



30<sup>th</sup> November 2017

Department of Industry  
<http://industry.gov.au/digitaleconomy>

To whom it concerns,

## **Submission re: The Digital Economy – Opening up the Conversation**

Thank you for the opportunity for Internet of Things Alliance Australia (IoTAA) to submit a response to the 'Digital Economy: Opening up the Conversation' consultation paper.

Digital savvy customers are making demands that are already redefining our industries from Food and Agribusiness to Transport to Manufacturing, driving businesses and industries at large to provide not only a product, but also real-time services that deliver experiences.

New business models have emerged and are emerging that undermine traditional approaches, bringing a world of benefit and uncertainty for consumers and a world of pain for pre-digital businesses with significant legacy investments.

Where, in the past, digital was considered an appendage to business as usual, today digital **is business as usual**. Now, more than ever, as a nation we must consider how to disrupt our own legacy businesses before new entrants, unencumbered by pre-digital investments, do it for us.

IoT, which encompasses the Industrial Internet of Things, Industry 4.0 and Consumer IoT, demands a systems view of products, services and experiences which in turn requires increased collaboration between government, business (demand and supply), research and people to make it work.

We would like to highlight three key points of our submission. The need for:

1. A shared narrative to lead and guide nation-wide engagement in the challenge and opportunity of the digital/IoT economy and the economic and social benefits this 'market making' will deliver both domestically and for export. This should highlight goals that we all share, in areas such as export, leadership in key sectors and citizen engagement.
2. Adapting the Australian workforce to be skilled to meet not only the demands (and jobs) of the digital economy, but also to drive leadership in industries where Australia can leverage its natural advantage.
3. Accelerating the understanding and adoption of key digital principles and practices that underpin a vibrant digital economy. These include:
  - a. Managed widespread data sharing

[www.iot.org.au](http://www.iot.org.au)

1

- b. Security in digital services
- c. Ready spectrum availability (e.g. for 5G) and wide connectivity coverage
- d. Early collaborative experimentation of new business models and regulation across government, industry, start-ups, research organisations and community

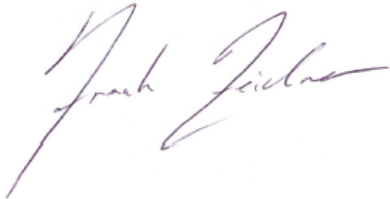
We welcome the opportunity to discuss our thoughts in more detail with the Department at your convenience.

Should you wish to discuss any aspect of this submission, kindly contact Frank Zeichner or Geof Heydon and they will coordinate our further input.

Frank Zeichner – [frank.zeichner@iot.org.au](mailto:frank.zeichner@iot.org.au) 0408 233 762

Geof Heydon – [geof.heydon@iot.org.au](mailto:geof.heydon@iot.org.au) 0419 203 993

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Frank Zeichner', written in a cursive style.

Frank Zeichner

Chief Executive Officer  
IoT Alliance Australia

[www.iot.org.au](http://www.iot.org.au)

## Submission: Consumer representation: Review of section 593 of the *Telecommunications Act 1997* Issues paper

This submission can be published on the World Wide Web: Yes

**Date of submission:** 30<sup>th</sup> November, 2017

Logo of organisation – if an organisation making this submission



Name and contact details of person/organisation making submission:

Frank Zeichner, Chief Executive Officer, IoTAA

### **General comments**

The Internet of Things (IoT) technologies and practices are now at the heart of the digital transformation of industry, the economy and society. IoT has the potential to significantly improve Australia's competitiveness, productivity, jobs and export. It is estimated to potentially expand the Australian economy by up to \$120 billion by 2025.

While the impact of IoT on our businesses and lives will be profound over the next five to ten years, it will depend very much on how well users understand and trust the changing IoT paradigm of increasing levels of data collection, sharing, personalisation and new permission regimes – to mention a few.

IoT includes the collection of data through sensors and social media, connectivity of sensors to networks, IP communications networks, data storage and curation, cloud computing, analytics, user interface, applications and automation and artificial Intelligence. IoT enables the creation of virtual digital time-based data 'twins' of the physical environment, interactions, customer preferences etc. which opens insight and capability to oversee, predict and automate services and enable new business models.

The dramatic and relentless decrease in cost of the above technologies enables data collection and data-driven analytics and automation at an unprecedented level. In addition, IoT promises to change the balance from government and corporates dominating the generation of data, by enabling small businesses, communities and citizens to generate significant quantities of data, share that data and unleash greater opportunities for innovation.

## About IoT Alliance Australia, (IoTAA)

IoTAA is a not-for-profit industry association incorporated in July 2016. We are the peak Australian IoT industry body. The vision of IoTAA is:

**“To empower industry and society by accelerating IoT innovation and adoption for Australian economic and societal benefit.”**

We see ourselves as a prime instigator of IoT collaboration and advancement in Australia through a network which includes community and citizens, government, research and industry – all of whom contribute to our work.

IoTAA now has over 380 organisation members and 700 participants and is growing at 5% per month. IoTAA runs seven programs (workstreams) covering:

- Collaboration
- Smart industries and cities
- Data use, access and privacy
- Spectrum availability and licensing
- Cyber security and network resilience
- IoT start-up innovation and
- Platforms and Interoperability.

For more details, please visit our website [www.iot.org.au](http://www.iot.org.au)

## Response

### 1. How are advances in digital technology changing the way you work, your industry and your community?

IoTAA operates across the providers, suppliers and users of IoT technology and services. We currently focus on five market sectors: Water, Energy, Transport, Food and Agribusiness, and Smart Cities and work to address the key enablers and inhibitors for successful adoption of IoT.

Key areas that are changing the way we work due to IoT and which affect how successful we will be in advancing our economy and society are:

