- Strong industry vertical markets, such as in mining, agriculture, finance etc.
- A highly skilled and productive research sector
- Pockets of excellence, e.g. in robotics

- Instances of IoT activity and collaborative innovation centres

The potential Australian IoT eco-system is rich with capable players at all layers of the IoT landscape. The following diagram is an attempt to show a small number of the active players. It is in no way trying to show all the action as this would not be possible.

It serves to illustrate how players are distributed across the eco-system. In many cases, players cover more than one layer and this has also not been reflected. This gets more difficult at the services layer because almost every service provider in every industry gathers information that is used in some way to serve their clients. In the digital economy this will expand to every business.

Observation 23: IoT solutions are derived from collaborations across all the layers of our model. Partnering and collaboration will be critical for IoT innovation in Australia.

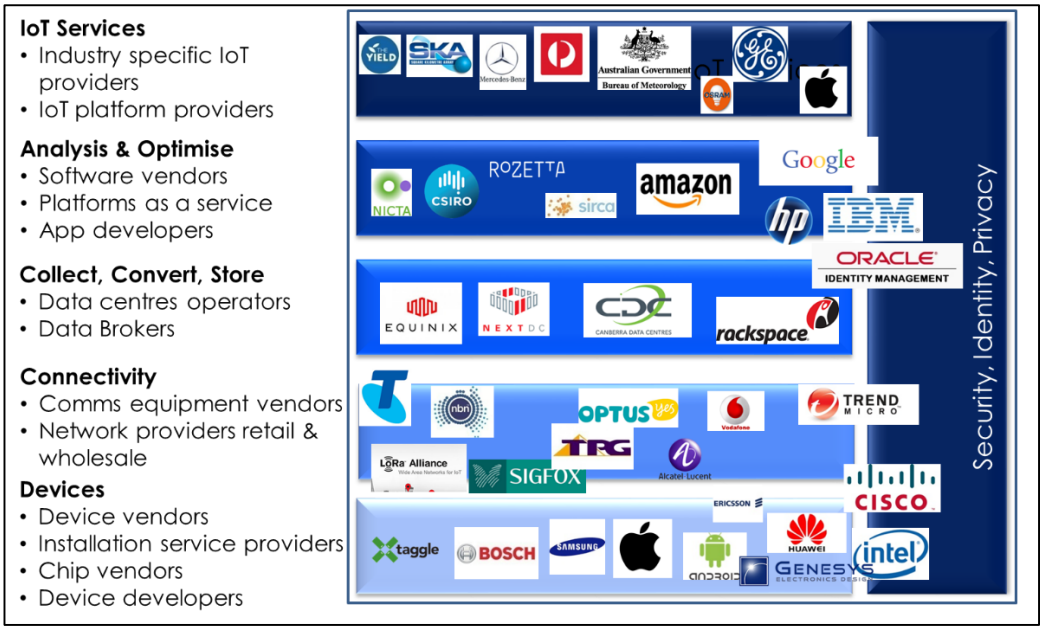


Figure 31: IoT reference model and some players

From a telecommunications perspective, every fixed and mobile service provider is a part of the IoT eco-system and every electronics and computer player is in the eco-system. Every software company and every app developer too.

There are a few significant multi-nationally-led IoT collaboration initiatives that are emerging and are contributing to the general evolution of the IoT industry in Australia.

One example of this is Cisco's IoEInnovation Centre program. Another is the Knowledge Economy Institute evolving from Sirca/Rozetta and other partners in a new eco-system. See Appendix D for further details and an additional sample of local Australian collaborative initiatives, bodies that are aligned to support IoT and some Australian IoT capability.

Bosch

Bosch's global business is operated as four groups. Mobility, At Home, Industry and Trade and Software Solutions. The four addressed sectors are mobility, energy, consumer and industrial technologies. In Australia they have significant engineering and manufacturing capabilities.

Bosch describes IoT as the next tsunami of disruption. In 2010 it made a corporate decision to make all their products/services network connectable across the entire portfolio from consumer goods and tools to major industrial and transport solutions. Today this is delivering new data and analytics based services, products and capabilities.

Refer to www.bosch.com.au to explore the extensive range of solutions which is as diverse as tracking a tradesman's tools through to expectations of every vehicle being connected by 2020. Bosch is also a major supplier of sensors with about 60% of the global smartphone sensor business. It has recently begun investing in data analytics businesses as it sees major opportunities emerging from the 'connecting everything' model. So clearly open data, security and privacy models are very important and still emerging for widespread applications.

In terms of sensor connectivity, Bosch sees great opportunities in the agriculture sector specifically in Australia and is looking at LoRa and 6LowPan as connectivity models for farm/wider area based sensors. Environmental sensing is on its radar, with collaboration underway with the Knowledge Economy Institute.

Observation 24: Notwithstanding laudable individual company initiatives and some standout IoT pilots, there is an evident lack of coordinated, persistent industry and /or Government focus on IoT.

7.4 Sectoral Activity and Focus

Harnessing the IoT capability of Australian industry and Government for the benefit of the economy will require focus for best results. This premise is supported by observations of early success overseas in specific sectors in many countries we consider our peers and key partners. Where to focus should depend on some key criteria including:

- Net benefit to the economy
- Priority sectors
  - where efficiencies and new business models are recognised
  - where there is an industry willingness to take a lead
  - where there is positive Government alignment
- Ability to leverage and build on local capability and existing strengths
- Where IoT focus can give Australian industry a competitive advantage and also export potential
- Where barriers to entry can readily be overcome

Below is a view of which industry sectors should receive priority focus which has been derived from recent IoT Think Tank workshops, extensive industry interviews and a market survey.

The top five sectors identified for local economic benefit in order were;

- Transport
- Agriculture
- Energy management
- Smart cities
- Health

The top five sectors identified for international impact as potential export in order were;

- Agriculture
- Mining

- Health
- Transport
- Smart cities

Agriculture

Agriculture is almost universally agreed to be one of the sectors where Australia can take a lead.

"By 2050 we will need to double the amount of food produced to feed the world's growing population whilst at the same time having access to less land, half the amount of fresh water, increasingly expensive fertilizer and unprecedented changes in climate. Technology, particularly the IoT, is seen as a potential solution to this urgent challenge. As a member of the KEI Centre, our aim is to combine Australia's strengths in agriculture with technology innovation, to make Australia the epicentre for IoT R&D in agriculture." (Ros Harvey, Founding CEO of The Yield, previously Sense-T Program Director at UTAS, driving a major initiative in IoT in agriculture.)

Mining

It is evident that our two largest mining companies are funding impressive and in some cases world-leading internal IoT initiatives. These are relatively sporadic though and not reflected at the next tier.

General Electric believe there is considerable potential both within the industry and for export yet to be exploited.

Energy management

There seems massive scope for efficiencies in the management of energy peak load (the largest cost driver of the industry), better distribution and user generated and managed power generation.

Recent federal legislation mandating a single meter for multiple distributers is a simple and sensible approach, and may ultimately be a transformative catalyst for better IoT applications in the space.

Smart cities

While noting that Australian State Government organisations have placed their ICT strategies centrally within their service transformation roadmaps, IDC says their progress varies, with Queensland, Victoria, and New South Wales leading the race in terms of transformation maturity and strategic agility.

According to Accenture, Smart city investments are developing in Australia, although at a slower pace compared to peer Asia/Pacific cities, and these investments will be an increasingly important way to manage operational efficiencies while delivering improved service capability. In our region Singapore stands out as an early mover.

Australia is lagging behind many nations in the application of IoT to both smart homes and smart cities, and leadership needs to come from the Government, says Frost & Sullivan. The research company is preparing to publish, later this year (2015), separate reports on smart cities and smart homes and according to Audrey William, head of research for the ICT Practice in ANZ, the company's research has shown Australia to well behind on both counts.

Observation 25: The development of smart city plans and deployment in Australia is apparently lagging behind the rest of the world. Anecdotally, smart cities seem bedevilled by governance issues across local, departmental, state and federal jurisdictions. This makes the necessary collaboration complex and often unwieldy.

A good example of good state and local Government collaboration is to be found in Adelaide. The State Government and Adelaide City Council have entered into an MoU with Cisco to create a smarter, more connected city through a number of pilot projects. Currently, two pilot projects – Smart Lighting and Smart Parking – are in the process of being implemented by the Adelaide City Council. Further pilot project opportunities are being considered. Also refer to Appendix E10.

Transport (and logistics)

As a key subset of smart cities infrastructure, and importantly with advances made and ongoing challenges to be overcome across Australia's vast distances, transport and logistics looms as a sector where major efficiencies can be realised in Australia (a great example are the massive driverless trains transporting ore from the mines). There is massive opportunity for 'value-adding' our produce through logistics tracking and 'proof of source'.

Health

According to Frost &Sullivan, much like most evolving markets, in Australia eHealth is still at its infant stage and its full potential in addressing some of the major care delivery challenges is yet to be realised. And, while the study finds that clinical use of eHealth continues to be fraught with challenges in adoption, it does reveal that the greatest concern is about the management of eHealth generated data because there are still gaps in regulations governing data ownership and privacy.

"Moreover, physicians tend to question some of the claims made by eHealth companies and need a federal stamp before they consider clinical uses. In the absence of proven clinical applications, eHealth vendors find it challenging to design a sustainable business model because the big question of who pays for the offering remains unanswered." (Frost & Sullivan)

Observation 26: Gaps in regulations governing data ownership and privacy, as well as service trust are significant barriers to overcome for eHealth in Australia.

This evolution of digitally enabled business models may see even our most basic market segmentation models change. Preventative health may not be part of the medical treatment segment. The treatment of chronic disease may be funded quite differently compared with the prevention models for improved quality of life for the elderly. With perhaps more connection with lifestyle, exercise and food rather than medicine. Preventative medicine may be driven through innovation from genetic analytics enabled by digital representations of every individual's genetic data enabling targeted therapies and treatments. Nobody can predict how this might play out over the coming decades but there is little doubt that it will dramatically change the current health sector.

Observation 27. Preventative health is a major beneficiary of many IoT based solutions and this could greatly reduce healthcare costs overall.

As we consider Australia's traditional strengths and challenges, the opportunity for cost efficiencies and the barriers to entry, there a three sectors that stand out as most likely to transition to an IoT enabled global leadership position.

The three sectors are: mining and resources, food and agribusiness possibly including the environment, and transport and logistics.

Observation 28: Mining and resources, food and agribusiness, and transport and logistics appear to be sectors where Australia can make a significant global contribution.

7.5 Alignment between Government and Industry in Key Sectors

Collaboration and alignment, where sensible, will be key in advancing IoT progress in key sectors. Some important Government and industry entities that may help in this process are identified below:

7.5.1 Australian Industry Growth Centres

The Industry Growth Centres Initiative (the Initiative) is the centrepiece of the Government's new industry policy direction and part of the Industry Innovation and Competitiveness Agenda. Its goal is to lift competitiveness and productivity by focusing on areas of competitive strength. This is designed to help Australia transition into smart, high value and export focused industries.

The federal Government has chosen five Growth Centres represented in the following diagram.

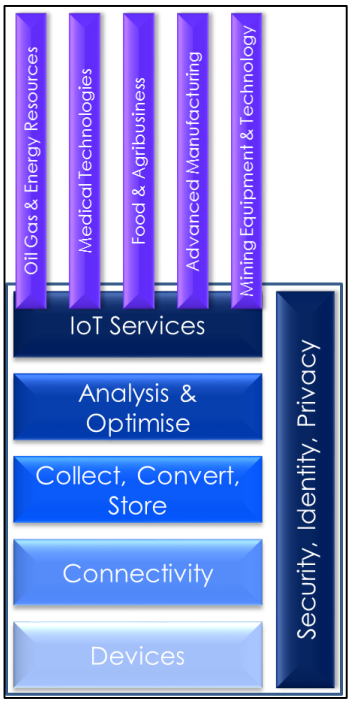


Figure 32 The Federal Government's Industry Growth Centres

The Initiative is intended to enable national action on key issues such as deregulation, skills, collaboration and commercialisation. It will drive excellence, not dependence and create an economy that ensures Australia's ongoing prosperity.

The Initiative is ongoing with $225 million in Australian Government funding over the four years from 2015/16 to 2018/19. Industry Growth Centres are being established to deliver the Initiative in five growth sectors in which Australia already has a competitive advantage, these are:

- Advanced manufacturing;
- Food and agribusiness;
- Medical technologies and pharmaceuticals;
- Mining equipment, technology and services; and
- Oil, gas and energy resources.

The Growth Centres will also facilitate engagements between enabling services and technologies, such as information and communications technology where they provide essential and direct support to the growth sectors.

Observation 29: The federal Government's Industry Growth Centre strategy offers an opportunity to leverage IoT innovation and to align sectoral activities.

7.5.2 The National Infrastructure

Infrastructure Australia

Infrastructure Australia is an independent statutory body with a mandate to prioritise and progress nationally significant infrastructure.

It provides research and advice to Governments and the community on the projects and reforms Australia requires to fill infrastructure gaps.

Its recent Infrastructure Australia Audit, published in 22 May 2015, focusses on four key national infrastructures:

- Transport
- Energy
- Telecommunications
- Water

The audit identifies key infrastructure challenges for the above being:

- Transport – congestion is the dominant challenge in cities and infrastructure networks.
- Energy – the energy sector will need to focus on efficiency and environmental impact.
- Water – the water sector needs reforms to address quality, reliability and supply issues.
- Telecommunications – the telecommunications sector's economic contribution will be best served by continuing support for effective competition.

The report, however, fails to identify IoT as introducing major infrastructure innovation for the telecommunications sector and creating a key enabler for all of the above infrastructure challenges.

Observation 30: Infrastructure Australia appears to have overlooked IoT as a significant innovation for the telecommunications infrastructure and is missing the opportunity to use IoT to address the major challenges in transport, energy and water.

House of Representatives Parliamentary Inquiry into "The role of smarter IT in design and planning for infrastructure"

The Standing Committee on Infrastructure and Communications has commenced an inquiry specifically to look at how smarter IT (in effect IoT) can or should be used to build better national infrastructure. While findings are yet to be made, there appears an overwhelming view from the more than 40 submissions to date that smarter IT can have a significant productivity effect for the management of Transport, Energy and Water.

It is to be hoped the inquiry supports some of the recommendations from the submitters which include:

- Harmonisation of data formats
- Proactive use of smarter ICT in Government planning and procurement
- Better Government collaboration
- Road-testing smarter IT innovation

Many of the recommendations align with recommendations of this Report and hopefully can be acted upon to help build IoT into the fabric of our infrastructure productivity plans.

Australian Competition and Consumer Commission (ACCC) Infrastructure Consultative Committee

The ACCC's Infrastructure Consultative Committee (ICC) was set up in 2006 to facilitate discussions on the broad issues of infrastructure and infrastructure regulation. The committee was selected to be representative of the diversity of infrastructure interests and includes representatives from energy, telecommunication, water, rail, ports, and airports.

The committee is an important mechanism for the ACCC to gain feedback from stakeholders in the infrastructure sector. Operational issues and the specifics of decisions that are before the ACCC and Australian Energy Regulator (AER) are not the focus of this committee. Rather, the emphasis is on issues in the practice of regulation that cross the different infrastructure sectors.

The committee also commissions research studies. One major work that was commissioned was a major benchmarking study of regulatory practices and processes used in the economic regulation of seven key infrastructure and network industries in 11 OECD benchmark countries and the European Union. This study is divided between a final report and detailed country-based studies that are provided as an appendix to the report. This work is being updated by the ACCC.

The ACCC ICC current membership is:

- Association of Australian Ports & Marine Authorities
- Australian Airports Association
- Australian Pipeline industry Association
- Australasian Railway Association
- Australian Communications Consumer Action Network
- Australian Water Association
- Board of Airlines Association of Australia
- Communications Alliance
- Competitive Carriers' Coalition
- Energy Networks Association
- Energy Users Association

- Grid Australia
- Infrastructure Australia
- Infrastructure Partnerships Australia
- Macquarie Capital Advisers
- nbn
- Sing Tel Optus
- Standard & Poor's (Australia)
- Telstra
- Water Services Association of Australia

Observation 31: Building smarter and more productive infrastructure in Australia, will require IoT technologies, and moreover collaboration between the key industry and Government organs, including Infrastructure Australia, the ACCC iCC, Departments of Industry and Communications etc.