- **How we work together** – Major gains in efficiency and business innovation are realised by marrying IoT technologies and practices with domain understanding to address industry and societal challenges. This requires far greater collaboration across technology and service providers, supply chain nodes, customers, industries, research, community and government. IoTAA is developing and connecting the Australian IoT ecosystem to accelerate the process.
- **How we share and protect data** – Understanding what data we have, its accessibility and how it is classified and shared is an increasingly important digital economy driver. IoT enables unprecedented volumes of data to be generated by a plethora of sources. However, the real economy-wide benefits will only be realised through the establishment of a trusted, managed data sharing regime that allows us to connect hitherto isolated data islands trapped within businesses, government, research organisations and communities.
- **How we secure services and build trust** – With widespread connectivity and increasing access to and connection of IoT sensors and devices, there is a growing security risk to people and services. IoT leverages the Internet and, as such, relies on existing Internet security provisions. IoTAA is determined to improve security practices through better awareness, skills and transparent market signals that expose bad players and support good practices.
- **How we adapt our business models and regulation** – Connecting the supply chain with customers, services utilities, cities etc. introduces many opportunities for service innovation and productivity gains, but only if industry is flexible and open to opportunities. Legacy national regulation is an inhibitor in this respect, rendering Australian businesses unable to compete with international players.
- **How we raise awareness and excitement across industry and community** – Anecdotally, Australians seem less enthused and ready to embrace new IoT technologies than our Asian neighbours and competitor/customer nations. Uncertainty and elements of fear are evident regarding the onset of new digital technologies, possibly attributed to concerns regarding the potential for job loss and the lack of security of services. Industry also seems less aware of the potential opportunity afforded by IoT. This undermines Australia's ability to increase its competitiveness and productivity.
- **How we develop the skills to support the digital economy** – Shortages in important IoT technology skills are limiting the rate of adoption in Australia. Looking to a future where the jobs mix will shift significantly to favour those with digital skills, we are witnessing a

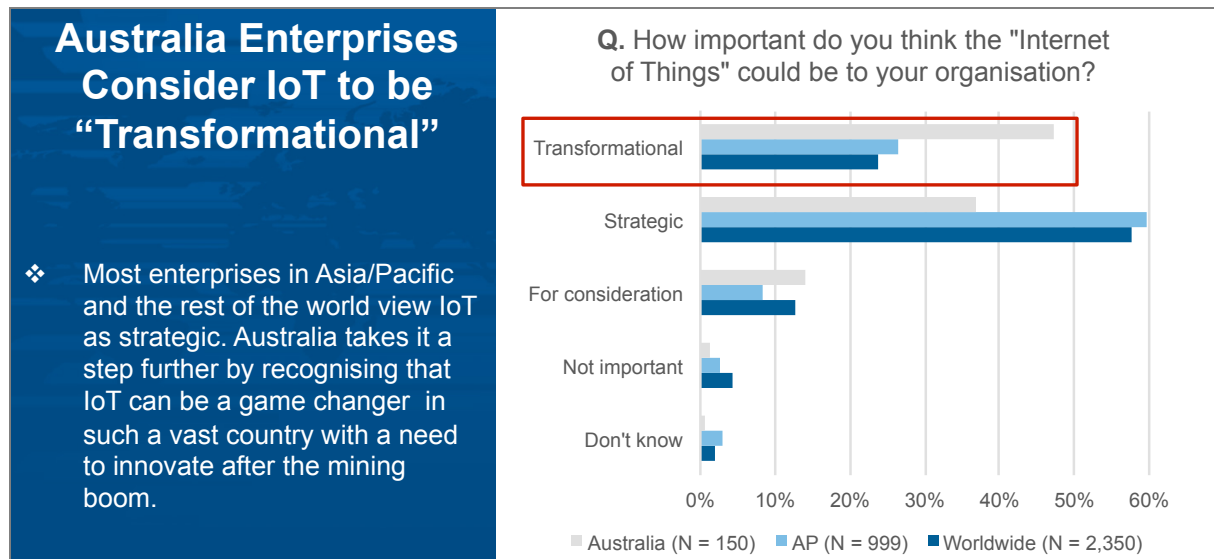
failure of supply to meet industry demand. Furthermore, the accelerating pace of digital innovation and consequent economic and societal transformation will require constant adaption and re-training of our workforce. We see our current education systems as ill-equipped to meet the task of providing “life-long” learning, nor are citizens prepared for a future of multiple careers during a lifetime.

- **How we maintain and enhance competitive digital connectivity** – we will need to rapidly understand and adopt new digital connectivity services and business models comprising new digital wireless technologies, including Low-Power Wide-Area Network (LPWAN), Satellite and 5G. These technologies will underpin exponential growth in IoT devices, data generation and sharing, as well as new service models for real-time control. Bridging the gap in digital connectivity outside of Australia's major cities is of essential importance. IoT presents the opportunity to unlock the economic potential of Australia's regional areas, where a large number of Australia's key industries are located.

## 2. What is your vision for an Australia that thrives in a digital economy? Where would you like to see Australia in five, 10 and 20 years' time?

Multiple studies by industry and research organisations estimate the potential global annual GDP opportunity of IoT at various figures up to US\$11 trillion. This translates into an opportunity for the Australian economy of an uplift of up to AUD\$120 billion by 2025<sup>1</sup>.

According to IDC, Australian enterprises also recognise the potential and view IoT as an important strategic investment with transformational opportunities.



Source: IDC, *Global IoT Decision Maker Survey*, August 2015

<sup>1</sup> Communications Alliance, *Enabling the Internet of Things for Australia*, October 2015

However, Australia has lagged in terms of competitiveness and innovation adoption:

- Australia ranked 22<sup>nd</sup> in the World Economic Forum's 2016-2017 'The Global Competitiveness Report', falling one place from the previous year. Australia was deemed to be trailing far behind its competitors in terms of business sophistication and innovation.
- In the 2016 'Performance Review of the Australian Innovation, Science and Research System' conducted by Innovation and Science Australia, Australia ranked last regarding the application of new ideas.

Our vision for Australia is one guided by a national narrative which embraces the opportunities unleashed by IoT and the digital economy, particularly in sectors where we can leverage natural advantage or need. Sectors where we see opportunities for leadership and growth from focused IoT adoption, both in Australia and in export markets include:

- Food and Agribusiness – food provenance, quality, supply chain, precision farming
- Transport – integrated supply chain, multi-modal customer services, urban design and informatics, driverless cars
- Water – fit for purpose water, customer behaviour management, precinct water management, asset optimisation
- Energy – demand managed supply, distributed energy models, energy/water/transport optimisation
- Smart Cities – climate adaption, congestion management, responsive urban design, enhancing liveability
- Manufacturing is a significant component of the above sectors, which will thrive if it can embrace IoT

Setting ambitions for leadership in the above sectors will help focus effort, education and investment. Fostering a culture that supports new market development with an eye to drive export from these successes is critical.

Australia will need to take leadership in critical areas of IoT enablement, such as:

- Data sharing models and interoperability standards – consistent across all levels of government, industry, research and society
- IoT security – our ambition is for Australia to become branded as secure for IoT services in a similar way as we have been for safe food
- Collaborative experimentation – across technology, business model and regulation – including the involvement of research and start-ups.