7.6 Support for Innovation – Start-Ups

Innovation needs and demands start-up mentality to be disruptive, break old business models, and find new ways. IoT represents a huge opportunity to tie start-ups, research and business opportunity.

There is considerable industry recognition of the importance of start-ups as triggers for innovation to occur.

Observation 32: Australian competitive advantage and IoT leadership will require a thriving IoT start-up community, supported by a wider IoT eco-system. Conversely huge market potential for IoT offers significant opportunity for start-ups.

However, Australia's history to date in transitioning evident research leadership into start-up entrepreneurship and innovation has been relatively poor.

The Federal Government's 'Accelerating Commercialisation' program is up and running again. The program encourages and assists small and medium businesses, entrepreneurs and researchers to commercialise novel products, processes and services. It works by providing expert guidance and connections through commercialisation advisers to help find the right commercialisation solutions for novel product, process or service. This may include matched funding to support commercialisation activities. Accelerating Commercialisation comprises the following activities:

- Commercialisation guidance
- Accelerating Commercialisation Grants
- Portfolio services

An important feature of Accelerating Commercialisation is the construction of a portfolio of Australian businesses that are undertaking early stage commercialisation activities. The portfolio brings qualified early stage commercialisation opportunities together in one place so that they are visible to investors, other entrepreneurs, domain experts, supply chains and strategic corporations.

Details of more than 200 Australian businesses who are already qualified members of the portfolio can be found at http://www.business.gov.au/advice-and-support/EIP/Accelerating-Commercialisation/Pages/AC-The-Portfolio.aspx.

7.7 Open Data/Principles for Data Sharing

An estimation of the size of the economic benefit of open data in Australia has been undertaken by Gruen, Houghton and Tooth (2014) with a view to illustrating the potential for open data to contribute to the Group of 20s (G20) growth target of 2% agreed during the G20 finance ministers and central bank governors meeting in Sydney in February 2014. They estimate the current aggregate direct and indirect value of Government data in Australia at up to $25 billion per annum.

The authors argue that open Government data is important because it could contribute half of the G20s 2% growth target in Australia but more importantly, unlike most micro-economic reforms, there are minimal 'losers' from the policy. In Australia, Governments have opened many data sets. For example the Federal Government runs www.data.gov.au, NSW runs www.data.nsw.gov.au, Queensland runs www.data.qld.gov.au, and the ACT runs www.data.act.gov.au and so on. Furthermore www.govpond.org is a tool that searches across the federal and state sites for open data. There are currently 3,600 data sets available. The Atlas of Living Australia is also a substantial resource (www.ala.org.au).

Using the McKinsey Global Institute Study, Gruen et al. (2014) estimate that, given the relative size of the Australian economy, the total potential of open data to Australia is around $64 billion per annum. This estimation is of output rather than value added and includes business data as well as Government data. From a policy perspective, Gruen et al. find that by reinvigorating open data policies, there would be a contribution to Australia's cumulative GDP growth of $16 billion per annum or around 1% of GDP over the next five years.

The following figure represents characterisation of four classes of data, ranging from completely private or 'anonymized' through to completely open as described above. It is the intermediate two categories that offer an enormous opportunity to monetize the data and together with fully open data provides a massive resource that is critical for realising the full potential of IoT.

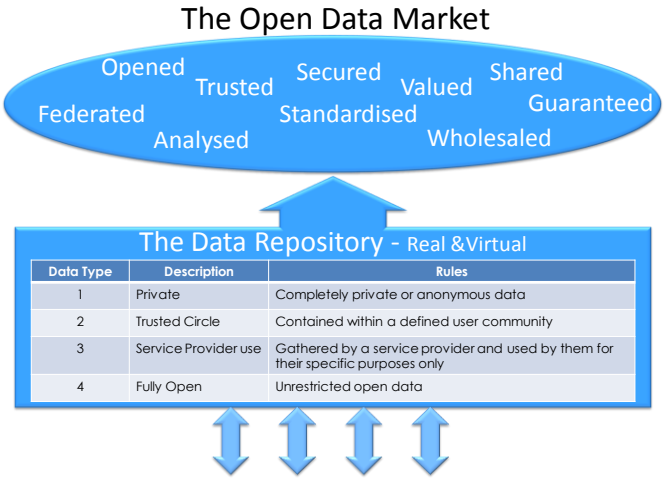


Figure 33: An open data market approach

Access to open Government data is a major enabler for IoT and for industry. The Federal Government Open Data Program may offer a mechanism for wider accelerating sharing of Government data. In the meantime individual jurisdictions such as Brisbane City Council seem to be taking the initiative in opening data.

Observation 33: "By reinvigorating open data policies, there would be a contribution to Australia's cumulative GDP growth of $16 billion per annum or around 1% of GDP over the next five years". Australia could take the lead in opening up data sets and enabling sharing which can underpin IoT acceleration.

From NICTA's submission to the parliamentary inquiry in "The Role of smarter ICT in the design and planning of infrastructure", the following example is a high profile instance where the development of a national map has opened value and productivity.

Example: Open data and flexible models boost productivity: National Map and Terria Analytics

Working for the Australian Department of Communications and working closely with partner Geoscience Australia, NICTA's Terria team developed the software for the National Map initiative (www.nationalmap.gov.au), placing government spatial data, which was previously difficult to access, into the hands of community, software developers and industry. The sort of searchable data that is available is varied and includes data about broadband coverage, location of surface water and waste management facilities, infrastructure developments such as gas lines, and electoral boundaries.

This initiative is acting as a key enabler of innovation to boost government and industry productivity, prompting new business and providing better services to the community. The National Map website also acts as an incentive to government to release more data, in a searchable and reusable format, into the community. This platform saves departments reinventing the same tools and also allows the whole community to see a single view of all the infrastructure and resources in any location. The long-term productivity benefits will be substantial.

Terria™ has developed a suite of web-based analytics tools to extract insight and make probabilistic predictions using data in a web-based mapping environment. These tools are built from state of the art machine learning algorithms designed specifically for large-scale spatial inference.

Within the Government there is a number of departments addressing aspects of open data, including policy, making data sets available and providing open data sharing services:

- The Digital Productivity Division of the Department of Communications has done significant work on making spatial data available
- The Department of Prime Minister and Cabinet has a Public Data Management project
- The Department of Finance is releasing Government data sets

Trusted Data storage/exchange

The notion of a data repository has been discussed and is gaining traction but it is important to understand that this is not a centralised database. It may well be a centralised clearing house or trading function through federating data from perhaps many sources. The challenge is to consider who one would trust to enforce policy, protect and open your data? If it is possible to establish a trusted data repository, this may become a critical enabler for many new business models. Perhaps a model a little like the Australian Stock Exchange could work. Policy and regulation would be necessary to regulate such an entity so that trust and guarantees etc. can be valued and monetised.

7.8 Technical Challenges

Our interviews and survey have provided some insight into the issues that the current players see as important. These issues are:

7.8.1 Complexity of Technology Choices/Architectures and Standards Involvement in Australia.

While it makes little sense for Australia to develop its own standards, given the plethora of alternatives, the question of what level of Australian participation and oversight is needed may need to be considered.

7.8.2 The Need for Wider Broadband Network Access via the NBN and Others

The NBN will, over time, facilitate broadband access to all Australian premises. This is a significant connectivity resource but not sufficient for many places that IoT will need to penetrate.

Network access will be needed in more places than existing homes and businesses. There will be a need for connection points in more diverse locations including lamp posts, traffic controllers and bus shelters including via wireless network extensions.

It will be important to consider opportunities that may arise from fixed/wireless and connections to such 'non-premises' locations.

Observation 34: The NBN may need to be connected to locations that today are not described as premises such as traffic controllers, lamp posts, bus shelters etc. for IoT applications. Providing such access may also be an opportunity for other service providers.

7.8.3 Opportunity for Lower Cost Narrowband Wireless IoT Connectivity

Existing network fixed and Mobile services are sufficient for a number of IoT applications, as is evidenced by a steadily growing M2M market e.g. the recent Telstra success with the Australian Rail Track Corporation (ARTC).

The business case for wider spread IoT however depends on significant lower costs per bit and lower power consumption IoT devices. In Australia, there are some early and small deployments of such networking, e.g. by Taggle for low cost meter reading. There is also a longer term promise in the advent of 5G technologies, due for deployment from around 2020.

Lower power wide area wireless technologies wifi, LoRa, Bluetooth are examples technologies available today that provide the opportunity to kick-start cost effective IoT business models e.g. as promoted by the recently announced National Narrowband Network in Australia, with a forecast trial in North Ryde (Sydney) later in 2015.

As an incremental offering, lower cost tariffs for narrowband IoT services, such as for metering, could also be an opportunity for existing service providers as add-on low tariffs on existing wireless and broadband connectivity.

Observation 35: Lower cost connectivity is essential to many IoT business cases, for low bit rate IoT services, such as metering. There is significant opportunity in Australia for low cost services to be enabled in Australia, through new low power wide area wireless technologies and services and/or by innovative lower tariffs for low-bit rate services on existing service platforms.

7.8.4 IPv6 to Become the IoT Default

A fundamental enabler is IPv6 as it adds a major component of networking simplicity. However, Australia is not yet setting IPv6 as the default.

Recent statistics, revealed at the 2nd IoT Think Tank workshop on 20 August by Mike Biber, regarding IPv6 penetration in Australia show IPv6 adoption to be significantly lower in Australia compared with the rest of the world, despite the capability to do so already exists with many or even most service providers.

Observation 36: IPv6 is a major enabler of IoT. Australia's adoption of IPv6 is poor compared to a number of our major peers. 1.44% versus 21.7% US, 18.1% Germany, world average approx. 7.6%. (Source Google IPv6 statistics).

7.8.5 Spectrum Management

Current licensing of spectrum, apparatus and class may not provide the right environment for the multitude of low cost wireless sensors that need some level of protection (i.e. not class licensed) from interference but not requiring sole use spectrum (i.e. expensive spectrum or apparatus licence).

One idea might be 'shared spectrum parks' for agreed device types/characteristics managed by a 'park managers' under the governance of the ACMA.

Along with this idea would be an 'ACMA spectrum play area' where innovators could trial IoT applications with assurance that if adopted for application/commercialisation, the ACMA would designate a 'shared park'.

Here in Australia the company Taggle is facing this dilemma at the moment as is the 'electricity meter' industry in finding 'free' class licensed spectrum that is not subject to interference while exclusive spectrum is too expensive and too complex to achieve; e.g. finding a third party to put up the cash such as www.lora-alliance.org in the USA.

There is no single right answer. Rather, there will be the right answer for a specific business model and technical scenario and the challenge for the ICT industry is to provide the right advice and share the right information so that sound decisions can be made in every other sector of the market. If we can achieve this then innovation will thrive, not only within every sector but across sectors as cross-sector innovation becomes more important in the digital economy.

Suggested LPWA connectivity solutions which provide a cost effective for low bit rate sensors, such as the National Narrowband Network, or from rival SIGFOX, are also not readily accommodated, at scale.

The ACMA is already considering the future needs of spectrum in the context of IoT and have made the following observations:

- A mix of spectrum solutions may be required including access to:
    - Licensed spectrum, as well as
    - Class/unlicensed spectrum
- Existing spectrum options are numerous and it is unlikely there is a one size fits all approach. Different applications may require access to spectrum with different characteristics. For example:
    - Existing class-licensed low interference potential device bands
    - Existing fixed link options
    - Existing cellular/mobile broadband options
- ACMA has identified future options to support machine-to-machine communications and IoT applications including:
    - Intelligent Transport System applications in 5.8 GHz
    - Low power, low duty cycle, wide area extension available in the 900 MHz band

- Planning for 5G technologies that are expected to support IoT

Observation 37: The challenge of the Australian IoT industry is to inform, share and drive the timely allocation of spectrum and spectrum usage models, through ACMA, to support a thriving and innovative IoT market.

7.8.6 Network Neutrality

Network Neutrality is a regulatory risk issue for the IoT eco-system development in that it could be a source of regulatory disputation between regulated telecommunications providers and non-regulated IoT providers.

Network neutrality is based on the principle of an 'open internet' where every service or digital stream over the internet is treated equally to prevent possible abuse of market power by telecommunications providers and service providers. In the United States in particular the issue has produced extensive public debate and the FCC has made a rule to regulate internet service providers to prevent market abuse. Europe has also had a debate on network neutrality but has not gone as far as the US in regulatory intervention. Essentially the debate is whether the internet, the source of so much innovation needs a 'special form of regulatory intervention' in addition to more common anti-competition measures to prevent possible market abuse.

Examples such as network providers blocking services by other providers are clearly anti-competitive, but pricing for levels of internet network service to 'manage' network congestion are more controversial. There has been relatively little debate in Australia about whether there is a need for network neutrality regulatory intervention.

In relation to the development of the IoT eco-system, telecommunication network providers have clearly indicated their plans to be major players in the IoT eco-system and have extensive network infrastructure to support future IoT services but at a cost that might be higher than non-network providers. However, telecommunications providers could 'bundle' IoT services with other services to both be able to provide low cost IoT services and differentiate between providers.

Observation 38: Given the potential fast pace of future innovative IoT services, it will be important that ACCC is vigilant to prevent 'possible' market abuse of network neutrality in providing and bundling IoT services

7.9 Trust and Security

Consumer security/data privacy

Consumer privacy has been raised many times as a concern in Australia as it has been overseas. By adopting classes of data for sharing (see above) IoT innovations especially for non-private classes can be enabled more confidently.

Separate consideration for IoT privacy will be essential in Australia. Issues will include:

- Applicability of privacy protections across borders (for increasingly borderless services e.g. Apple Health).
- Benefits/pitfalls of alignment with overseas privacy regimes.
- Suitability of existing laws for covering IoT privacy
- Notice and choice for unexpected use of data

Network resilience and service security

As the IoT develops and encompasses an increasing number of services on which citizens and consumers come to rely, it will become increasingly important to ensure that the networks delivering these services are robust and the data delivered over them is secure. This creates particular challenges as the traditional security approaches used in telecommunications may not be applicable in the high volume, low cost devices likely to be used by many IoT services. (Ofcom)

A similar view to Ofcom's is held here in Australia. Indeed as IoT services extend to more critical infrastructures (e.g. management of energy and water resources) and health (automatic dispensing of drugs, etc.), for example existing standards and guidelines for telecoms networks resilience and performance may need to be augmented for particular verticals and service types.

Observation 39: Trust and security will be vital to build IoT service confidence and underpin growth. On the other hand, there is also a risk that failure to address security concerns early on or by applying onerous security restrictions as an afterthought can significantly inhibit the deployment of IoT services.

Government security and surveillance requirements

The Australian Government collects and receives information to fulfil its functions and expects all those who access or hold this information to protect it. Agencies are to develop, document, implement and review appropriate security measures to protect this information from unauthorised use or accidental modification, loss or release by:

- Establishing an appropriate information security culture within the agency;
- Implementing security measures that match the information's value, classification and sensitivity; and
- Adhering to all legal requirements.

The mandatory requirements of this core policy are based on the three elements of information security:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods; and
- Availability: ensuring that authorised users have access to information and associated assets when required.

Observation 40: Government law enforcement regulations regarding telecoms are already becoming onerous and an additional cost burden and inhibitor for certain service types. As IoT becomes more pervasive this overhead may become an increasing burden and inhibitor.

Action in Australia

As was outlined in Section 4.9, some work on models and architectures has begun, and can be expected to develop. However, there would be benefit in Workstream 5 dealing with Security (see Section 8.4) reviewing the current literature and developing a draft working model of security based on the best of current approaches which allows the security of current and future IoT devices and systems to be discussed in common terms.

To that effect, CA could usefully establish dialogue with both the Online Trust Alliance and the Cloud Security Alliance.

For the health sector, David Lake's paper on an eHealth IoT architectural framework, providing a sector specific perspective of how security could be architected, could usefully apply the to a case study in Australia.

There may also be value in producing a handbook on testing IoT security which promotes the OWASP IoT Top 10 as a common standard, and provides guidance in the form of an IoT cybersecurity health check.

7.10 Skill Shortages

7.10.1 100,000 ICT Workers Shortfall by 2020

A 2015 study by Deloitte Access Economics revealed that Australia will need an extra 100,000 information and communications technology workers by the end of the decade. Employment in the ICT sector is expected to grow by 2.5% per year until 2020, higher than the economy at 1.6%.