### 3. What is the role of government in achieving that vision?

Government plays a fundamental set of roles in helping Australia leverage IoT to achieve a competitive edge, productivity improvements and improved services for communities, including:

- **Setting a Digital Economy narrative** – that is embraced nationally across government, industry and community. The narrative should convey the critical importance of the adoption of digital technologies (including Internet of Things, Industrial Internet of Things, and Industry 4.0) for Australia's competitive advantage, productivity improvements and jobs growth. The narrative should also outline how this can be achieved in collaboration with industry, research and communities. Consequently, a foundation would be established for raising awareness and bringing the community and industry along the journey.

Furthermore this narrative should encompass a global vision for sectoral leadership and jobs growth. The digital economy is a global phenomenon, will be disruptive and will be built from innovation prowess. Success in this context mandates ambition and big thinking. Otherwise it will be easy for Australia's international competitors to roll over the top of even our most established sectors. This will limit opportunities for value creating innovation in Australia which will limit success of Australia's digital economy.

- **Government as a collaboration partner and experimenter** – the government is an important partner in the operation and delivery of services for the economy. Therefore, we see the government as a key contributor in the co-design of the new digital economy. This includes experimenting and participating as a user, not just a provider of services.
- **Government as purchaser and user of digital services** – the government can (and should) act as a major catalyst for digital innovation, for example by promoting:
  - Data sharing capabilities in infrastructure projects
  - IoT security certification for IoT sensors and services
  - Participation in test-beds and pilots of Australian SMEs, start-ups and research organisations (universities, CSIRO, CRCs etc)
  - Businesses to commercialise IoT and automation products and services
- **Driving digital (IoT) skills education and development** – in a digital economy where most people will have multiple careers and jobs, continuous skills development will be required from school through to retirement. This in many ways reflects the accelerating pace of change of new technologies and consequent business disruption and re-invention. Within the framework of a national digital economy narrative, the government has a critical role to play in working with state governments and industry to reshape our education system to be fit-for-purpose in order to prepare and continually re-educate our workforce.
- **Recognising the opportunity to make markets in the digital economy rather than evolving markets** - The nature of the digital economy is to disrupt markets and create new markets, limited only by imagination and openness. There is a need at a national level to cultivate market making. This is not a norm for Australia which means it requires some advocacy. It is new markets that will be the basis for investment and will provide the opportunity to sell into with higher value services (e.g. mass market critical infrastructure



based services such as required for autonomous vehicles or health related robotic remote surgery). Success in domestic new markets can become the basis for proving innovation for export.

- **Nimble regulator and standards setter** – the digital economy presents many opportunities for service innovation and productivity gains – but only if industry is flexible and nimble to the opportunities and **if old regulation is not used as a barrier to entry**. The government has a key role in being alert to and dismantling where necessary incumbent regulation that impedes important innovation. To enable economies of scale and encourage competition, clear standards can act as accelerators of innovation. Standards Australia has a key role to play here.
- **Supporting and encouraging Industry IoT R&D investment** – the recent ACS 'Digital Pulse' authored by Deloitte Access Economics pointed to Australia's poor international comparison regarding Business ICT R&D expenditure. This investment is critical to support early experimentation.

#### **4. What key disruptive technologies or business models do you see? What do you predict is on the horizon in five, 10, 20 years' time?**

IoT demands a systems view of product, services and experiences and employs a diverse range of disruptive technologies. Most of the underlying technologies are rapidly evolving, including the collection of data through sensors, connectivity of sensors via a growing range of wireless technologies, cloud computing and data management, analytics, machine learning, artificial intelligence, automation, robotics and security.

Various technology elements of IoT will have differing maturity and capability over the coming years, for example:

- Lower cost sensors are already impacting asset management, environmental management and more. It is still relatively early days in terms of broad deployment, with mass market availability for certain types likely to be a few years off yet (as component wireless technologies mature)
- LPWAN – LoRa and Sigfox from now, NB-IoT from 2018/19, 5G from 2020
- Data management and curation tools – these are rapidly coming on the market and are a necessary pre-requisite for effective data sharing and for underpinning analytics and AI.
- Artificial intelligence and machine learning – there are and development of algorithms and learning applications. Australia has some depth in this area, especially in the finance domain
- Augmented reality from now, virtual reality from 2020
- Blockchain – currently at a nascent stage, however there is significant opportunity for Australia to apply Blockchain in some key sectors to prove provenance and shore up value, for example in Food and Agribusiness
- Security technologies and practices – the application of good practices and understanding for security requirements across the IoT products and services value chain is relatively immature. This is likely to remain a long-term challenge and an opportunity for Australia to take a leadership position.

## **5. What communication services, and underlying data, platforms and protocols, does Australia need to maximise the opportunities of the digital economy?**

With regard to communication services:

- According to the World Economic Forum, in the 2016-2017 'The Global Competitiveness Report', Australia is falling behind in several key areas. High performance broadband, a key plank of the digital economy, is one such area. In the decades to come, optical fibre and wireless technologies will offer the combination of communications services required.
- The IoTAA strongly supports the use of both licenced (3G, 4G, 5G and beyond) and unlicensed (ISM band and WiFi) spectrum for wireless solutions. All of these solutions will be needed to provide the degree of connectivity foreseen as critical in the digital economy. We support the use of LoRaWAN and Sigfox technologies and recognise that these offer valuable choices to the market which is already strongly developing around early deployments. 5G is further into the future and, as it matures, will offer significant opportunities to the market.

After communications, the next critical capability in the digital economy is the ability to appropriately share information in a consistent way. We must learn how to classify and handle sensitive information about individuals, about critical infrastructure and about security. Data sharing, described in our response to Q6 below, is a priority consideration.

Enabling integration across industry verticals to enhance services and customer experiences holds out significant opportunities for the Australian economy, for example:

- Integration for remote mining
- Precision farming techniques with remote sensing

In addition, through adoption of good security practices, we see an opportunity for Australia to build a reputation for secure digital services.

## **6. What opportunities do we have to accelerate the development of technologies that will underpin Australia's digital economy?**

We have a number of opportunities to accelerate the development of technologies that underpin Australia's digital economy. The acceleration requires a nationwide focus within a framework that includes all parties – government, industry, research and community. To achieve this we require:

- 1. A shared narrative to lead and guide nation-wide engagement in the challenge and opportunity of the digital economy.**
  - 2. Ensuring the Australian workforce is skilled to meet not only the demands and jobs of the digital economy, but also to drive leadership in industries where Australia can leverage its natural advantages.**
- IoT is fundamentally about the operations of systems, and it is this systems understanding which needs to be embedded in IoT/STEM education. While individual disciplines and technical components continue to be taught in isolation of each other, the importance of this horizontal view is ignored, along with the collaboration and mix of skills required to unlock the potential of IoT.