When exploring challenges specific to the IoT, IT decision makers named network performance to support a growing number of clients and faster internet speeds among their top concerns. With nearly half of Australian IT departments already spending more than 10 hours a month on managing IP addresses (47%), the findings suggest more needs to be done to prepare the Australian IT workforce to meet the demands on the IT department accelerated by the IoT.

Joel Dolisy, CIO/CTO at SolarWinds, says IT professionals must be armed with not only the skill, but also the tools needed to maximise opportunities created by the IoT and empower their organisations to embrace even greater efficiency, cost-savings and agility.

"As networks become increasingly complex, maintaining visibility and control over those networks and the full application stack becomes more difficult. Network monitoring and management is a critical component of a successful IoT environment and as a result, a necessity for organisations looking to harness the potential of new, smart and interconnected technologies or to manage the new IT reality. Businesses need to arm IT professionals with the skills and capability needed not only to maintain visibility over the growing number of connected devices, but also to pinpoint potential IT infrastructure issues in order to minimise impact to the networks and application performance and keep up with the growing expectations of their company workforce," said Dolisy.

IT decision makers also highlighted several opportunities driven by the IoT including, improved capabilities for remote maintenance (39%), security management (32%) and the ability to offer high-margin personalised services (27%) to stakeholders

Nearly 80% of organisations with 200 or more employees feel the IoT will make their network management more complex (77%).

More than half of all organisations believe that security is essential to overall network management in an IoT environment (51%), followed by network monitoring and management capability (39%) and IP address automation (32%).

While there is widespread consensus about the transformative potential of the IoT, most organisations are not doing enough to prepare. Businesses need to be ready for more acceleration in additional users and internet-enabled devices connected to the network

as well as the resulting deluge of data and increased demands on bandwidth, security systems, storage, and application performance.

Solarwinds in collaboration with Redshift Research conducted a Survey in Australia to explore the preparedness of Australian IT to meet the complexity of the IoT. This survey was reported in June 2015.

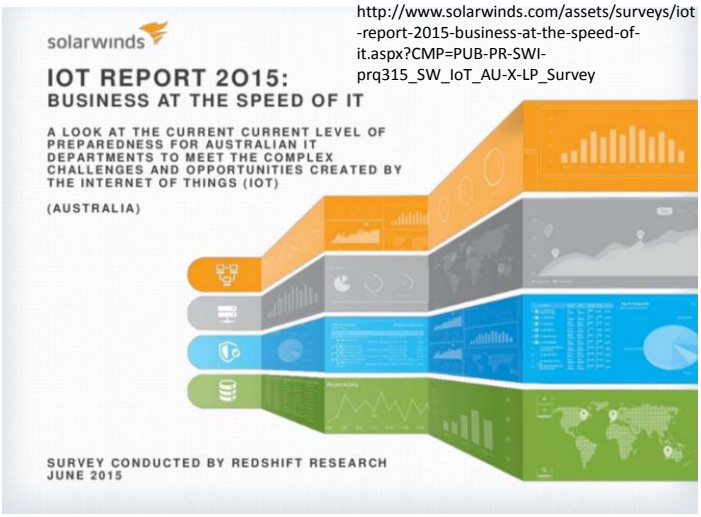


Figure 34: Solarwinds IoT Report

The key findings were:

Australian IT departments cite concerns over a lack of IT skills, security issues and growing network complexity as the key challenges for organisations looking to adopt IoT technology in the next three to five years.

Nearly 60% or respondents said that more or different IT skills will be required as devices and robots become more intelligent and 73% feel workforce is currently ill-equipped.

Insufficient skills was also named as the top barrier to the uptake of IoT technologies (30%) with 44% of respondents also agreeing that staying current with technology is the number one challenge impacting their work in the next three to five years.

Respondents also cited that maintaining security (42%) and growing network complexity (38%) among challenges that will most impact their work in the next three to five years.

IT decision makers also highlighted several opportunities driven by the IoT including improved capabilities for remote maintenance (39%), security management (32%) and the ability to offer high margin personalisation services (27%) to stakeholders.

Observation 41: There is a widespread recognition of an educational shortfall in STEM subjects, which risks exacerbating an already growing and evident shortage in the skilled ICT and industry practitioners needed for IoT. New roles such as 'data scientist' will become increasingly vital.

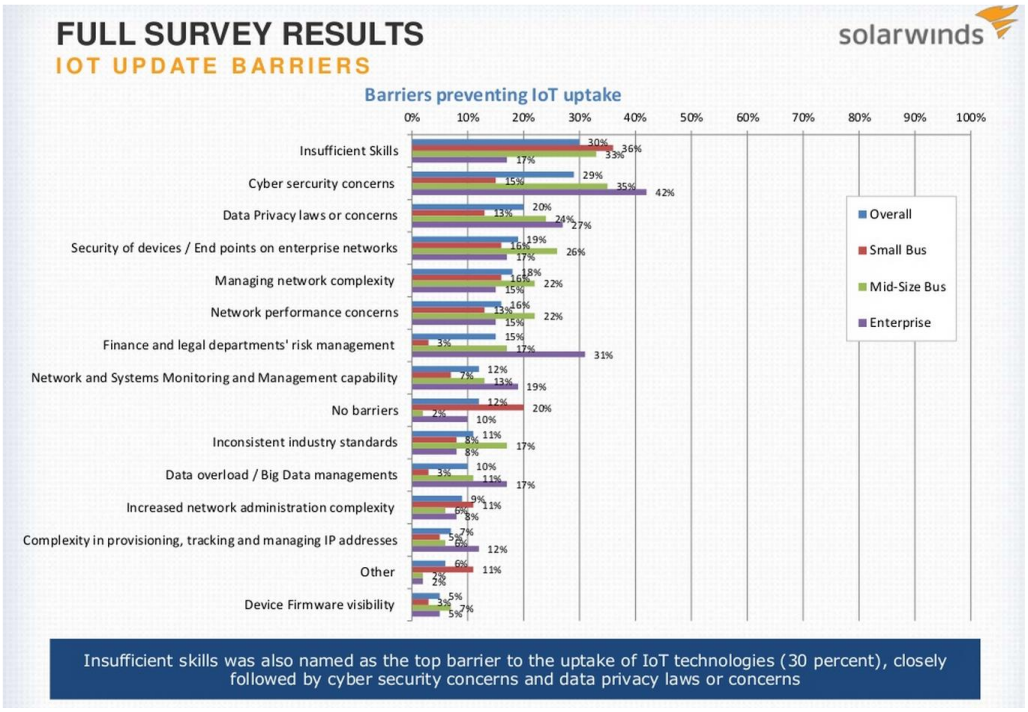


Figure 35: Solarwinds IoT Report – barriers

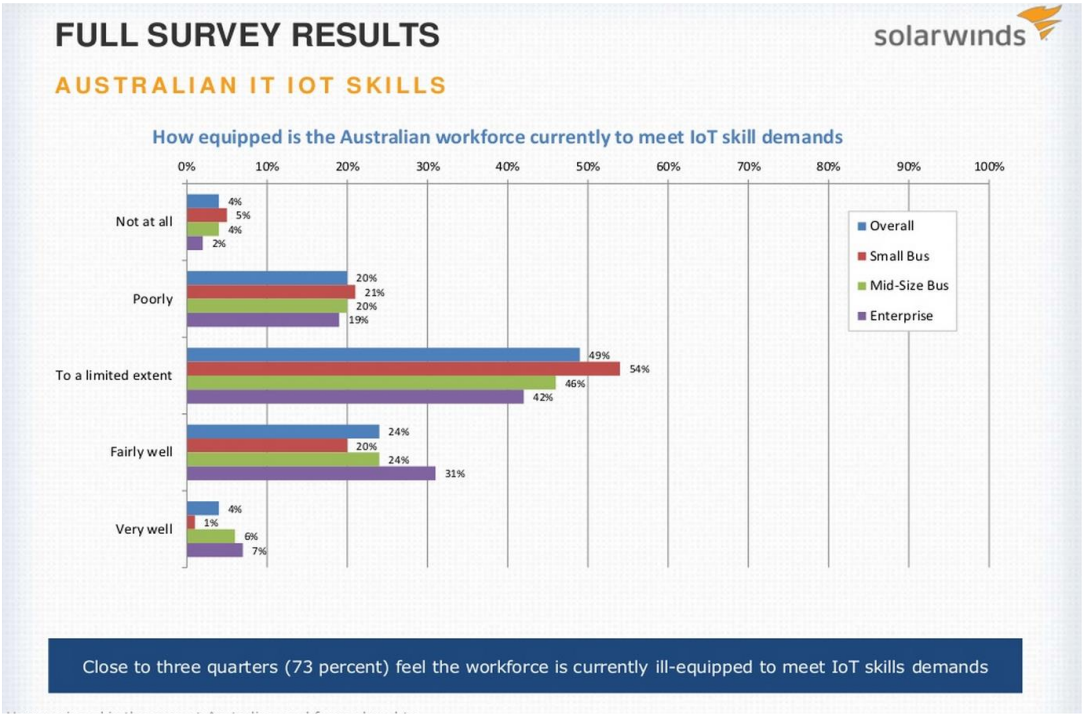


Figure 36: Solarwinds IoT Report – skills

7.10.2 Develop an Appropriately Educated Workforce

Brian McCarson, Intel's chief IoT architect, ended his talk at the AIIA IoT conference in Canberra in March 2015 with some advice for Australia. "My simple observations for any

geography, but especially Australia, is that there are three things that need to be done to help IoT become a major economic driving force for this country.

"The third area is science technology engineering and mathematics. To me this equation is very simple. It starts at age five and goes to 50 plus. It can't be just a process where you make sure that individuals in their junior year of college choose to stay in engineering programs.

"There has to be an entire culture of innovation and making sure that the workforce and the future workforce are embracing the need for technological innovations in these four key areas. Those are critical to make sure you have a competitive workforce for the future of IoT."

8 RECOMMENDATIONS

This section contains the observations, recommendations and possible future work streams to help to facilitate the successful growth of the IoT based emerging digital economy. This is the combined outcomes arising from the IoT Think Tank public workshops, interviews with more than 30 companies and Government departments, and the guidance from the CA IoT Executive Council, made up of leaders from major global and local ICT industry players.

8.1 Observations

Following are all the observations made throughout the document (in order of their appearance):

Page 9:

Observation 1: There is a huge potential economic promise of productivity gain, business innovation and competitive advantage through the use of IoT.

Page 10:

Observation 2: IoT can be seen as both an industry vertical in its own right as well as a horizontal enabler for all other sectors within the ICT sector.

Page 11:

Observation 3: IoT innovation and deployment is more mature in some sectors than others. Those that are more advanced are characterised by strong collaboration within the sector in specific countries.

Page 12:

Observation 4: Innovation in the consumer IoT market is evident today with the growth of new home automation services. These are introducing a multi-dimensional, fragmented and complex service model for consumers.

Page 14:

Observation 5: Long-term cross-sectoral opportunities are huge but initial success seems sector-focused overseas, due to a focus on common and achievable goals, trust, more easily identified mutual interest and fewer governance barriers.

Page 24:

Observation 6: Australia's peer countries and customers are further advanced in articulating and encouraging IoT industry benefits.

Page 24:

Observation 7: A key factor in IoT success and leadership is collaboration at many levels. Collaboration is required between Government, industry, research and education, within and between industry sectors, between 'eco-system' partners.

Page 26:

Observation 8: Interoperability is a key enabler for IoT systems, for which open systems are essential.

Page 26:

Observation 9: There are many open architectures with corresponding standards choices – each fit for certain purposes. Choosing the right one will be important depending on each industry, application or service level.

Page 27:

Observation 10: Australia should not try to establish new IoT standards. There are already more than the average engineer can cope with and enough to serve our needs well.

Page 29:

Observation 11: IoT is very sensitive to connectivity costs and today tariffs are set from the perspective of a person accessing the internet – either fixed or mobile. New lower cost and lower tariff models will be required that support very low data volumes for a few cents per month.

Page 36:

Observation 12: The advent of IoT will introduce the possibility of increasing fragmentation of the service components across potentially many sub-component service providers. For example, access, core network, data storage and distribution etc. Similarly, with the advent of eSIMS, consideration will need to be given to what service obligations and licencing conditions should apply to the 'service provider' to ensure customer service obligations are met and a level-playing field exists between service provision at the appropriate layers and segments.

Page 43:

Observation 13: IoT will force a re-evaluation in the value of wireless spectrum for connectivity, accessibility, sharing and licencing across existing and new bands. National regulators of spectrum are recognising this and providing focus on preparing for a more pervasive IoT future.

Page 44:

Observation 14: IPv6 is the universally agreed, preferred communications protocol for IoT for scalability, security by design and simplicity.

Page 45:

Observation 15: There are profound implications and opportunities, in how, where and by whom data is captured and stored for IoT.

Page 48:

Observation 16: The development of IoT advanced analytics is in its early days. There is opportunity for developers and service providers who can specialise and demonstrate insightful capability within analysis domains.

Page 50:

Observation 17: Data visualisation and open service APIs are key for unlocking big data insights and proving usable, insightful IoT services and collaborating with partners and customers.

Page 52:

Observation 18: Security technology and processes at design, management and service delivery will be critical for certain market sectors and applications. These will need to be consistent with any Government/industry regulations and guidelines regarding data privacy, security and network resilience.

Page 57:

Observation 19: So-called data silos within Asia-Pacific organisations – including many in Australia – are limiting the ability of major organisations to make insight-based decisions, and resulting in increased IT costs.

Page 61:

Observation 20: Frameworks for sharing data are proving to be useful in opening usage and value. This is occurring in some sectors and in are in discussion and development at Government level in many countries.

Page 66:

Observation 21: IoT policy areas under review or development coalesce around a few areas, which are: spectrum management, personal privacy, use of IPv6, network resilience and security, open Government data, interoperability and national innovation and competitiveness.

Page 68:

Observation 22: A potentially realisable $100 billion economic impact of the IoT on the Australian economy by 2025 is worthy of a considered national IoT strategy and focus.

Page 69:

Observation 23: IoT solutions are derived from collaborations across all the layers of our model. Partnering and collaboration will be critical for IoT innovation in Australia.

Page 70:

Observation 24: Notwithstanding laudable individual company initiatives and some standout IoT pilots, there is an evident lack of coordinated, persistent industry and /or Government focus on IoT.

Page 72:

Observation 25: The development of smart city plans and deployment in Australia is apparently lagging behind the rest of the world. Anecdotally, smart cities seem bedevilled by governance issues across local, departmental, state and federal jurisdictions. This makes the necessary collaboration complex and often unwieldy.

Page 72:

Observation 26: Gaps in regulations governing data ownership and privacy, as well as service trust are significant barriers to overcome for eHealth in Australia.

Page 72:

Observation 27. Preventative health is a major beneficiary of many IoT based solutions and this could greatly reduce healthcare costs overall.

Page 73:

Observation 28: Mining and resources, food and agribusiness, and transport and logistics appear to be sectors where Australia can make a significant global contribution.

Page 74:

Observation 29: The federal Government's Industry Growth Centre strategy offers an opportunity to leverage IoT innovation and to align sectoral activities.

Page 74:

Observation 30: Infrastructure Australia appears to have overlooked IoT as a significant innovation for the telecommunications infrastructure and is missing the opportunity to use IoT to address the major challenges in transport, energy and water.

Page 76:

Observation 31: Building smarter and more productive infrastructure in Australia, will require IoT technologies, and moreover collaboration between the key industry and Government organs, including Infrastructure Australia, the ACCC iCC, Departments of Industry and Communications etc.

Page 76:

Observation 32: Australian competitive advantage and IoT leadership will require a thriving IoT start-up community, supported by a wider IoT eco-system. Conversely huge market potential for IoT offers significant opportunity for start-ups.

Page 77:

Observation 33: "By reinvigorating open data policies, there would be a contribution to Australia's cumulative GDP growth of $16 billion per annum or around 1% of GDP over the next five years". Australia could take the lead in opening up data sets and enabling sharing which can underpin IoT acceleration.

Page 79:

Observation 34: The NBN may need to be connected to locations that today are not described as premises such as traffic controllers, lamp posts, bus shelters etc. for IoT applications. Providing such access may also be an opportunity for other service providers.

Page 79:

Observation 35: Lower cost connectivity is essential to many IoT business cases, for low bit rate IoT services, such as metering. There is significant opportunity in Australia for low cost services to be enabled in Australia, through new low power wide area wireless technologies and services and/or by innovative lower tariffs for low-bit rate services on existing service platforms.

Page 80:

Observation 36: IPv6 is a major enabler of IoT. Australia's adoption of IPv6 is poor compared to a number of our major peers. 1.44% versus 21.7% US, 18.1% Germany, world average approx. 7.6%. (Source Google IPv6 statistics).

Page 81:

Observation 37: The challenge of the Australian IoT industry is to inform, share and drive the timely allocation of spectrum and spectrum usage models, through ACMA, to support a thriving and innovative IoT market.

Page 81:

Observation 38: Given the potential fast pace of future innovative IoT services, it will be important that ACCC is vigilant to prevent 'possible' market abuse of network neutrality in providing and bundling IoT services

Page 82:

Observation 39: Trust and security will be vital to build IoT service confidence and underpin growth. On the other hand, there is also a risk that failure to address security concerns early on or by applying onerous security restrictions as an afterthought can significantly inhibit the deployment of IoT services.

Page 82:

Observation 40: Government law enforcement regulations regarding telecoms are already becoming onerous and an additional cost burden and inhibitor for certain service types. As IoT becomes more pervasive this overhead may become an increasing burden and inhibitor.

Page 84:

Observation 41: There is a widespread recognition of an educational shortfall in STEM subjects, which risks exacerbating an already growing and evident shortage in the skilled ICT and industry practitioners needed for IoT. New roles such as 'data scientist' will become increasingly vital.

8.2 The Key Enablers and Inhibitors

The key inhibitors and enablers for IoT success in Australia are drawn from the observations above.

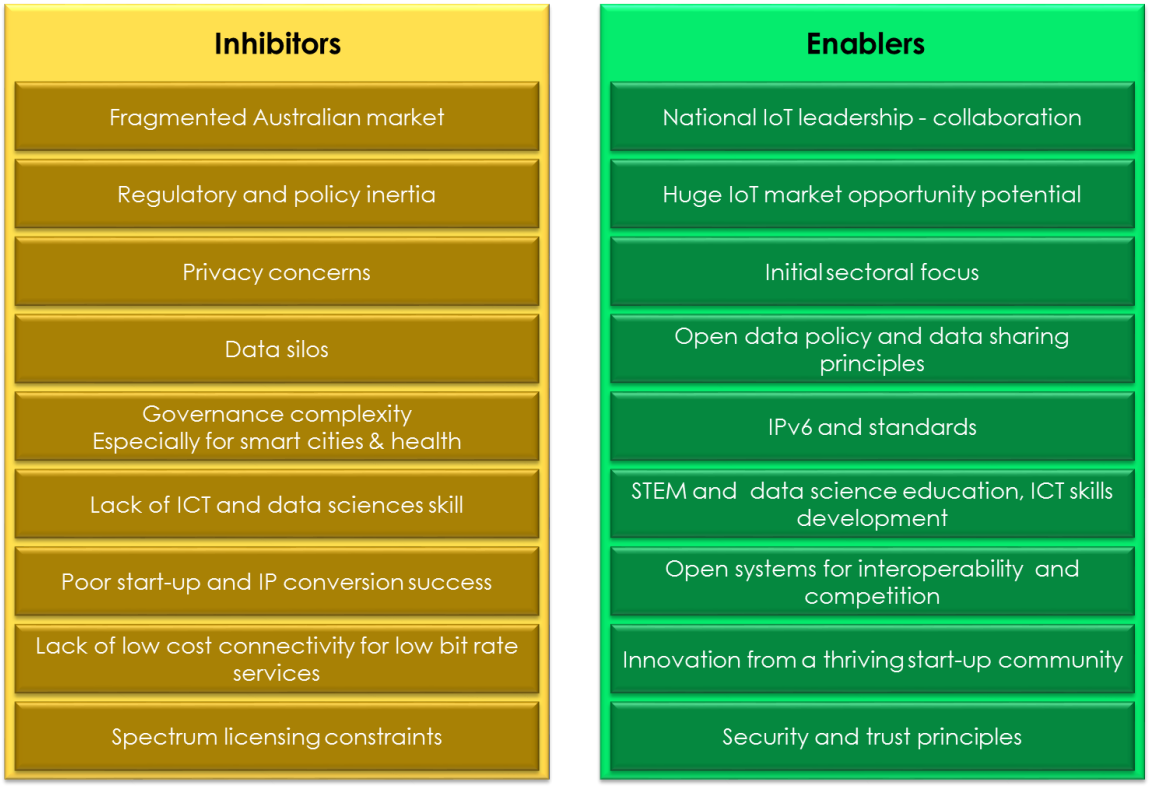


Figure 37: Key Inhibitors and enablers

8.3 Industry Recommendations

In order to address the issues related to the IoT inhibitors and to pursue the opportunities that the enablers offer, and with a view to the IoT overarching aim to invigorate the Australian IoT industry and help Australia to market leadership in some key focus areas, some key recommendations are offered for consideration:

Recommendation 1: Develop and support a coherent and collaborative Australian IoT industry enabled by appropriate policy and regulation settings to drive productivity and innovation aligned with national economic objectives.

Recommendation 2: Choose leadership in a few key sectors where additional efforts are made at industry and Government level and collaboration is enhanced. Sectoral focus prospects where Australia may lead are in mining, agriculture, transport and telecommunications.

It makes sense to align with key Government agency programs and strategies in the focus sectors of the DIS Industry Growth Centre activities and Infrastructure Australia.

Recommendation 3: Develop a model and principles for IoT data sharing and opening of public data.

Recommendation 4: To build confidence and trust in IoT use by addressing IoT privacy concerns with clear policy and guidelines for access to, consent and use of private data. Align with policies on open data and data sharing.

Recommendation 5: Develop minimum network/service security guidelines for the IoT service chain, from sensor/actuator, to network, to data. This needs to consider both security from attack and service resilience.

Recommendation 6: Encourage a thriving IoT start-up community through alignment, where sensible, with Industry Growth Centre activities, start-up incubators, focus industry sectors and collaboration to build eco-systems of innovation.

Recommendation 7: Review the adequacy of the current spectrum settings and licencing in accommodating new IoT wireless technologies and scale with particular focus on spectrum for low-bit rate services.

Recommendation 8: Encourage use of IPv6 by default on all platforms, including Government and internet Service Providers (ISPs).

Recommendation 9: Add weight to the drive for greater science, technology, engineering and mathematics (STEM) learning programs and develop IoT training programs, with particular emphasis on data engineering.

Recommendation 10: Review the adequacy of Australian oversight and participation in the key IoT standards bodies with a view to having the capability to provide knowledgeable industry guidance on implications for trade impediments, data protection and local regulatory impact

Recommendation 11: Consider reduction and simplification of governance in the development of smart cities in Australia.

Recommendation 12: More detailed economically sound, evidence-based research should be commissioned to confirm preliminary observations, recommendations, enablers, inhibitors and sectoral focus and which parties are best placed to drive initiatives and assume leadership roles.

8.4 Proposed Workstreams

The following workstreams for the Think Tank have been derived from the recommendations above and are being proposed to further advance the vision of the Think Tank.

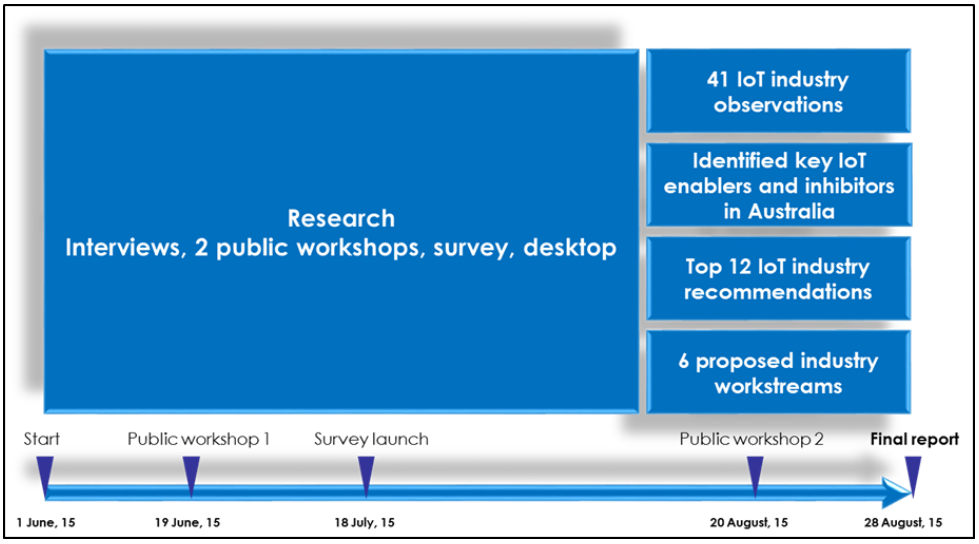


Figure 38: Report outputs – observations, recommendations, workstreams

Workstream 1: Collaborative Australian IoT industry – Canvass support and develop a coherent, collaborative and globally-aware Australian IoT community with industry, Government and other key stakeholders to foster innovation and inform appropriate policy and regulatory settings.

Workstream 2: Sectoral engagement – Develop sectoral IoT advancement and alignment in key sectors, through Government Industry Growth Centre activities and key sectoral bodies with focus on mining, agriculture, transport and telecommunications.

Workstream 3: Open data – Develop IoT open data and data sharing principles and guidelines with possible sectoral focus. Data privacy – develop privacy guidelines for use of IoT data.

Workstream 4: Spectrum availability – Working party including the ACMA and broader stakeholders to address the spectrum settings and licencing needs for low bit rate wireless services, such as LPWA.

Workstream 5: Security – Develop security guidelines for IoT services and service elements, including data protection.

Workstream 6: IoT start-up innovation – Develop policy and IoT eco-system frameworks in support of a national IoT program, which is linked to Industry Growth Centres.

APPENDIX

A The IoT Think Tank

Vision: to be a leading ICT industry initiative under a broad industry framework shaping the regulatory framework to harness for Australian industry the opportunities generated by the internet of Things. The Think Tank aims to define the IoT eco-system, inform and enable Australian companies to exploit the business opportunities afforded by IoT technology and services.

Goal: by mid-2016 have an activated, globally-aware Australian IoT industry community, with a future strategy and vision that is understood and supported by industry and key stakeholders and which positively influences Government policy directions.

Executive Council Members

- Alcatel Lucent
- Bureau of Communications Research
- Communications Alliance
- Creator Tech
- Ericsson
- Hewlett-Packard
- Huawei
- IBM
- Intel
- Knowledge Economy Institute (KEI)
- KPMG
- nbn
- Telstra

B Methodology of Study

B1 Initial Scope

Identify Australian regulatory and policy enablers and inhibitors for Australian IoT industry success:

- Comparison with leading overseas IoT countries
- Australian activity and status
- Cross-sectoral implications
- Focus areas and recommendations

Australian industry readiness and focus:

- Description and mapping of the Australian IoT eco-system
- industry SWOT
- Potential work-stream definitions for next phase
- Focus areas of opportunity for the Australian economy, including within specific industry verticals and through cross-sectoral collaboration
- Recommendations for policy and industry initiatives designed to generate measurable economic outcomes

B2 First IoT Workshop – 19 June 2015

70 attendees across industry Government, regulators, consumer groups, etc.

Important themes:

- What regulatory/industry reforms are needed to adapt to IoT?
- Collaboration is fundamental for opening opportunities and breaking down barriers
- Data sharing/openness
- Spectrum availability for IoT
- How to help start-ups participate and thrive?

B3 Interviews

B.3.1 Peter Leonard, Athea Carbon, Michael Burnett – Gilbert and Tobin

B.3.2 Mike Briers – Knowledge Economy Institute

B.3.3 Paul Paterson, Nick McClintock – Bureau of Communications Research

B.3.4 Steve Killeen, Danny O'Driscoll – Downer Communications

B.3.5 Michael Biber – IPv6

B.3.6 Geoff Sizer – Genesys Design

B.3.7 Chris McLaren – KPMG

B.3.8 James Halliday, Rebekah Lam, Patrick Fair – Baker McKenzie

B.3.9 David Bridge, Sarah Goss, Warren Chaisatien, Pia Seeto – Ericsson

B.3.10 Rob Zagarella – NNN Co

B.3.11 Reg Coutts – Coutts Communications

B.3.12 Peter Crocker, Nick Chryssostomidis – IBM

B.3.13 John Tuckwell – EU Horizon 2020

B.3.14 John Zic – CSIRO

B.3.15 Michael Cox – Huawei

B.3.16 Warren Lemmens – Alcatel-Lucent

B.3.17 Tim Williams – City of Sydney

B.3.18 Anthony Murfett – Growth Centres Branch Sectoral Growth Policy Division, Department of industry and Science

B.3.19 Helen Owens – Department of Communications, Digital Productivity Division

B.3.20 Ryan Kolln – Telstra

B.3.21 Ros Harvey – The Yield

B.3.22 Peter Shutz – Agrigulture Growth Centre

B.3.23 Roger Lawrence – HP

B.3.24 Lee Hickin, Dave Glover – Microsoft

B.3.25 Jennifer Mulveney, Peter Robles – Intel

B.3.26 Christian Bennett, Mark Sheppard – General Electric

B.3.27 Cameron McNeill, Anthony Stewart – Optus

B.3.28 Catherine Caruana-McManus – Giant Ideas

B.3.29 Gavin Smith – Bosch Australia

B.3.30 Duncan Giles – nbn

B.3.31 Peter Triantafilou, Office of Science, Technology and Research Department of State Development, South Australia

B.3.32 Trevor Townsend – Tech Advisory Partners

B.3.33 Nicholas Bellamy

B.3.34 John Reidl, Greg Irving – Pooled Energy

B.3.35 Malcolm Shore – BAE Systems

B.3.36 Danielle Storey – Director of Operations, Smarter Technology Solutions

B4 IoT Survey

CA conducted a simple online survey of its members. The survey has also been forwarded to the members of the Australian Information Industry Association (AIIA), Australian Computer Society (ACS) and Telsoc. The approach taken was to invite any of these members to respond on the basis that they already had some understanding of IoT and as such no definitions or clarifications were provided. Several simple questions were asked about IoT and some of the results follow:

Question 1: Please rank which market sectors in Australia you believe would benefit the most from IoT in the next 3-5 years?

Answer 1: The top five sectors identified in order were;

1. Transport
2. Agriculture
3. Smart cities
4. Health
5. The environment

Question 2: Please rank which market sectors you believe Australia could become a world leader in through IoT innovation?

Answer 2: The top five sectors identified in order were;

1. Agriculture
2. Mining
3. Health
4. Transport
5. Smart cities

Question 3: What two or three things best enable the development of IoT in Australia?

Answer 3: The most recurring answers were;

1. Better support for start-ups
2. Better policy and legal framework for IoT
3. Open, secure data framework
4. Government funded IP to be more effectively open to industry
5. Education and skills development
6. Forward looking regulation and policy for the digital economy
7. Government light touch approach
8. Collaboration – Government, academic, business and research
9. Collaboration – cross industries

Question 4: What two or three things most inhibit the development of IoT in Australia?

Answer 4: The most recurring answers were;

1. Lack of investment in IoT start-ups
2. Concerns over data privacy and security
3. Lack of local expertise
4. Lack of awareness if the potential impact
5. Cost of carriage
6. Spectrum management for IoT

7. Risk averse market generally
8. Fragmentation of the industry and the expertise

B5 Second IoT Study Workshop – 20 August 2015

Main points raised during the second public workshop were:

- Suggested inclusion of a horizontal industry focus (e.g. supply chain, asset management) for IoT, alignment with and leverage of the Infrastructure Australia Audit (which has water, transport, telecoms and energy as its infrastructure focus).
- Start-ups again a major theme – building an IoT eco-system in which to collaborate.
- Data sharing/privacy work streams should form one work stream.
- More emphasis needed on security and network resilience – possibly a new work stream.
- Good timing of report with regards a number of Government initiatives – for Department of Communications, Infrastructure Australia Audit and Industry Growth Centre activities.
- Need to highlight consumer/hub IoT a little more in light of recent Google announcement.
- Connecting to university work on IoT would be advantageous – it appears that there are interesting pockets of activity which could all be part of a national IoT strategy and collaboration.
- Confirmation that Australia is quite behind in take-up/deployment of IPv6 (a key enabler) compared to the rest of the world.