**3. Accelerating the understanding and adoption of key digital principles/practices, including:**

- Managed widespread data sharing: As digital technologies are increasingly used across the economy, more and more information is captured and stored in digital form. We need a commonly understood data sharing policy to enable managed secure sharing. The NSW Government, in collaboration with the IoTAA, the ACS and other partners, is leading by example in its development of a Data Sharing Framework that offers an approach to guide the creation of a Government Data Sharing Policy. There is growing support and alignment across most states and territories that the Framework should become a consistent reference point for Australia. Some of the benefits of a structured and consistent approach to open data/data sharing include:
  - Protecting citizen privacy
  - Increasing government transparency
  - Enabling innovation and jobs creation in the rapidly growing data analytics sector
  - Fostering an ecosystem for data-informed problem solving
  - Helping protect critical infrastructure
  - Improving environmental management
  - Enhancing the efficiency of services, e.g. waste management, transport, utilities, health
  - Improving the sharing of data between and across the three levels of government. Without a common framework, data sharing becomes more costly and less efficient, inhibiting value creation.

Security in digital services: The technology industry is facing a crisis in confidence particularly around privacy of information in the face of frequent data breaches in the largest and traditionally most trusted organisations. This undermines the public's trust and confidence in the ability for business and government to secure information. Concerted and consistent messaging around cyber security to business and the public is crucial. The Australian Government's 'Stay Smart Online Small Business Guide' and 'Stay Smart Online My Guide' are important starting points. There is an opportunity for Australia to lead in the development and application of good security practices to achieve a market edge.

Ready spectrum availability (e.g. for 5G) and wide connectivity coverage: ACMA is collaborating to make the best use of both licensed and unlicensed spectrum to maximise low cost sensing options for Australian industry/commerce. As we connect more and more sensors (predicted to be billions in the coming years) we will need to look to new ways of maximising the utility of scarce radio spectrum resources, both licensed and unlicensed. The evolution to 5G is a critical digital economy enabler, as is fixed broadband infrastructure.

Early collaborative experimentation of new business models and regulation: this is important to enable a more agile and less risk averse approach to investment in digital innovation, for example through more focussed R&D concessions.

## **7. What opportunities do we have in standards development and regulation to:**

- **enable digital entrepreneurship, innovation and trade?**
- **mitigate the risks associated with digital disruption?**

The IoTAA is an important contributor to the standardisation work undertaken by Standards Australia. Australia needs to be cognisant of emerging regional and sectoral practices and standards and 'learn by doing', which in some cases might involve playing a leadership role, e.g. ag-tech data standards, smart city guidelines and roadmap, security testing and certification.

The UK has pioneered the creation of data sharing tools in the Smart Cities context. This work resulted in the BSI standardising 'Hypercat' as a software tool to interrogate and discover the content of Smart City data and, in turn, support data sharing. We can both leverage this work and learn from the approach taken by the British Government. The IoTAA was able to bring this technology to the attention of Standards Australia.

The IoTAA has and continues to develop guidelines and templates to support the adoption of IoT. We are leading the way in guidelines for IoT Cyber Security and data sharing best practice and we are currently developing a model for characterising IoT platforms and tools to enable business and government to choose IoT platforms and be better informed about interoperability at both the networking and data sharing layers of the digital economy. This work is all welcome input to Standards Australia who see the need to collaborate with the IoTAA in order to establish the most valuable guidance.

## **8. What digital standards do we need to enable Australian businesses to participate in global supply chains and maximise the opportunities of the digital economy?**

There is an array of standards for connecting sensors to networks, many of which rely on wireless connectivity. The ACMA, in collaboration with the IoTAA, has been working to make available sufficient radio spectrum to support a number of these standards. Through further allocation of appropriate new spectrum class licences, as well as licenced spectrum for 3/4/5G networks and other RLANs, we are reasonably well positioned for the digital economy. In both cases, it is critical that local spectrum management reflect a worldwide ecosystem approach to better find economies of scale for devices and sensors for the comparatively small Australian market.

We are less mature regarding the standardisation of data sharing. The IoTAA and ACS are progressing work to enable effective data sharing. The IoTAA is a significant contributor to the NSW Government's initiatives in this area through the work of the NSW Chief Data Scientist. This work should continue and be more widely embraced to ensure that all layers of government can efficiently share data without risk. The alternative is a fragmented array of state/council-based data sharing policies, leading to significant inefficiencies detrimental to the development of the digital economy. Effective data sharing would not only drive domestic efficiencies but could also lead to the export of data sharing expertise.

The application and development of standards across cities is a major area of opportunity for local and export domains.

It is important to note that, in the fast changing IoT environment, final standards in some areas will be some time coming. In this environment “roadmaps to standards” good practice guides and other mechanisms will need to be applied to give confidence, enable and encourage industry and government experimentation and early deployment, in order to achieve and maintain market leadership – of course, with a sharp eye on and participation within global standardisation activities.

## **9. What opportunities do we have to build trust and community confidence through resilience to cyber threats, online safety and privacy?**

Key security principles for a digital economy and IoT ecosystem are:

- The integrity of device functionality should be protected to ensure the security of personal identifiable data
- System security ensuring that data is protected, both in transit and at rest
- System access should be appropriate to the sector; unauthorised persons must not be able to gain access to a protected resource.

The application and level of privacy protection will vary for different categories. For example, protection of patient data is paramount in healthcare, the automotive sector requires strict protection of driver identification, customer identity in the retail sector must be removed before data is made available for data analysis, and personal data collected from Smart Home technologies must be anonymised prior to data storage and analysis.

It is recommended that IoT deployments are based on a sector-appropriate open business model, a service-oriented IT architecture, and a user-centric trust model. Privacy and security protection must be built into the system configuration to enable secure data sharing.

The evolution of IoT requires an agile approach to security and privacy. While there is an extensive set of pre-IoT data privacy principles and standards (e.g. Australian Privacy Principles), a common understanding of good practice for internet and IoT security is lacking.

With its recent release of the *Good Data Practice Guide* (8<sup>th</sup> November, 2017) and *IoT Security Guideline* (May 2016, updated November 2017) IoTAA is creating common building blocks and building community trust regarding IoT security. These documents were developed in partnership with industry, government and consumer groups. There is still work to be done in terms of dissemination.

### **IoT Security – IoTAA 8-point strategy**

IoTAA security workstream 5 is developing an 8 point IoT security strategy for the nation. It includes the development of an industry IoT security certification process. The intent is to provide market signals for certified IoT devices to better protect consumers and drive improved vendor and service provider practices. Certification programs for IoT devices can provide confidence to consumers and businesses deploying IoT networks. Certification programs must be based on agreed standards and need to constantly evolve to maintain currency.

## **10. What roles should government, business and individuals play in protecting the community in a digital economy?**

Government, business and individuals all have a crucial role to play in protecting the community in a digital economy. Some of the relevant areas have been outlined in responses to questions 9, 11 and 12.

It is vital that all three work together on:

- Identifying and codifying good practice and standards
- Improving community awareness and education
- Understanding community concerns and accommodating them in the digital economy transition
- Testing and demonstrating new digital services to learn and uncover community issues

## **11. What integrity and privacy measures do we need to ensure consumers can protect their data?**

Existing information privacy laws ensure that APP entities must:

- implement privacy by design and information security by design into their products and services;
- make reasonable and transparent disclosures as to collection, uses and disclosures of personal information about individuals; and
- provide individuals with reasonable access to that personal information.

The PM&C Data Taskforce is currently reviewing the degree to which personal information should be accessible. In particular, the issue of whether individuals (and possibly small businesses) should have a 'consumer right' to have basic electronic information about their transactions made available to them or other agents in a form which would facilitate comparison with services available from alternative providers. The IoTAA awaits the Government's announcements in this regard. We note that more ready access to certain transaction information may reduce information asymmetries and thereby promote consumer choice.

We also note that release of data to entities purporting to act as agents for consumers in undertaking price comparisons or in offering alternative services needs to be appropriately controlled. This may be through certification requirements to ensure consumers are provided with a ready means to understand and evaluate the trustworthiness of an entity receiving information. Industry-based, regulator overseen, trust mark certification schemes as to appropriate access and security controls for sharing of consumers' transaction information would be an appropriate way to protect consumers. Such certification schemes could include certification of 'infomediaries' as trusted third parties to handle sensitive consumer information and undertake comparisons and analyses on behalf of consumers. Introduction of such schemes might be supported by education efforts by the regulator to promote the importance of ensuring that entities purporting to assist consumers through access to consumers' transaction information are appropriately independent and trustworthy.

Any consumer right should promote data availability, but not through overly intrusive regulation. We suggest that a scheme should also not require data retention for any particular mandated period, or in any particular mandated form. A provider should not be

liable in relation to information disclosed by mandate, so long as the provider takes reasonable steps to ensure data integrity and to inform prospective disclosees as to possible limitations and qualifications for data reliability and integrity.

We also consider that it is important that Australian-based providers of products and services are not materially disadvantaged as compared to offshore providers by virtue of being subject to obligations to disclose and provide transaction information in circumstances where offshore providers are not subject to similar obligations. This is particularly important given that some of the largest repositories of transaction information about Australian consumers are controlled by offshore providers.

Further, we note that consumer rights of access to transaction information should not enable alternative service providers to free-ride upon transaction information as transformed and analysed by an existing service provider, particularly where the transformation and analysis involve significant business expense by the existing service provider. Existing privacy laws appropriately protect subsequent uses and disclosures of any such identifying information. A consumer right should be in regard to appropriately basic and restricted transactional data, not value added data transformations.

The IoTAA promotes consumer and industry awareness about good business practice in provision of IoT services and IoT devices to consumers. By building that awareness, we aim to assist both businesses and consumers to anticipate and address possible concerns before they occur. Our Security Guide promotes good information security practices in design and specification of IoT devices and IoT services.

We are working on guidance around interoperability of IoT devices and IoT services to further promote awareness as to choices available to consumers and to assist consumers to understand the benefits of interoperable products and services.

Our recently published *Good Data Practice Guide for B2C IoT Services In Australia* focusses on measures that IoT providers can take to build trust and understanding of consumers regarding collection and use of data in the course of providing IoT services. This Guide is drafted principally to assist providers of IoT B2C devices and services to design fair and appropriate features and settings for privacy, security and accessibility into their products and services and to make available appropriate and readily understood guidance for consumers about their use. This Guide is also intended to assist the IoTAA and consumer organisations in developing general guidance for consumers about privacy protection, secure implementation and use of IoT devices and services. The *Good Data Practice Guide* seeks to achieve these objectives by:

- building trust and promoting mutual understanding between providers and consumers about the collection, handling, disclosure and security of personal information and other consumer data
- facilitating a common understanding of good business practices for B2C IoT services and devices, including through stating principles for fair information handling and 'plain English' language for consumer terms and notices, consumer disclosures and consents
- promoting simplicity and clarity in terms of use, enabling consumers to better compare terms for provision of particular IoT services and devices
- assisting service providers to ensure that consumers understand expectations that providers place upon them when consumers set up and use IoT services and devices, including by following good information security practices, by addressing implementation

risks and by promoting disclosures by customers who implement an IoT service or device to other individuals who may be affected

- stating good practice principles for handling data flows. Many IoT services involve three or more entities delivering to an end user, with relevant data flows required between those entities. The data flows between entities are sometimes referred to as 'data ecosystems'. These good practice principles seek to facilitate a better understanding between participants in those data ecosystems as to the rights and expectations of consumers, participants and affected individuals.
- stating good practice principles regarding disclosure to consumers on the potential provision of information derived from IoT services to law enforcement agencies, environmental and other relevant regulators, insurers, loss adjusters or other third parties, so that IoT users (consumers and affected individuals) are aware of relevant obligations of IoT service providers.

## **12. What are barriers for business, particularly small business, in adopting cyber security and privacy practices?**

There are a number of barriers for business, particularly small business, inhibiting the adoption of effective cyber security and privacy practices. These include:

**1. Basic denial** – Many businesses simply believe that “it won't happen to me” or “we are not big enough to be a target” or “we don't have any information that is worth attacking”. However, with the rise of distributed cyber-crime, the effects of attacks such as crypto-lockers/ransomware mean that criminals can monetise even the smallest business simply by having a user within that organisation's network click on a malicious attachment to an email. And such criminals are not necessarily seeking access to information, but are seeking to disrupt the availability of information as a means to coerce the organisation into paying the “ransom” to regain access (if they don't have an effective backup/recovery strategy in place to mitigate the attack).

**2. Resources** – Many businesses focus their time and financial resources on products and services. Consequently, such businesses require cheap, easy to implement cyber security strategies. However, many businesses remain under-prepared to recover from cyber-attacks due to a lack of forward planning.

**3. Priority** – Some businesses do not see securing their digital environments and assets as a high priority, and look to bolt on security provisions as an afterthought, instead of embedding security considerations within their infrastructure. This is a false economy as cyber incidents damage reputations and incur significant costs.

**4. Education/Awareness** – Often a lack of understanding inhibits the adoption of cyber security and privacy practices. Education is essential to build understanding, confidence and trust.