C Bibliography

Note that this entire document is intended to be a resource gathered from many sources. In most cases these sources are referenced below or with web links within the document. Our intention was to curate information gathered from many sources to assist the understanding of the reader rather than creating all new material. Some references may not be perfectly represented in every case but we felt it was better to share information freely than exclude useful information from incomplete referenced sources.

1. CISCO White Paper 2013; Embracing the internet of Everything – To Capture Your Share of $14.4 Trillion by Joseph Bradley Joel Barbier Doug Handler

2. McKinsey Global Institute Paper June 2015; THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE

3. Alcatel Lucent STRATEGIC WHITE PAPER 2015; The Future of Digital Services Delivery, Embracing co-dependency for growth of the National Digital Economy

4. Accenture Strategy Paper 2015; The Growth Game-Changer: How the Industrial internet of Things can drive progress and prosperity by Mark Purdy and Ladan Davarzani

5. SIGFOX Whitepaper 2015; One Network A billion dreams; M2M and IoT redefined through cost effective and energy optimized connectivity

6. ISO/IEC JTC 1 Information technology internet of Things (IoT) Preliminary Report 2014

7. One M2M Whitepaper January 2015; The Interoperability enabler for the entire M2M and IoT Eco-system

8. IEEE IoT Security and Privacy Article May/June 2015 by Susan Landau Associate Editor in Chief

9. Big Data Value Association BDV Report; The New Economic Asset www.bdva.eu

10. Cisco Whitepaper 2014; Attaining IoT Value: How To Move from Connecting Things to Capturing Insights Gain an Edge by Taking Analytics to the Edge by Andy Noronha, Robert Moriarty, Kathy O'Connell, Nicola Villa

11. OECD Digital Economy Outlook 2015 Report. ISBN 978-92-64-23227-3

12. Australian Government Department of industry and Science, industry Growth Centres Initiative Paper 2015; www.business.gov.au/industryGrowthCentres

13. Deloitte Access Economics Paper; Assessment of the economic benefits of open Government data, Bureau of Communications Research 2015

14. ForgeRock Whitepaper; The Identity of Things (IDoT): Access Management (IAM) Reference Architecture for the internet of Things (IoT)

15. Ericsson Whitepaper Uen 284 23-3242; February 2015; Understanding the Networked Society

16. Ofcom Statement 27 January 2015; Promoting investment and innovation in the internet of Things Summary of responses and next steps

17. ITU Workshop on the "internet of Things -Trend and Challenges in Standardization" (Geneva, Switzerland, 18 February 2014) with focus on SG13 activities Marco CARUGI ITU-

T Q2/SG13 Rapporteur ITU-T FG M2M Service Layer Vice-Chair Consultant, China Unicom marco.carugi@gmail.com Geneva, Switzerland, 18 February 2014

18. A report by the UK Government Chief Scientific Adviser; first published December 2014, The Government Office for Science URN: GS/14/1230; The internet of Things: making the most of the Second Digital Revolution;

19. Akamai's State of the internet Q4, 2014; Editor David Belson

20. IEEE Standards Association internet of Things Eco-system Study 2015

21. Australian Journal of Telecommunications and the Digital Economy VOLUME 2 NUMBER 4, DECEMBER 2014 ISSN 2203-1693; How the internet of Things Changes Everything. The next stage of the digital revolution by Kate Carruthers UNSW Australia

22. ARTICLE 29 DATA PROTECTION WORKING PARTY This Working Party was set up under Article 29 of Directive 95/46/EC. An independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013. Website: http://ec.europa.eu/justice/data-protection/index_en.htm 14/EN WP 223 Opinion 8/2014 on the on Recent Developments on the internet of Things; Adopted on 16 September 2014

23. Singapore IDA Smart Nation Platform industry Roundtable Report; April 2015

24. EY Sweeny Ernst & Young Australia 2015; Digital Australia Sector Report, Government

25. EY Sweeny for AIMIA Ernst & Young Australia 2014; Digital Australia State of the Nation 2014

26. Verizon State of the Market THE INTERNET OF THINGS 2015; Discover how IoT is transforming business results.

27. Never mind the IoT, here comes the third wave. Aricent http://www.aricent.com/

28. Australian Journal of Telecommunications and the Digital Economy VOLUME 2 NUMBER 3, SEPTEMBER 2014 ISSN 2203-1693. Copyright © 2014; http://doi.org/10.7790/ajtde.v2n3.47; The Digital Universe Rich Data and the Increasing Value of the internet of Things by Matt Zwolenski and Lee Weatherill EMC ANZ

29. WS02 White Paper; A Reference Architecture for the internet of Things Version 0.8.0 http://wso2.com

30. Ovum Connected Nation: M2M in Australia 2014-2019 for Vodafone

31. ITU 2015GSR; Discussion Paper, Regulation and the internet of Things,

32. ABI Research, Big Data and Analytics in IoT and M2M

33. Cisco 2013, internet of Everything (IoE) Value Index

34. The Economist (Telstra commissioned); Land of Sweeping Change: Powering Australian Business Towards a Connected Future

35. IoT6 – Ipv6 for IoT. IoT6 is a 3 years FP7 European research project on the future internet of Things. It aims at exploring the potential of IPv6 and related standards

(6LoWPAN, CORE, COAP, etc.) to overcome the current shortcomings and fragmentation of the internet of Things.

37. The internet of Everything through IPv6 An Analysis of Challenges, Solutions and Opportunities" Antonio J. Jara, Latif Ladid, Antonio Skarmeta.

38. The internet of Things: Seizing the benefits and addressing the challenges; OECD report of the working party on common infrastructures and services policy, 1 June, 2015

39. The internet of Things, What needs to Change; James Halliday, Patrick Fair, Baker and McKennzie presentation to 1st IoT Think Tank public workshop, 19 June, 2015

40. Asia Pacific IoT Market Overview, Frost and Sullivan, 2014

41. Australian Journal of Telecommunications and the Digital Economy VOLUME 2 NUMBER 4, DECEMBER 2014 ISSN 2203-1693; Enabling Technologies for Effective Deployment of internet of Things (IoT) Systems: A communications networking perspective, Jamil Khan, Dong Chen, Oliver Hulin.

42. Accenture Technology: Driving unconventional growth though the Industrial internet of Things Paul Daugherty, Prith Banjerjee, Walid Negum and Allan E. Alter

43. Budde report: Australia – M2M and The internet of Things, 2015

44. Harvard Business review: internet of Things: Science Fiction or Business fact?, 2014, sponsored by Verizon.

45. Gigaom Research: Ebaling IoT, Jon Collins, 29 Jan, 2014

46. Internet of Things – Some legal and regulatory implications, James Halliday and Rebekah Lam, Baker McKenzie, June, 2015

47. Australian Infrastructure Audit, Our Infrastructure Challenges, April 2015.

48. European Commission Directorate-General for Communications Networks, Content and Technology, Sustainable and secure Society. Trust and Security. Report on the public consultation on IoT Governance. 16/1/2013

49Internet of Things: Risk and Value Consideration, an ISACA internet of Things paper.

50. Intel White Paper Privacy Principles February 2014; Applying Privacy Principles in a Rapidly Changing World. By Stuart Tyler, David Hoffman, Paula Bruening

51. Jasper Technologies Inc, White Paper; Best Practices for Implementing Global IoT Initiatives. Key Considerations for Launching a Connected Devices Service.

D Economy-Wide Quantitative IoT Impact Estimates

By Gruen, Houghton and Tooth (2014)

Three considerations for assessing this approach include:

The estimate is considered a 'best guess' by the authors rather than a base-line figure estimated using conservative assumptions.

As noted in more detail below the specific methodology and assumptions in the underlying McKinsey study are not available for detailed critique.

Using Australian GDP to select a proportion of the global estimates is reasonable for providing a 'best guess' estimate but it does not take into account any particularities of Australia's policies or industry contexts.

In order to give an indication of how this value might be divided among sectors, Gruen et al. divide the sector shares from the McKinsey study (without regard for structural differences between economies) based on the estimated $64 billion of total potential of open data in Australia.

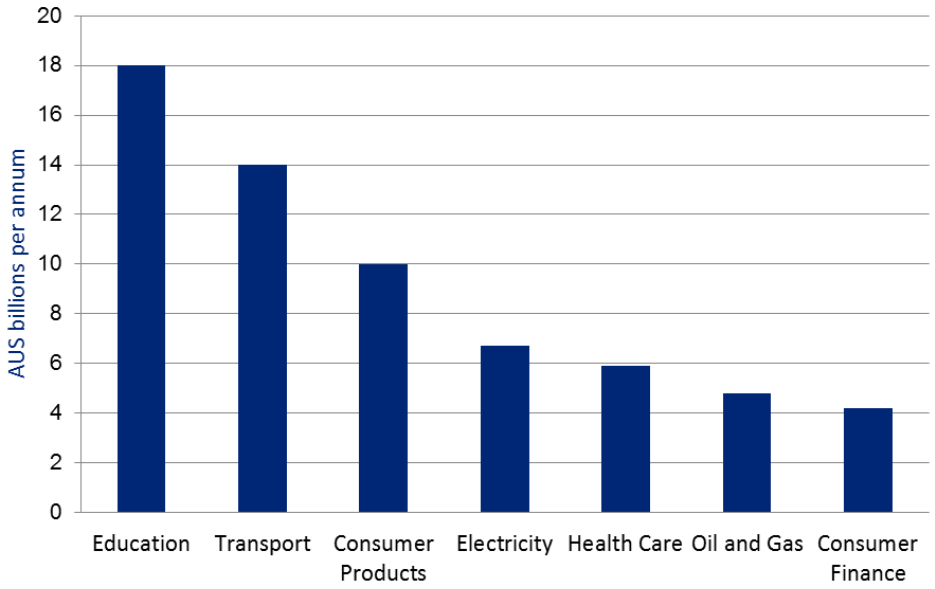


Figure 39: Potential value of open data for Australia

9Source: Gruen et al. analysis of data from McKinsey Global Institute (2013) Open data: Unlocking innovation and performance with liquid information. New York0

An alternative methodology of 'the return on investment (ROI)' of creation and collection of data is also employed by Gruen et al. (2014). Three different methods to estimate Government spending on the creation and collection of data were used: first using previous reports and experience; second using previous international analysis; and third using Commonwealth Government budget appropriations. The estimations are that approximately $4 to $5 billion are spent by the Commonwealth Government on data creation and collection per annum and total Government expenditure (including state and territory Governments) could be in the magnitude of $8 to $10 billion.

In addition to Government data, Gruen et al. (2014) include publically funded research, which is approximately $12 billion per annum. Using a range of assumptions, they find

that at the mid-point, the return from one year's data spending would be around $17 billion NPV over 20 years, a return worth 1.5 times the investment. Finally the point is made that these are likely to be conservative estimates because it assumes constant returns when information is often characterised by increasing returns.

Deloitte Access Economics consulted with Nicholas Gruen regarding the "Open for Business" report, and note his contention that since measuring the economic benefits of open data is particularly difficult, it is better to make a 'best guess' rather than follow a precise methodology with conservative assumptions knowing that the final figure is a gross underestimate of the potential impact. Attention was also drawn to the fact that despite not knowing the specific details of the methodology of the McKinsey study, it returned a figure ($16 billion) quite close to its own ROI model ($17 billion).

Data-driven innovation

An additional estimation of the role that data is playing in the Australian economy is provided in the Google Australia commissioned report "Deciding with data: How data-driven innovation is fuelling Australia's economic growth", undertaken by PriceWaterhouseCoopers Australia (PwC). This report looked at the role of all available data in the economy (not limited to Government open data) and found that in 2013, data-driven innovation added an estimated $67 billion in new value to the Australian economy, or 4.4% of GDP (PWC, 2014).

The report particularly highlights the importance of the health industry in Australia as a potential driver for future productivity growth. The report argues that increasing the uptake of data-driven innovation by business and public sector organisations using open data is a means to achieving productivity gains. To achieve these benefits and gains, technical and legal barriers to access need to be overcome.

Geospatial data

Geospatial or spatial data is of particular importance because it can be used to produce location maps to find goods and services from a wide range of sectors in a variety of end-using devices, with most added value coming from combinations with other information, such as demographic, traffic or environmental data (Vickery, 2011). The importance of assessment of the economic benefits of open Government data, geospatial data was highlighted in PIRA (2000), with approximately half of the total value of public sector information coming from geospatial information.

The first major report to aggregate the impact of spatial information on a national economy was undertaken for the Cooperative Research Centre for Spatial Information (CRC-SI) by ACIL Tasman (2008). It estimated the impact of modern spatial information technologies on the Australian economy in the 2006–07 financial year, finding the following impacts:

- industry (revenue): $1.37 billion annually
- industry (gross value added): $682 million

In addition, constraints on access to data are estimated to have reduced:

- productivity in some sectors by between 5% and 15%
- GDP and consumption by 7% (around $0.5 billion)

The study used a value-added methodology because a 'willingness to pay' approach was not possible due to a lack of data and prohibitive costs, nor could direct impacts be studied due to a lack of data. The value-added approach used 22 case studies from a

range of sectors to estimate direct impacts that were then applied to the Tasman Global Computable General Equilibrium model of the economy to estimate the macroeconomic impact of the spatial information. The sectors studied in 22 case studies were: agriculture, fisheries, forestry, mining and resources, property and services, construction, transport and storage, utilities, communications, and Government.

To summarise, the full range of Australian estimates is included in Table 3.1 below. Many of these were not specific studies, rather they were international studies that have been applied to Australia given the relative size of the Australian economy and have not accounted for the difference in the Australian context in any meaningful way.

Table: Range of Australian estimates

Sector/Agency	Estimate	Year	Source
Economy-wide	Current value of open Government data of up to $25 billion.	2014	Gruen et al. (2014)
Economy-wide	Potential for all open data (not restricted to open Government data) in Australia to contribute an additional $64 billion per annum.	2014	Gruen et al. (2014)
Economy-wide	Reinvigorating open data policies could contribute an additional $16 billion per annum.	2014	Gruen et al. (2014)
Economy-wide	Data-driven innovation added an estimated $67 billion in new value to the Australian economy.	2013	PWC (2014) for Google Australia
Economy-wide	Assuming similar levels of investment and use in Australia, the PIRA (2000) study would estimate an investment value for open Government data in Australia of $2.5 billion and a use value of around $18 billion.	2011	Houghton (2011) from PIRA (2000)
Economy-wide	Assuming similar levels of activity in Australia, applying the MEPSIR (2006) study to Australia would place the value of the open Government data at $3.2 billion.	2011	Houghton (2011) from MEPSIR (2006)
Economy-wide	Assuming similar levels of activity in Australia, the teVelde (2009) study would place the value of the open Government data market in Australia at around $500 million.	2011	Houghton (2011) from teVelde (2006)
Australian Bureau of Statistics	Assuming similar levels of activity in Australia, the DotEcon (2006) study would suggest an open Government data value in Australia of approximately $2.4 billion.	2011	Houghton (2011) from DotEcon (2006)
Office of Spatial Data Management and Geoscience Australia	Estimates overall costs associated with free online access to publications and data of $4.6 million per annum and measurable annual benefits of up to $25 million.		Houghton (2011)

Geoscience Australia (GA)	On average, social returns to annual expenditure on data collection suggest an increase in social returns of $15 million.	2011	Houghton (2011)
Spatial data	Comparing the impacts of free provision of GA topographical data relative to cost recovery was overall increase in net welfare gain of $4.7 million per annum.	2001-06	PwC (2010)
Spatial data	Given Government expenditure on fundamental spatial data of around $70 million, the net welfare benefits from providing free access over cost recovery are around $25 million per annum.		Houghton (2011)
Geoscience Australia	Estimates that industry revenue could be of the order of $1.37 billion and industry gross value added around $682 million.	2007-07	ACIL Tasman (2008)
	Estimated increase in GDP due to the accumulated impact of GA's provision of geospatial products and services of $1.8 billion .	2010	Australian Government (2011) referencing ACIL Tasman

E Australian Collaboration/Industry Initiatives

Examples of IoT activity and collaboration emerging in Australia are discussed here. This is not intended to be a complete list of activities. Rather, it reflects examples across the spectrum of the market that in most cases highlight collaboration in some form. Collaboration is seen as a vital ingredient to a successful IoT eco-system in Australia. Note that the following descriptions have been gathered from various interviews and searches and in some cases text provided by the organisation as input to this Report. Some explanatory text can be read as sales and marketing material and should be read with this in mind. This therefore does not reflect the views of CA.

E1 www.iotaustralia.org.au

Established by industry journalist, Stuart Corner, the site aims at being a focal point for news, views, comments and information in general on the exciting and rapidly developing world of the IoT primarily for people in Australia and New Zealand interested in IoT. It contains information about the importance of IoT and its likely impacts. The site is also providing a forum for discussion on all aspects of IoT.

E2 Start-Up Planning Australian LoRaWan Network

Extract – June 22, 2015 by Stuart Corner

"Australian start-up company National Narrowband Network Communications is planning a dedicated low power wide area wireless network based on the LoRaWan standard for connecting IoT devices.

The Australian LoRaWan network would be open to any organisation to use for its own IoT applications and devices and the company is looking to partner with Australia's Government Owned National Broadband Network Company, nbn, and with large user organisations, such as water utilities, to expedite network rollout.

LoRaWan is one of several low power wide area wireless technologies developed specifically for IoT applications. Zagarella said that NNN Communications had chosen it over competing options on the strength of its performance, the breadth of its technology and the strength of the companies backing it. "They have standardised all the components end –to-end and there are five companies that have network server software platforms available, including IBM."

Once the network is operational anyone would be able to install LoRaWan certified sensors and get data from these in standard format over the network.

In Australia LoRaWan devices would need to be certified by ACMA for conformance to the requirements of the band and, separately, for conformance to the LoRaWan specification. Zagarella said he hoped that certification facilities could be put in place in Australia."

E3 Alcatel-Lucent's ng Connect (Next Generation Connect) Program

The following is text extracted from the ngConnect.org web site – "Alcatel-Lucent developed the ng Connect eco-system that bring partners together to collaborate on solution concepts, business models and market trials. These partners can be small or large

enterprises, Government departments and local councils, universities and other research organisations. The Program has built an eco-system that enables member companies to develop new products and services faster, and with a higher customer profile. This is all about partnering for innovation. Trialling new digital services to find how each participating business can make money and deliver a service in a way that the market will value. Finding and fixing business inhibitors and testing assumptions are all aspects of the ng Connect program.

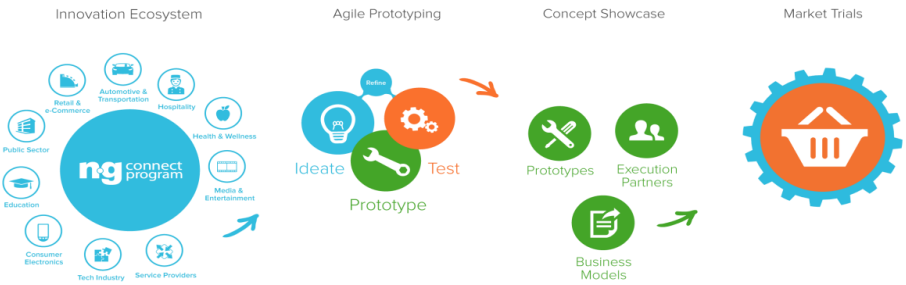


Figure 40: The ng Connect Program

ng Connect was developed to create the next generation of ultra-broadband enabled end user experiences that no single company can rapidly achieve alone. Working together, members develop ideas and solutions, validate, showcase and trial market new solution concepts, developing business models that create paths to new revenue for the entire value chain.

Solution concepts of prototype services in areas that touch our lives, including Retail, Health and Wellness, Entertainment, Financial Services, Transportation, Utilities and the Public Sector. Solution concepts include technologies from ng Connect member companies, along with business models and primary research to further test the market validity of a potential service offering.

After over five years of operations ng Connect now boasts a global membership in excess of 200 companies with active service concepts."

E4 The Knowledge Economy Institute: www.kei.org

The following material was provided by Mike Briers – the founder of the KEi. "The Knowledge Economy Institute (KEi), is an innovative Australian social enterprise dedicated to harnessing the transformative power of digital technology to solve the biggest challenges facing Australia and the world today. It brings together business, researchers, Government and civil society in one single focussed effort. Partners currently include Bosch, Cisco, Rozetta, Curtin University, University of Tasmania, CMCRC, University of Technology Sydney and Queensland University.

The KEi gathers a key asset – our data – makes it more useable and then, with the help of powerful tools and careful privacy protection, brings the possibility of unparalleled innovation and growth. IoT is a key enabler and the initial focus will be in Agriculture and natural resources management applications.

The digital revolution is making it possible to know things that were previously hidden from us. We can now see patterns, connections and interdependencies that will allow us to solve complex problems, make better decisions and monitor impacts in real-time. The possibilities are endless. We can use data to see the connection between air pollution, hospital admissions for kids with asthma, and school attendance rates. Or we could

combine data from tractors applying fertilisers, with weather data and understand run-off patterns that affects the food safety of our aquaculture products. We can use data to predict patterns and take action to save money and improve products and services.

To take advantage of the digital revolution, Australia needs to develop new products, new services and business models. We also need to make sure that everyone can participate in this transformation. This is where the KEi comes in. Our purpose is to bring the power of digital technology and big data to all so that together we can solve complex problems through collaboration and innovation."

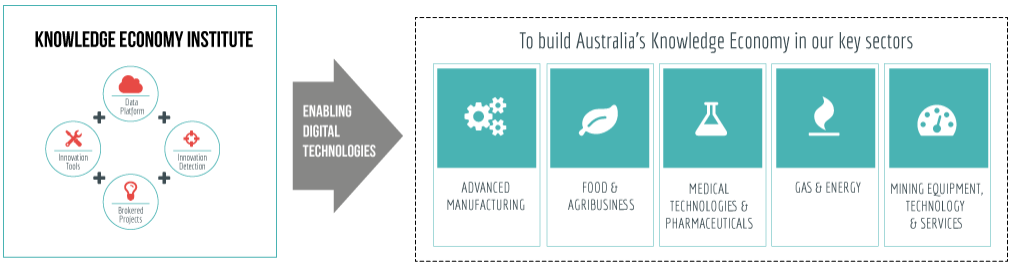


Figure 41: The Knowledge Economy Institute

E5 The Yield

The following text was provided by Ros Harvey – Founder of The Yield. "The Yield is an Australian agricultural technology company developing an integrated end-to-end intelligent solution for farmers, food processors, regulators and their suppliers. The solution will enable stakeholders across the agricultural supply chain to use digital technology to increase yields and reduce risk through reducing uncertainty.

The Yield was founded by Ros Harvey and is based in Tasmania. Ros was the Founding Director of the Sense-T program which pioneered IoT research in agriculture. Ros left the University of Tasmania to create The Yield in 2014. The Yield is taking a lead in commercial applications of IoT in Agriculture.

Ros Harvey says 'IoT technology is moving rapidly. The challenge is creating the business models that underpin successful commercialisation. The key is focusing on creating real value for customers.'

The Yield's first commercial offering will be in the $100 million Australian Oyster industry. They currently have a prototype being trialled in Tasmania. Their patented technology combines wide-area environmental and weather data with local sensor data at the harvest level which is transformed through data analytics to solve business problems. This data powers user-interfaces, which have been designed with the growers needs in mind and a focus on solving three business problems.

- Reducing unnecessary farm closures, potentially saving the industry over $7 million per year
- Improving labour scheduling by accurately predicting the water depth on leases
- Tracking food safety conditions for exports and consumers

The Yield has a pipeline of add-on solutions which it will progressively release as the product matures and is working with Bosch which is one of the world's largest manufacturers of sensing technology.

The Yield is also working with the Knowledge Economy Institute (KEi) and its partners to make its data available to the science community to fast-track research that is relevant to The Yield's end-user markets."

E6 Cisco IoE (internet of Everything) Innovation Centre Australia

The following text was derived from Cisco's Press release describing this initiative. "Cisco IoE Innovation Centre Australia is intended to help local and global organisations improve business outcomes. Their IoE Innovation Centre hub is planned to be focussed in Sydney and in Perth. The Perth hub is located on the Bentley Campus of Curtin University, with initially two large, long term partners: Woodside Petroleum and Curtin University. The South Korean start-up N3N is also partnering with the hub.

As an innovation centre and workplace for customers, partners, start-ups, universities and open communities, the Innovation Centre is pursuing its mission in three ways:

- Demonstrating IoE in action to solve business and public sector problems
- Engaging in rapid solution and product prototyping
- Research and investments in local resources, including companies and people

Cisco appears to be targeting agriculture, the resources sector and astronomy with this initiative. Together with their eco-system, they offer access to technology expertise, development equipment, some investment funds, joint marketing, and rapid prototyping. Their customers can take advantage of the infrastructure they have and introduce new capabilities and technology solutions as needed."

E7 The AIIA's Data and Analytics SIG

The following text was taken from Dr Roger Kermode, the SIG Chair. "The AIIA's Data and Analytics SIG was formed in May 2015 with the purpose of supporting and influencing Government and Businesses operating in Australia to maximise the use of data within their decision making processes at all levels with an organisation for the benefit of the Australia economy and Society."

AIIA's communiqué issued on conclusion of its IoT conference in March, 2015 committed the organisation to "Encourage the Federal Government to consider how smart IoT capability can be used to achieve the business, social and economic objectives of Government supported industry growth centres; promote partnerships between Government, industry and academia to drive innovation of IoT solution development and where required, the scaling of IoT applications; and build awareness of IoT capability across Government (federal and state)."

E8 The AIIA's Innovation SIG

The following text was provided by HP's Roger Lawrence – the Chair of this SIG. "The Innovation SIG was initiated in July 2012. The SIG is currently determining its strategic direction for 2015 and onwards and is keen to encourage input from and activities in all States and territories. The group is a horizontal SIG that traverses across industry vertical groups such as Government, Banking and Finance, Health etc.

The SIG aims to highlight true ICT innovation and promote ICT as an enabler of highly value-added products and services. While we believe in Innovation with all sizes of

organisation, we see a special role for the SIG in assisting newer and younger innovative companies get traction with Government and major commercial organisations."

E9 Genesys Design – an Australian Electronics M2M IoT Business

The following test was derived from an interview with Geoff Sizer – CEO and Founder of Genesys Design. "The Genesys team is equipped with a large depth and breadth of specialist skills, and such skills are core to maintaining a successful business over a 25 year period.

Genesys is a leader in partnering with infrastructure providers companies to provide M2M (Machine-to-Machine) technology solutions to our customers as their applications press toward the "internet of things". Typically any of the technologies on this page can be integrated and made to interoperate, with distributed internet-enabled monitoring and control.

Development of embedded systems and associated hardware, software and interfaces for such systems is very much "bread and butter" work for Genesys. The majority of products developed include embedded software, running on a platform of complexity that best suits both commercial and engineering requirements. They tackle a broad range of embedded systems developments, from simple/low-cost, through DSP and embedded Linux, to embedded PCs.

They also have developed sophisticated server applications that collect and aggregate data via the internet from remote platforms, store this data in local SQL databases, and provide remote control and data access functionality via HTML web pages.

All of these capabilities are necessary to deliver into the emerging Australian IoT market with customized designs for innovative services and solutions."

E10 Ericsson Energy Management – Regulation Has Made a Difference

The following information was derived from an interview with David Bridge, Sarah Goss, Warren Chaisatien and Pia Seeto – Ericsson. In February 2015 Ericsson published a White Paper titled "Understanding the Networked Society". This paper can be found at: http://www.ericsson.com/res/docs/whitepapers/wp-understanding-the-networked-society.pdf

This paper is largely a smart society paper highlighting all the key aspects of the internet of Things emphasising the network connectivity, the devices and the data and analytics that underpin an extensive array of applications. In Australia Ericsson is targeting the Utilities and Transport sectors.

In Utilities their work is focussed on smart electrical metering at present and this has led to an understanding of how difficult it is to offer solutions that make the consumers' life simpler while supporting all layers of Government. Each state has a different approach and there has over the last decade been a strong push to get Government to be consistent and promote competition for the benefit of the consumers. In fact, after years of work, it is only very recently that federal policy established that a single smart meter can be installed in a consumer premises and that meter can be used to deliver retail services from any retailer. This was achieved only when it was apparent that if left to market forces alone, each retailer would install their own meter so if the consumer

churned through several service providers they would end up with several smart meters installed and only the most recent one would be in use. Of course this is an obvious problem for the market and the consumer so the federal Government has put in place overarching legislation to prevent this absurd outcome.

This problem of multiple service providers across all the utility markets will create an even bigger problem and this is one area where federal policy can help. It would be a very poor outcome if a consumer found themselves with several gas meters, several electricity meters and several water meters when a single meter could adequately perform this function for all service providers.

E11 Adelaide's Smart City Initiative

The following text was derived from information provided by Peter Triantafilou, Office of Science, Technology and Research Department of State Development, South Australia.

"The Adelaide wifi network has been a successful joint undertaking between the South Australian Government, Adelaide City Council and Internode (iiNet subsidiary), utilising Cisco wifi Access Points to provide contiguous wifi coverage across the Adelaide CBD and selected surrounding areas.

An evolution of this initiative is to consider ways of leveraging the Adelaide Free wifi network through Smart City and internet of Things (IoT) opportunities.

The State Government and Adelaide City Council have entered into an MoU with Cisco to create a smarter, more connected city through a number of Pilot Project. Currently, two Pilot Projects – Smart Lighting and Smart Parking – are in the process of being implemented by the Adelaide City Council. Further pilot project opportunities are being considered.

An IoT Innovation Hub is also planned and will have a number of key elements including:

- An eco-system involving industrial partners, Universities, Start-up companies and Entrepreneurs
- A connection point for entrepreneurs to smart city data and sensors for rapid innovation of new applications that can be developed, built, tested and validated using Adelaide's data before being launched in a full scale environment
- Utilising ICT infrastructure and internet of Things – to interconnect a network of sensors to collect data and undertake further analysis using data analytics and "big data". This data generated from the network of sensors can be made available to entrepreneurs and start-ups to develop useful and commercially valuable applications. New business opportunities can be generated by treating a Smart City as an open platform in which entrepreneurs and developers can create and experiment with sensors and data collection hardware/software. Adelaide will be a Smart City "living laboratory"

Adelaide has been accepted into Cisco's global Smart and Connected Communities Lighthouse City program (the first mid-sized city globally, and the first city in Australia to receive this recognition). The relationship brings economic and social development opportunity and will raise Adelaide's global profile. Adelaide was accepted into Cisco's Lighthouse City program for a number of reasons:

- Strong visionary leadership (as demonstrated by the strong collaborative relationship between the Government and City Council as shown by the success of the Adelaide Free wifi project)
- An established innovation eco-system and ability to embrace smart city technologies
- The commitment to the MoU
- A defined scope of Smart City solutions for a mid-sized city"

E12 IPv6 Forum Australia

The following text was derived from an interview with Michael Biber – IPv6 Forum Chair in Australia. "Since 2001, IPv6 Forum Australia has been a force for local IPv6 development. It has supported major events and projects, including the annual IPv6 Summits and the pioneering Australian study 'IPv6 for e-Business'.

IPv6 Forum Australia has been engaged with international IPv6 discussion since 2000, in both the global IPv6 Forum and other IPv6-focussed internet bodies. Through the IPv6-SIG there have been long-term discussions with AGIMO and the Australian Government, resulting in the earliest comprehensive IPv6 transition plan for a national Government, copied around the world."

E13 Internet Society of Australia

The following information was extracted from the ISA web site. "Founded in 1996, internet Australia (The internet Society of Australia Limited, ACN 076 406 801; also formerly known as 'ISOC-AU') is the not-for-profit peak organisation representing all Australian internet users. We are a broad member-based organisation not an industry lobby group.

Our mission – "Helping Shape Our internet Future" – is to promote positive internet developments for the benefit of the whole community, including business, educational, Government and private internet users. Our directors and members hold significant roles in internet-related organisations and enable us to provide high level policy and technical information to internet user groups, Governments and regulatory authorities.

As the Australian chapter of the global internet Society, internet Australia leverages the expertise of a truly global network of experts as well as providing an Australian perspective on global issues. At a global level, the internet Society is a very active participant in many international forums for policy and regulation development, and is the administrative home for the internet Engineering Task Force (IETF): the open community of network designers, operators, vendors, and researchers who create the protocols and standards that are fundamental to internet operation."

E14 Pooled Energy

The following information was provided by John Reidl – Founding CEO of Pooled Energy. "Swimming pools represent about 30% of a typical household electricity bill and they require regular (often difficult) maintenance, including chemicals. "Pooled Energy" is an Australian Electricity Company using sensors and computer controls linked over the internet to:

- Manage your pool to reduce electricity consumption;
- Manage the pool chemistry; and
- Monitor the pool operation.