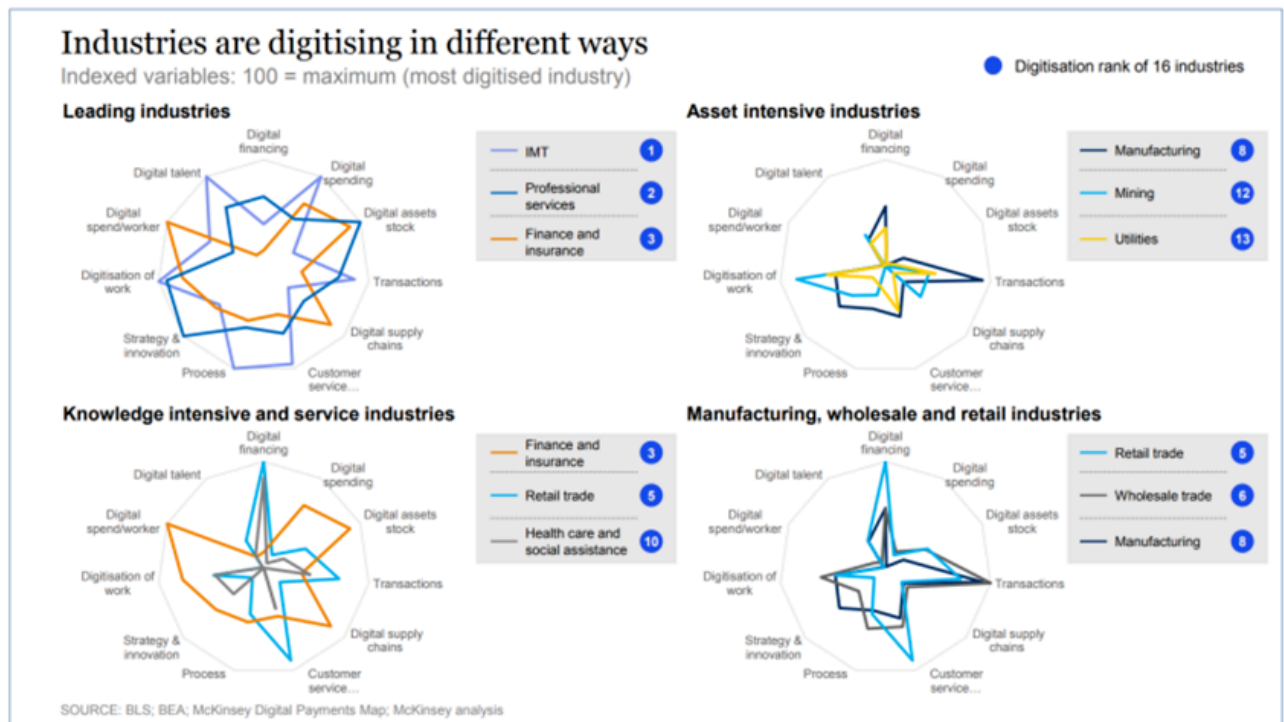


### 13. What integrity measures do the Australian Government and the private sector need to take to ensure business–consumer transactions are secure?

IoTAA's *Good Data Practice Guide* and *Security Guideline* go a long way in identifying integrity measures that need to be applied. See [www.iot.org.au/resources](http://www.iot.org.au/resources)

### 14. What is holding Australian businesses back in terms of benefiting from digital technologies?

The adoption of and value capture from digital technologies by Australian businesses has been uneven. While Australia's knowledge-intensive industries (International Mobile Telecommunications, Financial, Professional, Administrative sectors) display a relatively high degree of digital maturity, Australia's service industries (retail, arts, health, education etc) and asset intensive industries (manufacturing, mining, agriculture etc) are at a less digitally developed stage. There is also variance in the shape of digitisation within industries, as displayed in the figure below.



Source: McKinsey, *Digital Australia: Seizing the opportunity from the Fourth Industrial Revolution*, May 2017

A lack of digital literacy and skills is cited as a key barrier for Australian businesses across all industries. This shortage is resulting in the import of talent from abroad or in decisions to curb further digital adoption due to a lack of capability. In addition, data security and privacy concerns inhibit Australian businesses from reaping the benefits of digital technology.

Many businesses lack integrated digital strategies and are frequently distracted by 'innovation theatre', perceiving technology adoption as an end in itself, rather than as an enabler for achieving a specific customer or commercial outcome.

**How we work together** – Major gains in efficiency and business innovation are realised by marrying IoT technologies and practices with domain understanding to address industry and societal challenges. This requires far greater collaboration across technology and service providers, supply chain nodes, customers, industries, research, community and government. IoTAA is developing and connecting the Australian IoT ecosystem to accelerate the process. This collaboration is also important for developing a shared narrative to lead and guide nation-wide engagement in the challenge and opportunity of the digital/IoT economy and its economic and social benefits. This ‘market making’ will deliver both domestically and for export. This should highlight goals that we all share, in areas such as export, leadership in key sectors and citizen engagement.

## **15. What would help Australian businesses to embrace digital technologies?**

Building a collaborative digital ecosystem spanning Australia's regions and sectors is essential to enable Australian businesses to embrace the digital revolution. ‘Clustering’ facilitates the generation of new ideas and the sharing of resources to achieve goals which are out of reach for entities operating in silos. An ecosystem is particularly important to support Australia's start-up community in the testing and scaling of innovations.

Addressing Australia's digital divide is necessary to enable businesses to embrace digital technologies. The Australian ‘Digital Inclusion Index’ highlights a clear divide between capital cities and regional areas, as well as across socio-economic levels regarding digital access, affordability and ability. Narrowing this divide is necessary to both increase the digital capability of businesses across Australia in order that they can unleash the benefits of digital technology, and to increase the digital literacy of potential revenue-generating customers. The Government has an important role to play, for example through investment in nation-wide ubiquitous connectivity infrastructure (the continued roll-out of the NBN, free public Wi-Fi etc.) digital skills training, and R&D expenditure in sectors of the economy which are not usually targeted (e.g. the mining sector scored 10 times lower than the financial services sector in terms of R&D investment in the Digital Inclusion Index).

The development of common standards and guidelines, led by Government, would assist Australian businesses in cutting through the complexity of data security and consumer privacy issues. Businesses could use such guidelines and standards to build robust cyber security strategies which would enable them to embrace additional technologies and unlock new opportunities. The potential value of data sharing and data marketplaces through open APIs, within and across sectors, is to date relatively unexplored terrain in Australia due to the fear around opening up data silos, but the anticipated economic dividend is substantial.

## **16. What efforts are you or your organisation making to respond to digital transformation? Why?**

The vision of IoTAA is: “To empower industry and society by accelerating IoT innovation and adoption for Australian economic and societal benefit.”