This provides the consumer with a ready-to-swim pool, reduced energy consumption and a reduced electricity bill while eliminating the need to purchase and dispense chemicals.

Pooled Energy Pty Ltd is a subsidiary of Efficiency Filters Pty Ltd and part of the Efficiency Filters Group. It is a fully operational and functional, high-technology based Electricity Retailer and Pool Services Company, selling an integrated bundle of Electricity and Pool Services to households and businesses with swimming pools. Having deployed its systems and technology in successful field (Beta) trials to paying customers during 2014, it is now in full commercial operation.

Pooled Energy was authorised by the Australian Energy Regulator on 12th December 2013 to operate in the Australian States and Territories regulated by it (ACT, NSW, South Australia, Tasmania and Queensland). Following additional approvals by the operator of the National Energy Market (NEM), it commenced operations with paying customers on 5-year contracts, commencing in July 2014.

Pooled Energy sells Retail Electricity to swimming pool owners and operators only. This includes the separate market segments of residential, shared and commercial pools. As part of a bundled offering, Pooled Energy provides:

- Electricity for the entire premises,
- An upgrade of the existing equipment at the pool to:-
    - Reduce its energy consumption,
    - Improve its operating efficiency,
    - Change the filter pump to variable speed,
    - Provide automatic chemical manufacturing and dispensing equipment,
    - Provide electronic sensors,
    - Upgrade the saltwater chlorinator in capacity and efficiency where required,
    - Upgrade plumbing where required,
    - Provide control electronics, known as the Intelligent Pool Controller
    - Add water level management
- Continual on-line automation, operation and optimisation of the pool. This is controlled by both the Intelligent Pool Controller and a Cloud based Central Computer system.
- Supply, delivery and automatic dispensing of any Pool Chemicals not manufactured on-site by the Pooled Energy equipment (typically:- salt, stabiliser and buffer),
- Maintenance of all equipment provided,
- An annual visit to visually verify the equipment, calibrate the sensors and update non-manufactured chemicals to the correct levels.
- Optional additional services (cleaning and leaf removal), at extra cost.
- Optional equipment additions (sweeps, heaters, water features), at extra cost.

The overall bundled offering provides the customer with major energy, chemical and operational cost savings, typically of an estimated $1,000 p.a. gross. Since the Establishment Fee is less than this and spread over time, most users have no net cash-out to sign up to a contract. The offer described is for Residential customers with swimming pools."

E15 Smarter Technology Solutions (STS)

The following text was provided by Danielle Storey – Director of Operations, Smarter Technology Solutions Smarter Technology Solutions. "(STS) is an example of a start-up initiative targeting the integration and aggregation of IoT solutions for enterprise. They help their customers collect, analyse and action data from various sources, systems and things, turning this data into valuable information and knowledge. STS, live and breathe innovation, digital disruption and emerging technology trends and the opportunity to collect and apply data from previously unconnected systems is what STS aim to achieve. STS Network Solutions Director, Ashley Hare noted that IoT isn't about reinventing the wheel, rather, we are helping customers to challenge their thinking and adopt smarter approach to technology to solve business problems.

As a specialised systems integrator, consultancy and service provider, STS aim to leverage internet of Things (IoT) based technologies to achieve three key outcomes:

- To create operational efficiencies
- To create new business
- To support other initiatives such as improved customer satisfaction, safety, security or to attain environmental/sustainability outcomes

Data is available everywhere and STS is able to help their customers to make sense of that data, collect it, analyse it and apply it to turn 'data' it into 'actionable intelligence'. This intelligence can be used to gain competitive advantage, automate manual activities and improve business workflows as well as to gain greater insight into their customers, processes and behaviours to make smarter business decisions. STS apply this approach to its various industry verticals including examples such as:

- Smart Cities
- Smart Buildings
- Smart Healthcare
- Industrial and Mining Industries
- Transport and logistics
- Utilities
- Retail
- Agriculture
- Automotive

STS Operations Director, Danielle Storey explained this approach further in saying that by not only focussing on the technology (the 'things') STS are able to understand the end user (people), context that the data and information is required in and how this is presented to the user (process), in the format required along with any systems that it must be integrated with (turning data into applied intelligence). This approach forces STS to look more broadly at IoT pulling together elements from various systems, vendors, technologies and capabilities to deliver holistic solutions and successful IoT outcomes. Due to the close industry engagement with vendors and industry experts, where the STS skillset end, one of the STS strategic partnerships begin (for example STS partner with leaders in Industrial computing, building automation and heavily specialised industries to ensure they can assist customers in the core Operational Technologies (OT) present within each sector). This simplifies the engagement for the end customer and reduces the complexity and multi-vendor IoT eco-system that customers would otherwise have to contend with and STS deliver and manage the engagement to the customer as a single provider."

F IoT Standards Bodies

This Appendix provides a very high level summary of the most significant standards bodies and their work associated with IoT. It is obvious from this that there are many standards bodies hard at work to support the IoT. In many ways this is important work but it also highlights the difficulties facing any business trying to make decisions about solution architectures and vendors. It is likely today that every IoT vendor can genuinely claim to be standards based while not necessarily interworking with any other vendor. The following text has been extracted from the web sites and press releases of the standards bodies, with an occasional clarifying comment from the authors of this Report.

F1 ITU

"ITU-T Study Group 13 – Future Networks including Cloud Computing and NGN – has approved new standards offering a definition of the internet of Things (IoT), characterizing the emerging IoT environment, and outlining the functional requirements of machine-oriented communication applications in an NGN context:

- Recommendation ITU-T Y.2060 "Overview of the internet of Things"
- Recommendation ITU-T Y.2061 "Requirements for support of machine-oriented communication applications in the NGN environment"

ITU-T Y.2060 marks ITU members' approval of a definition of IoT, terming it: "A global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies."

Recommendation ITU-T Y.2060 provides an overview of the internet of Things (IoT), clarifying the concept and scope of IoT, identifying its fundamental characteristics and high-level requirements, and offering a detailed description of the IoT reference model. Additionally, the standard presents an informative appendix discussing the IoT eco-system and the business models of which it will be composed.

The definition is accompanied by a qualification which notes that, from a broad perspective, IoT can be perceived as a vision with technological and societal implications; which will, through the exploitation of identification, data capture, processing and communication capabilities, make full use of "Things" to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

Recommendation ITU-T Y.2061 provides an overview of machine-oriented communication (MOC) applications in next-generation network (NGN) environments; covering the NGN extensions, additions and device capabilities required to support MOC applications. Additionally, the standard's appendices describe the actors in an MOC eco-system and the roles they are to play, as well as a number of use cases relevant to the study of MOC applications in an NGN environment.

SG 13 has also approved Recommendation ITU-T Y.2080, Functional architecture of distributed service networking, and has consented the approval of another fourteen new standards, the most noteworthy being Recommendations ITU-T Y.2069, *Terms and definitions of the internet of Things*; Y.2705, *Minimum Security Requirements for Interconnection of Emergency Telecommunications Service (ETS)*; Y.2027, Functional Architecture of Multi-connection; and Y.2063, Framework of Web of Things."

F2 LoRa Alliance

"LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated Things in regional, national or global network. LoRaWAN target key requirements of internet of things such as secure bi-directional communication, mobility and localization services. This standard will provide seamless interoperability among smart Things without the need of complex local installations and gives back the freedom to the user, developer, businesses enabling the role out of internet of Things.

LoRaWAN network architecture is typically laid out in a star-of-stars topology in which gateways is a transparent bridge relaying messages between end-devices and a central network server in the backend. Gateways are connected to the network server via standard IP connections while end-devices use single-hop wireless communication to one or many gateways. All end-point communication is generally bi-directional, but also supports operation such as multicast enabling software upgrade over the air or other mass distribution messages to reduce the on air communication time.

Communication between end-devices and gateways is spread out on different frequency channels and data rates. The selection of the data rate is a trade-off between communication range and message duration. Due to the spread spectrum technology, communications with different data rates do not interfere with each other and create a set of "virtual" channels increasing the capacity of the gateway. LoRaWAN data rates range from 0.3 kbps to 50 kbps. To maximize both battery life of the end-devices and overall network capacity, the LoRaWAN network server is managing the data rate and RF output for each end-device individually by means of an adaptive data rate (ADR) scheme.

National wide networks targeting internet of things such as critical infrastructure, confidential personal data or critical functions for the society has a special need for secure communication. This has been solved by several layer of encryption:

- Unique Network key (EUI64) and ensure security on network level
- Unique Application key (EUI64) ensure end-to-end security on application level
- Device specific key (EUI128)

LoRaWAN has several different classes of end-point devices to address the different needs reflected in the wide range of applications:

- Bi-directional end-devices (Class A): End-devices of Class A allow for bi-directional communications whereby each end-device's uplink transmission is followed by two short downlink receive windows. The transmission slot scheduled by the end-device is based on its own communication needs with a small variation based on a random time basis (ALOHA-type of protocol). This Class A operation is the lowest power end-device system for applications that only require downlink communication from the server shortly after the end-device has sent an uplink transmission. Downlink communications from the server at any other time will have to wait until the next scheduled uplink.
- Bi-directional end-devices with scheduled receive slots (Class B): In addition to the Class A random receive windows, Class B devices open extra receive windows at scheduled times. In order for the End-device to open its receive window at the scheduled time it receives a time synchronized Beacon from the gateway. This allows the server to know when the end-device is listening.

- Bi-directional end-devices with maximal receive slots (Class C): End-devices of Class C have nearly continuously open receive windows, only closed when transmitting. Class C".

F3 SIGFOX

"SIGFOX provides an end-to-end solution for the IoT communication chain, from objects through to information systems, with unprecedented pricing models and low energy consumption. As a network operator SIGFOX operates fixed-location transceivers enabling your objects to be connected "out of the box". However contrary to the telecommunication networks, the SIGFOX transceivers and the entire SIGFOX connectivity solution has been developed, built and deployed to only serve the low throughput M2M and IoT applications.

As an operated long-range network, SIGFOX provides connectivity without the need to deploy specific network infrastructures for each application. The SIGFOX network is simply available to any object equipped with our certified connectivity solutions. From an application point of view, the SIGFOX connectivity solution functions as follows:

- SIGFOX compatible modems are integrated within the physical objects by our certified partner network
- The objects instruct the modems to send messages whenever and wherever needed
- The transmitted data is picked up by the SIGFOX transceivers, and routed to our managed service
- The SIGFOX servers verify the data integrity and route the messages to the application's IT system

The SIGFOX network is highly scalable and built for a high volume of devices. It provides two-way communications with your devices and is surprisingly easy to integrate with software applications.

SIGFOX uses a UNB (Ultra Narrow Band) based radio technology to connect devices to its global network. The use of UNB is key to providing a scalable, high-capacity network, with very low energy consumption, while maintaining a simple and easy to rollout star-based cell infrastructure.

The network operates in the globally available ISM bands (license-free frequency bands) and co-exists in these frequencies with other radio technologies, but without any risk of collisions or capacity problems. SIGFOX currently uses the most popular European ISM band on 868MHz (as defined by ETSI and CEPT) as well as the 902MHz in the USA (as defined by the FCC), depending on specific regional regulations.

Communication on SIGFOX is secured in many ways, including anti-replay, message scrambling, sequencing, etc. The most important aspect of transmission security is however that only the device vendors understand the actual data exchanged between the device and the IT systems. SIGFOX only acts as a transport channel, pushing the data towards the customer's IT system.

An important advantage provided by the use of the narrow band technology is the flexibility it offers in terms of antenna design. On the network infrastructure end it allows the use of small and simple antennas, but more importantly, it allows devices to use inexpensive and easily customizable antennas.

The SIGFOX protocol is compatible with existing transceivers and is actively being ported to a growing number of technical platforms."

F4 AllSeen Alliance

"Their mission is to enable widespread adoption and help accelerate the development and evolution of an interoperable peer connectivity and communications framework based on AllJoyn for devices and applications in the internet of Everything. The AllSeen Alliance is committed to making the internet of Everything secure.

The code used by the AllSeen Alliance has been open source from the beginning. When everyone jointly develops and uses the same freely available code, companies can develop innovative services on top of it and get to market faster.

The Alliance is open to anyone interested in collaborating and contributing to the AllJoyn open source project. It incorporates more than 20 of the most important open technical standards in its work.

The AllSeen Alliance has launched "Designed for AllSeen" – a comprehensive certification and compliance program with third-party test labs to ensure smart products in the eco-system are truly interoperable. By joining a network of companies, products and applications, certified products that display the AllSeen certification mark convey that they are smart products and are part of a truly interoperable eco-system for the internet of Everything.

AllJoyn supports Android, iOS, Linux, OpenWRT Windows, OS X and embedded systems with limited memory and processing power.

The Alliance manages the AllJoyn open source project with software code using open standards to enable all the 'things' in the internet of Things to work together. The code is available for download.

The initiative includes more than160 member companies including leading consumer electronics manufacturers, home appliance makers, automotive companies, internet of Things cloud providers, enterprise technology companies, innovative start-ups, chipset manufacturers, service providers, retailers and software developers."

F5 Open Interconnect Consortium (OIC)

Following is an extract from the OIC website openinterconnect.org. This Consortium was established and is led by Samsung, Intel, Media Tek, Cisco and GE who all have seats at their board.

"Their mission is to support the connecting of the next 25 billion devices for the internet of Things. Providing secure and reliable device discovery and connectivity across multiple OSs and platforms. There are multiple proposals and forums driving different approaches. But no single solution addresses the majority of key requirements.

We need industry consolidation around a common, interoperable approach. The OIC supports a broad industry consortium of companies to create a scalable solution.

They are working on the specification, certification & branding to deliver reliable interoperability -- a connectivity framework that abstracts complexity. This standard will be an open specification that anyone can implement and is easy for developers to use.

It will include IP protection & branding for certified devices (via compliance testing) and service-level interoperability. There will also be an Open Source implementation of the standard. This Open Source implementation will be designed to enable application developers and device manufacturers to deliver interoperable products across Android, iOS, Windows, Linux, Tizen, and more.

Consumers, Enterprise, Industrial, Automotive, Health, etc. who want smart devices to easily interconnect and communicate with appliances, embedded devices, etc all need this. Developers of operating systems, platforms, and applications who want their products to interoperate seamlessly across many brands and eco-systems. End users who want consistent levels of security and identity across smart devices down to the smallest connected appliance.

Their goal is to define a comprehensive communications framework to enable emerging applications in all key vertical markets. The framework must enable multiple new modes of communication, such as Peer-to-Peer, Mesh & Bridging, Reporting & Control, etc.

The framework should include a consistent implementation of identity, authentication and security across the modes of User ID, Enterprise / Industrial ID &Credentials. It should include a sense of proximity for the internet of Things and Wearable devices and include support for On-boarding and Provisioning. And the framework must support a "building block" architecture and provide an Open Source implementation.""

F6 ETSI

ETSI, the major European telecommunications standards body has developed a program of work for the next year and can be found here:
http://www.etsi.org/images/files/WorkProgramme/etsi-work-programme-2015-2016.pdf

An extract from this Program follows highlighting ETSI's attention to IoT and M2M.

'This program details their work in M2M and IoT.

An ever increasing number of everyday machines and objects are now embedded with sensors or actuators and have the ability to communicate over the internet. Collectively they make up the 'internet of Things' (IoT). The IoT draws together various technologies such as Machine-to-Machine (M2M) service platforms and wireless sensor networks.

Potential applications and services include smart devices, smart cities, smart grids, the connected car, eHealth, home automation and energy management, public safety and remote industrial process control. Machine-to-Machine Communications It is widely acknowledged that the IoT and M2M communications will change the way we live and work through new and innovative services, while at the same time offering unprecedented new business opportunities. But the development of the IoT is complicated by the use of different platforms, proprietary software, protocols and networking options, and the complexity of seamlessly connecting all the disparate devices which together make up the IoT is hampering its growth.

Smart Appliances Our own Smart M2M Communications committee (TC SmartM2M) addresses services and applications, including aspects of the IoT. We continue to update our existing specifications on M2M service platform interfaces on a regular basis. Smart appliances In 2015 we will look in particular at the use of the service platform to interface with smart appliances, allowing interoperability of applications and 'plug and play' connectivity.

In the future, domestic and industrial appliances will be highly intelligent, networked smart devices. To ensure such systems are commercially successful and widely adopted, it must be possible to add new appliances from different vendors. These systems will also need to be able to communicate with service platforms from different energy service providers. This requires open interfaces. Interoperability will therefore be a key factor in creating an eco-system for the IoT, and the availability of standardised test suites will be an important enabler. In line with our action plan for the creation of a new standard for smart appliances communications, we expect to produce the first ETSI Technical Specifications (TSs) in this area by mid-2015.

One of these will define a framework for smart appliances communications based on ETSI M2M and oneM2M specifications. A second TS will review the European Commission (EC) study on smart appliances ontologies and adapt it to the structure of a standard, and then develop the ontology and map it onto ETSI M2M and possibly oneM2M standardised resources and services. In parallel, we are developing a four-part TS for the conformance testing of the ontology and the communications framework for smart appliances."

F7 Industrial Interconnect Consortium – IIC

"The Industrial internet Consortium (IIC) is the open membership, international non-profit consortium that is setting the architectural framework and direction for the Industrial internet. Founded by AT&T, Cisco, GE, IBM and Intel in March 2014, the IIC's mission to coordinate vast eco-system initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards.

Current scope of activities:

- Deliver best practices, reference architectures, case studies, and standards requirements to ease deployment of connected technologies;
- Utilize existing and creating new industry use cases and test beds for real-world applications;
- Influence the global standards development process for internet and industrial systems;
- Facilitate open forums to share and exchange real-world ideas, practices, lessons, and insights;
- Build confidence around new and innovative approaches to security.

By joining the Industrial internet Consortium you can:

- Influence the requirements development, technology adoption, standards development process and future direction of the Industrial internet by joining with leaders in technology, manufacturing, academia and the Government on working committees to capture requirements and priorities
- Participate in selected research projects and test beds
- Have a role in creating best practices, patterns, use cases and standards roadmaps and other deployable content of the Industrial internet
- Network with industry innovators to create and develop critical new business collaborations
- Minimize risk by keeping up with technology developments
- Gain industry recognition for yourself and your company through speaking engagements, roundtable participation, publishing venues and more.

Membership in the IIC is open to any organization, regardless of size or mission. For a current listing of members, please visit www.iiconsortium.org."

F8 Thread Group

"The Thread Group formed in July 2014. The organization is now launching its internet of Things technical specification and says it will kick off a certification program in September, 2015. It is a supporter of an all IPv6 mesh network for low power device connectivity.

The Thread Group also announced that Qualcomm Inc. (Nasdaq: QCOM) has joined its Board of Directors, bringing the total number of sponsor companies to ten, including big names like Google (Nasdaq: GOOG)-owned Nest, Samsung Corp. and Tyco International Ltd. (NYSE: TYC; London: TYI).

Thread is designed to enable a second network in fixed locations like smart homes and other connected facilities. Combining low power and high reliability, the protocol isn't meant to replace traditional wifi, but instead enable another layer of networking for utilitarian devices like sensors, lighting controls and thermostats.

Several characteristics make Thread suitable for an in-home machine-to-machine network. The protocol supports a self-healing mesh architecture with the ability to scale to hundreds of devices. It includes "banking-class encryption," and, built on standards like IPv6 Low-power Wireless Personal Area Network (6LoWPAN), it will work with millions of existing wireless devices with just a software upgrade. Thread is also application agnostic, meaning it sits below the application layer and will work with any application developed on top."

F9 Open Data Platform Consortium (ODP)

"The Open Data Platform Initiative (ODP) is a shared industry effort focused on promoting and advancing the state of Apache Hadoop® and Big Data technologies for the enterprise. For more information refer to: http://opendataplatform.org/

Platinum members are General Electric, Hortonworks, IBM, Infosys, Pivotal, Telstra, SAS. Gold members are Altiscale, Capgemini, CenturyLink, EMC, PDLT, Splunk, Teradata, Verizon, VMwere, Wandisco and Silver members are BMC, Data Torrent, Linaro, Syncsort, Squid, Unifi, ZData, Zettaset.

Their mission is to:

- Accelerate the delivery of Big Data solutions by providing a well-defined core platform to target.
- Define, integrate, test, and certify a standard "ODP Core" of compatible versions of select Big Data open source projects.
- Provide a stable base against which Big Data solutions providers can qualify solutions.
- Produce a set of tools and methods that enable members to create and test differentiated offerings based on the ODP Core.
- Reinforce the role of the Apache Software Foundation (ASF) in the development and governance of upstream projects.
- Contribute to ASF projects in accordance with ASF processes and Intellectual Property guidelines.
- Support community development and outreach activities that accelerate the rollout of modern data architectures that leverage Apache Hadoop®.

- Will help minimize the fragmentation and duplication of effort within the industry."

F10 OneM2M

For more detail of OneM2M; http://www.onem2m.org/

"Eight of the world's regional ICT standards bodies have come together to create oneM2M.

The regional standards bodies are joined by six globally active industry consortia.

And over 200 member companies from across all industrial sectors.

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. Initially, oneM2M shall prepare, approve and maintain the necessary set of Technical Specifications and Technical Reports for use cases, protocols, service layer definitions, security and privacy issues, reachability, data sharing models etc.

OneM2M exists to enable all of these disparate technologies to talk to one another in a single framework. Take the example of excavation equipment in the mining industry, an industry with a huge footprint across the globe of heavy industrial plant and site equipment in different locations. A mining company may run excavators made by Caterpillar, JCB, Volvo and Doosan; each may have M2M capability embedded by the manufacturer.

The technologies and equipment may be aging, in some cases up to 20 years old. M2M capabilities may have largely been deployed to assist the manufacturer and focus on functions such as preventative maintenance, vehicle tracking and monitoring the number of hours the equipment has worked for. The data and information is fed back to the manufacturer to aid its design of new products, to help it set prices for leasing of equipment and to understand the different loads put on vehicles performing specific tasks or working in specific terrains and climates.

Much of the data would be of great value to the mining company. Knowing, for example, that at a mine in Chile a machine needs to run longer to shift the same volume of material than is required at a mine in Siberia would be useful. Another example might involve the same type of excavator requiring a new part more rapidly at the site in Siberia than is required in Chile.

The challenge involved in extracting all of this data is that each excavator is likely to have a proprietary system that typically communicates back to its manufacturer; the data collected from a Caterpillar excavator will be collected in a different way and in a different format from a Doosan excavator or a JCB. The lack of standardisation radically increases the complexity involved in trying to correlate the data from such disparate sources and extract valuable insights from it.

An independent service provider might be the answer provided it is trusted by both the mining company and the excavator manufacturer to share only relevant data with each party.

An interworking framework like oneM2M holds the promise of enabling a system in a Doosan excavator, managed by a specialist provider, to integrate with the systems of Doosan and the mining company. The value each company gains from the insights can be enormous. For the mining company, it encompasses data on productivity, which machines work best in which situations, which machines are most effective and which are most durable."

F11 ISO/IEC JTC 1 – Information Technology

For more details about the ISO and it is work on information technology go to:
http://www.iso.org/iso/jtc1_home.html

"JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technology (ICT) standards for business and consumer applications. Additionally, JTC 1 provides the standards approval environment for integrating diverse and complex ICT technologies. These standards rely upon the core infrastructure technologies developed by JTC 1 centres of expertise complemented by specifications developed in other organizations.

Special Working Group 5 (internet of Things)
http://www.iso.org/iso/internet_of_things_report-jtc1.pdf- driven from Korea – members Austria, Belgium, Canada, China, France, Germany, Japan, Republic of Korea, Russia, Singapore, South Africa, Switzerland, the United Kingdom, and the United States.

The ISO/IEC JTC 1/SWG 5 was chartered to by JTC 1 in 2012 and modified in 2013 with the following "Terms of Reference":

1. Identify market requirements and standardization gaps for internet of Things (IoT).
2. Encourage JTC 1 SCs and WGs to address the need for ISO/IEC standards for IoT.
3. Facilitate cooperation across JTC 1 entities.
4. Promote JTC 1 developed standards for IoT and encourage them to be recognized and utilized by industry and other standards setting organizations.
5. Facilitate the coordination of JTC 1 IoT activities with IEC, ISO, ITU and other organizations that are developing standards for IoT.
6. Periodically report results and recommendations to JTC 1/SWG on Planning.
7. Provide a written report of activities and recommendations to JTC 1 in advance of each JTC 1 plenary meeting.

8. Study IoT reference architectures/frameworks and provide a study report. This study report should be written so it could be referenced in a possible JTC 1 New Work Item Proposal on IoT."

F12 World IoT Forum

For more detail regarding the World IoT Forum go to www.iotwf.com. "The internet of Things World Forum (IoTWF) was initially established in the US by Intel, Cisco and others. It is now driven by a steering committee. Members are comprised of industry visionaries, technologists, executives, and educators who are committed to accelerating the awareness and adoption of internet of Things (IoT) technologies.

The Mission of the Steering Committee:

- Establish a premier IoT leadership forum which provides high-level direction to accelerate the market adoption of the internet of Things
- Provide opportunities and infrastructure for members to collaborate, network, partner and build IoT eco-systems
- Coordinate and arbitrate the plans of multiple working groups
- Establish and foster lines of communications between members and working groups
- Set the framework for the next IoT World Forum

The Forum hosts an annual conference and has established a number of subsidiary regional events around the globe. Over 150 companies have joined this forum for information sharing and thought leadership. These include ICT vendors, start-ups, city councils, carriers and service provider, universities and others.

Their Forum events provide a forum for discussion and sharing of best practices on every front – flexibility, scalability, security, availability, and connectivity -- as individuals, companies, and Governments accelerate and optimize their IoT deployments, driving dramatic gains in efficiency, economic value, and quality of life."

F13 Transaction Performance Processing Council (TPC)

"The TPC is a non-profit corporation founded to define transaction processing and database benchmarks and to disseminate objective, verifiable TPC performance data to the industry.

The term transaction is often applied to a wide variety of business and computer functions. Looked at as a computer function, a transaction could refer to a set of operations including disk read/writes, operating system calls, or some form of data transfer from one subsystem to another.

While TPC benchmarks certainly involve the measurement and evaluation of computer functions and operations, the TPC regards a transaction as it is commonly understood in the business world: a commercial exchange of goods, services, or money. A typical transaction, as defined by the TPC, would include the updating to a database system for such things as inventory control (goods), airline reservations (services), or banking (money).

In these environments, a number of customers or service representatives input and manage their transactions via a terminal or desktop computer connected to a database. Typically, the TPC produces benchmarks that measure transaction processing (TP) and database (DB) performance in terms of how many transactions a given system and database can perform per unit of time, e.g., transactions per second or transactions per minute.

The TPC has announced plans to develop a set of benchmarks for the performance of IoT hardware and software. It has set up a new working group, chaired by Raghunath Nambiar, a distinguished engineer at Cisco, "tasked with developing industry standard benchmarks for both hardware and software platforms associated with the IoT."

Its justification for the move is: "As the number of interconnected platforms continues to multiply, vendors and customers increasingly require an impartial means of comparing performance, cost-of-ownership and energy consumption across a widening array of hardware and software systems.""

F14 IEEE, P2413 – Draft Standard for an Architectural Framework for IoT

"This IEEE standard P2413 will define an architectural framework for the internet of Things, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains.

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety." Furthermore, this standard provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. The reference architecture also addresses how to document and, if strived for, mitigate architecture divergence. This standard leverages existing applicable standards and identifies planned or ongoing projects with a similar or overlapping scope.

Most current standardization activities are confined to very specific verticals and represent islands of disjointed and often redundant development. The architectural framework defined in this standard will promote cross-domain interaction, aid system interoperability and functional compatibility, and further fuel the growth of the IoT market. The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.

This standard will help to reduce current fragmentation in the various IoT verticals. By addressing the need for an IoT architectural framework, IEEE will fulfil its mission to benefit humanity by increasing the interoperability and portability of IoT solutions to both the industry and the end consumer.

In the IEEE, there are more than 350 IEEE standards that are applicable to IoT, 40 of which are being revised to better support IoT. Furthermore, there are more than 110 new IoT related IEEE standards in various stages of development. The IEEE is also sponsoring 10 or more different IoT advocacy and support groups.

The list of IEEE-based standards and activities is too large to be included here. It may be found at http://standards.ieee.org/innovate/iot/stds.html. A list of IEEE projects under

development that are related to IoT can be found at http://standards.ieee.org/innovate/iot/projects.html. An IETF presentation at the Santa Clara roundtable presented the following list of IETF activities, which include providing IPv6 on small devices and several other issues that are protocol agnostic. Building on the success of 6LoWPAN (which supports IPv6 on IEEE 802.15.4™), IETF has the following active working groups (see www.ietf.org for additional details):

- 6Lo—IPv6 over Networks of Resource---constrained Nodes (extending 6LoWPAN to additional layer 2 technologies)
- 6man—IPv6 Maintenance
- 6TiSCH—IPv6 over TSCH mode of IEEE 802.15.4e™
- ACE—Authentication and Authorization for Constrained Environments
- ROLL—Routing Over Low power and Lossy networks
- DICE—DTLS In Constrained Environments
- LWIP—Light---Weight (IP) Implementation Guidance

The IEEE Wireless Communications magazine has issued a call for papers for an edition looking at enabling wireless communication and networking technologies for IoT. Among the topics listed is "IoT access network technologies and capillary networks." Manuscripts are due on 15 October 2015."

F15 Other organizations and related activities include:

- 3rd Generation Partnership Project (3GPP): http://www.3gpp.org/
- Alliance for Telecommunications industry Solutions (ATIS): http://atis.org/
- Allseen Alliance: https://allseenalliance.org/
- Bluetooth® SIG: https://www.Bluetooth.org/en-us
- Broadband Forum (BBF): http://www.broadband-forum.org/
    - TR-069: www.broadband-forum.org/technical/download/*TR-069*.pdf
- Consumer Electronics Association (CEA): http://www.ce.org/
- Digital Living Network Alliance (DLNA): http://www.dlna.org/
- Eclipse M2M industry Working Group: http://eclipse.org/org/workinggroups/m2miwg_charter.php
- European Telecommunications Standards Institute (ETSI): http://www.etsi.org/
- GSM Association (GSMA): http://www.gsma.com/
- Health Level Seven International (HL7): www.hl7.org/
- Home Gateway Initiative (HGI): http://www.homegatewayinitiative.org/
- Industrial internet Consortium (IIC): www.iiconsortium.org
- Institute of Electrical and Electronics Engineers (IEEE) www.ieee.org
    - IEEE 802.15.4: http://ieee802.org/15/pub/TG4.html
    - IEEE P2413: http://standards.ieee.org/develop/project/2413.html
- International Electro-technical Commission (IEC): www.iec.ch
- International Organization of Standardization (ISO): www.iso.org
- International Society of Automation (ISA): www.isa.org
- International Telecommunication Union (ITU): www.itu.int
- International Telecommunication Union – Telecommunications (ITU-T): http://www.itu.int/en/ITU-T/Pages/default.aspx
    - ITU-T Focus Group M2M: http://www.itu.int/en/ITU-T/focusgroups/m2m/Pages/default.aspx
- internet Engineering Task Force (IETF): www.ietf.org
- internet Protocol Smart Objects (IPSO) Alliance: www.ipso-alliance.org
- IoT European Research Cluster (IERC): http://www.internet-of-things-research.eu/
- oneM2M: oneM2M.org
- Open Interconnect Consortium (OIC): http://openinterconnect.org/

- Open Mobile Alliance (OMA): http://openmobilealliance.org/
- OpenIoT: http://openiot.eu/
- Organization for the Advancement of Structured Information Standards (OASIS): https://www.oasis-open.org/
    - OASIS Message Queuing Telemetry Transport (MQTT): http://mqtt.org/
- Personal Connected Health Alliance (PCHA): http://www.continuaalliance.org/pchalliance
- SAE International (SAE): http://www.sae.org/
- Smart Grid Interoperability Panel (SGIP): http://www.sgip.org/
- Smart Manufacturing Leadership Coalition (SMLC): www.smartmanufacturingcoalition.org
- Thread Group: http://www.threadgroup.org/
- Weightless SIG: http://www.weightless.org/
- World Wide Web Consortium (W3C): http://www.w3.org/
- Zigbee Alliance: http://zigbee.org/

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

PO Box 444
Milsons Point
NSW 1565

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