We see ourselves as a prime instigator of IoT collaboration and advancement in Australia through a network which includes community and citizens, government, research and industry – all of whom contribute to our work.

IoTAA now has over 380 organisation members and 700 participants and is growing at 5% per month. IoTAA runs seven programs (workstreams) covering:

- Collaboration
- Smart industries and cities
- Data use, access and privacy
- Spectrum availability and licensing
- Cyber security and network resilience
- IoT start-up innovation and
- Platforms and Interoperability

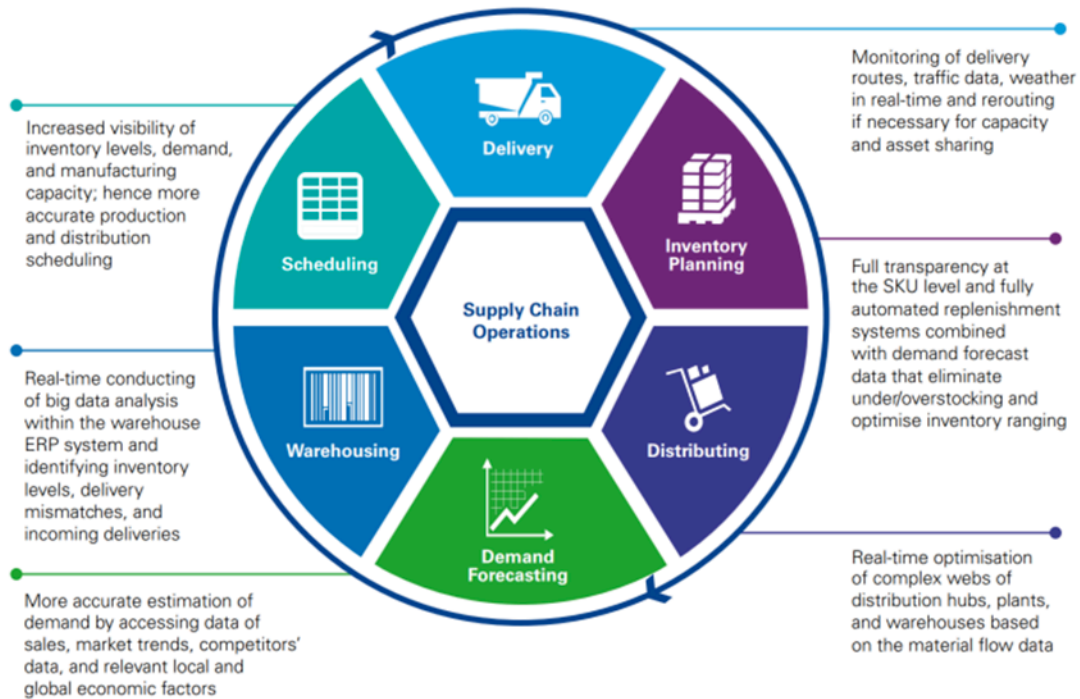
The IoTAA is fostering a nation-wide ecosystem to position Australia as a leader within the digital and IoT landscape. The IoTAA is currently conducting a national survey to benchmark the adoption of IoT across industry, government and academic in order to identify key opportunities and challenges for IoT innovation in Australia.

For more details, please visit our website [www.iot.org.au](http://www.iot.org.au)

## **17. What opportunities do we have to use digital technologies to improve linkages into export markets and global supply chains?**

The Internet of Things presents significant opportunities for Australia to overcome the tyranny of distance and improve linkages into export markets and global supply chains. As more things become connected, there are an increasing number of data channels available to be harnessed by organisations to increase visibility across the supply chain, enabling the orchestration of more responsive supply chains. The triangulation of a range of dynamic data inputs provides the capability to predict and proactively plan supply chain activities, e.g. estimation of demand, timeframes for delivery etc.

**Applications of big data analytics in supply chain operations**



Source: KPMG, *Supply Chain Big Data Series, Part 1: How big data is shaping the supply chains of tomorrow*, 2017

Machine learning is another form of disruption in supply chains facilitating the shift from reactive to proactive supply chain management. Machines are being programmed to learn from algorithms which reveal patterns in optimising upstream and downstream supply chain operations. These learnings can then be used to predict important events, e.g. when restocking is required or when the temperature of trucks carrying food products needs to be altered, serving to significantly reduce wasted resources.

Enhancing the reliability, security and transparency of the large volumes of data generated in supply chains, blockchain is disrupting supply chain management. Highly scalable, blockchain enables any number of entities to be integrated in a chain without damaging the integrity of the data. In addition, the data is shared by every entity along the chain, with certain predefined caveats to protect confidential information. Blockchain is serving to significantly lower transaction costs and improve efficiencies in supply chain management.

**18. What opportunities do small and medium-sized businesses have to embrace digital innovation to drive customer value, improve their services and unlock their potential?**

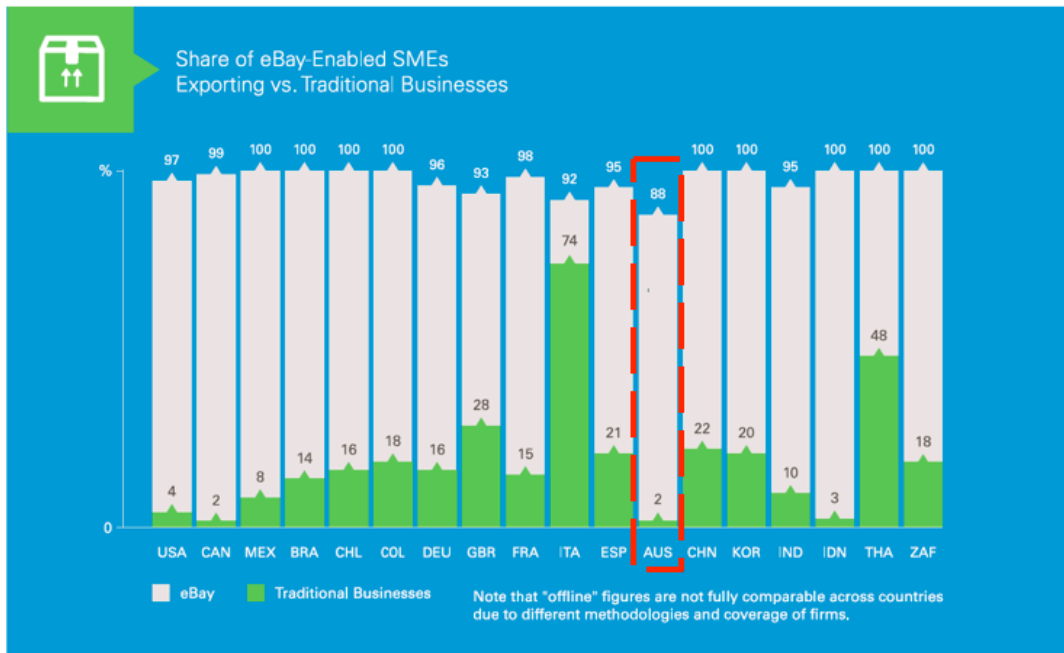
Australia's R&D tax incentives are key enablers for SMEs to embrace digital innovation. Providing certainty to the business community around the long-term nature of the incentive regime is important to encourage risk-taking and innovation.

A number of recent State Government initiatives, including the NSW Small Business Strategy and the Queensland Small Business Digital Grants scheme, offer significant growth opportunities for Australia's SMEs.

Australia's cities are also taking a leading role in supporting SMEs. For example, through the Digital Brisbane Strategy, Brisbane City is empowering SMEs to embrace digital technologies by building their technological literacy and capability through 'Power-Up Small Business Workshops', connecting them to resources such as venture capital and showcasing their achievements nationally and internationally.

A key challenge facing SMEs is finding the optimal opportunities available at the various levels of government and across other sectors in Australia. The national Digital Economy Strategy holds the potential to provide an overarching framework to better guide SMEs as they look to unlock their potential through digital innovation.

SMEs are also well-placed to tap into the new marketplaces of Australia's growing sharing economy. Sharing economy platforms lower transaction costs and enable SMEs to reach beyond immediate markets. In 2014, 88% of Australian eBay-enabled SMEs exported their products and services, in contrast with only 2% of traditional businesses, as evident in the figure below.



Source: eBay, *Small Online Business Growth Report: Towards an Inclusive Global Economy*, 2016

Building brand power and trust with customers are two key challenges that SMEs traditionally face. Digital platforms are supporting SMEs to overcome these challenges and compete with more established players by creating new avenues for trust and brand building, e.g. peer review systems. SMEs are also able to harness the data created through these avenues to tailor their strategies.

## **19. What are the key new growth industries that Australia should be tapping into? In what technologies and sectors should Australian businesses take the lead, and where should we be a 'fast follower' of international trends?**

Australia has the opportunity to capitalise on sectors where it has a natural advantage or proven track record through the application of IoT. The nature of the digital economy is to disrupt markets and create new markets. New markets will be the basis for investment and will provide the opportunity to sell higher value services. It is therefore essential that Australia looks to cultivate new market opportunities while focusing on its established industries.

Australia could take the lead in areas including:

- AgTech
- MiningTech
- TransportTech
- CityTech
- WaterTech
- EnergyTech

In addition, through adoption of good security practices, we see an opportunity for Australia to build a reputation and export market for secure digital services.

The digital economy is a global phenomenon requiring a global outlook from Australia's leadership. Learning from international examples of successful IoT deployments is important to accelerate benefit realisation. For example, Australia can learn from the UK cities of Bristol and Manchester which have developed innovation ecosystems, enabling cross-society collaboration and resulting in the development of new solutions to city problems.

## **20. What opportunities do we have to equip Australians with the skills they need for the digital economy, today's jobs, and jobs of the future?**

While some of today's jobs will disappear by virtue of the digital economy, there is significant opportunity for new job creation. Education to foster the necessary skills for new jobs is of critical importance. Australia requires an increased focus on systems and digital skills in conjunction with sectoral domain expertise and soft skills. This can be achieved through:

- Government programs for schools (STEM/STEAM)
- Increased skills based learning – post school and post grad through VET/universities
- Industry accredited courses, e.g. those being endorsed by Engineers Australia
- Managed job rotations

Increasingly, as governments shift to digital service provision, there is a need to ensure that services remain accessible to people with disabilities and those who experience other kinds of disadvantage. As such, it is necessary that government websites, apps and other digital platforms be developed using the Web Content Accessibility Guidelines (WCAG) 2.1 guidelines and are tested, prior to release, by those with disabilities.

Further support for Digital Accessibility training on a national basis is necessary as well as an increased focus regarding tailoring user testing of the government's own design processes.

## 21. What opportunities do we have to bridge the ‘digital divide’ and make the most of the benefits that digital technologies present for social inclusion?

Social inclusion starts with ubiquitous connectivity. Organisations, such as the Australian Digital Inclusion Alliance (ADIA), are helping to coordinate digital inclusion initiatives and are collaborating to develop digital solutions to reduce social exclusion. The ‘Be Connected’ program works to address the digital divide and skills gap with older Australians.

Current ABS statistics indicate that there is a considerable portion of people with disabilities in Australia without Internet access. The Digital Inclusion Index also found that a large portion of people with a disability felt disconnected from their community. There is huge potential for digital technologies to help address issues of access and participation for people with disabilities.

## 22. What opportunities do we have to ensure digital technology has a positive impact on the cultural practices and social relationships of Australians?

IoT enables greater citizen participation in the collection and sharing of data and presents significant opportunities to generate positive cultural and social impacts in Australia. There is an increasing number of digital technologies and incubators serving to foster a more cohesive, tolerant Australian society. Examples include:

**Ask Izzy:** Almost 80% of homeless people in Melbourne own a smartphone. Ask Izzy is an app that capitalises on the free public WiFi that has been rolled out across Melbourne’s CBD to provide access to a directory of services for homeless people including where to find food, legal advice, health services and accommodation.

**University of Wollongong SMART Infrastructure Facility and Briometrix:** The partnership is developing a crowd-sourced, real-time mapping system using IoT and advanced data analytics to provide wheelchair users with greater freedom of movement. Users will be able to track journeys, log key features of physical environments and access interactive maps.

**Remarkable:** Australia’s first accelerator providing funding, mentorship and master-classes to disability-focused start-ups.

**DHIVE:** Australia’s first indigenous-led digital inclusion and innovation incubator empowering entrepreneurs and start-ups from digitally disadvantaged and disconnected groups to grow opportunities, build business and improve their local communities.

**Eye-D:** an Android App which provides a ‘where am I?’ function i.e. an immediate street location to help people feeling lost. This program provides the ability to find specific stores and services in close proximity using a navigation tool supported via Google Maps. It also provides the ability to have a letter read aloud and identify pictures.

**Google Maps Disabled Access Guide:** For wheelchair users, Google Maps in the US has introduced a feature advising whether a particular place is wheelchair-accessible.

IoT holds the potential for Australia to enable cross-societal engagement and collaboration to work towards the achievement of common goals such as urban liveability, climate adaptation, social inclusion etc, as well as to unlock significant commercial opportunity and secure Australia’s global competitiveness.