FROST & SULLIVAN

The Digital Economy: Opening up the conversation

Frost & Sullivan's Response to RFC

Frost & Sullivan

www.frost.com

30 November 2017

CONTENTS

A. The Role for the Government and Private Sector

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

Digitalization has had significant impact on our market research and consultancy industry. Due to ease of access to information, the value placed on research data has reduced over the years. At the same time, other opportunities arose due to challenges faced by data users in interpreting and understanding the gamut of data available. Data analytics has become a mainstay of the industry in helping clients address the challenges they faced. There is also a rising demand for data specialists who are equipped with the necessary tools to analyze and interpret the data collated through different sources.

Internet of Things (IoT) is becoming a reality. Sensors and the adoption of smart devices across all applications and uses (including in Healthcare, Automotive and Retail) have made a difference in the lives of individuals. However, enhanced user experiences come at a price. In exchange for businesses to cater to individual needs/lifestyle, the barrier of privacy is eroded and businesses are in a position to collect increasing amount of personal information. Key challenge for Australia and other economies will be to provide a regulatory environment which is able to balance between providing access to information versus protection of individual privacy.

In view of the above, businesses need to have clear guidance (and regulations) which delineates appropriate collection of data, management of individual's data, and ensuring privacy of citizens. Enforcement will also need to shift from a reactive approach to a proactive approach. For purposes of this document, please use end notes in the "References" section, select "Insert footnote after highlighting the section to be footnoted.

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?

The backbone of a digital economy is innovation. Hence, the following quote from the Director-General of WIPO may apply here, "Innovation is the engine of economic growth in an increasingly knowledge-based global economy, but more investment is needed to help boost human creativity and economic output." In today's context, Australia is not ranked competitively in terms of innovation and digitalization. Australia's investment in R&D as percentage of GDP is lower as compared to other economies such as Germany, Singapore, USA and other OECD economies. In order for Australia to thrive in a digital economy and be at the forefront, more has to be done to drive investment and collaboration in innovation.

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

To achieve that vision, the government needs to play 2 key roles, one as a facilitator and the other as the regulator.

- Facilitator: As a facilitator, the government needs to look into developing initiatives that can nurture and develop the growth of digital knowledge communities made up of stakeholders from various groups. These stakeholders may include businesses, researchers, academics and relevant government representatives – this will form a network of partners for implementation. Citizens play a critical role in providing feedback to ensure that these ideas are aligned with social expectations and norms. Offering these communities a platform to share knowledge/viewpoints, as well as collaborate to develop new ideas will be one of its key aims. Where necessary, the government should also provide the necessary infrastructure where stakeholders may test-bed and nurture their ideas in a real-world context/environment suited to the needs of Australia. Lastly, the government plays a critical role of ensuring sufficient flow of funds which may support such initiatives.

- Regulator: As a regulator, the government will need to protect the rights and privacy of individuals. This includes ensuring that a balanced regulatory regime is in place which does not restrict innovation and at the same time, protect individuals and society.

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?

- Artificial Intelligence: AI is already a reality today. Combined with increasingly sophisticated computers or quantum computers, there are very few limits in terms of what computers can do in the next 20 years. Such technologies, together with IoT, Sensors and Robotics, will transform our behavior and affect the way we work and live. In an increasingly connected world, the virtual and physical space is bridged and humans will be in a position to hand off more control and responsibilities to AI to make decisions and act on our behalf. A key challenge lies in the amount of reliance which we should place in AI and the element of trust. Due to the inherent decision-making capabilities and nature of AI, there is a risk where AI may make decisions which are misaligned with our intentions and goals. These risks will need to be managed and mitigated accordingly.

- Robotics: Robots are essentially hardware which is highly reliant on the software (and AI) which governs the tasks they perform. Computers are not always reliable and they are prone to issues such as errors and 'wear and tear'. Problems arise when there is no guarantee on how these robots may endanger human lives when such issues occur. Reasonable safeguards need to be put in place to minimize or mitigate such risks.

- Sharing Economy: Business Models based on the concept of a sharing economy have significantly disrupted traditional businesses. Applications such as AirBnB, oBike and Uber are already bringing about benefits in the way we travel and live. At the same time, such business models have created a new set of problems which have negatively impacted society. A glaring problem is invasion of bicycles parked all over the city, a problem compounded by inconsiderate users of the system, causing obstruction to pavements and risk to pedestrians. As a result, there is an urgent need for governments, municipal councils, business owners and other

stakeholders to develop a framework which will allow such new Business Model businesses to operate with minimal risk and disruptions.

Business models based on the sharing economy concept is one of many examples of how new business models can disrupt existing ecosystems. In anticipation of future similar problems, the Australian government needs to take on a proactive multi-agency approach to provide the appropriate regulatory environment and guidelines for both businesses and users alike.

B. Digital Infrastructure

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

There are a few areas in networking where we see Australia can maximize the opportunity for the next generation Digital economy:

- Network virtualization: Australia took the lead with reference to the adoption of Software Defined Networking (SDN) and Network Function Virtualization (NFV). This can be now extended to Wide Area Networks (WAN). Software defined WAN may be an important aspect which Australia needs to closely evaluate when looking at maximizing the opportunities for the Digital Economy.

- Low Power WAN / Narrow Band-IoT: Australia has a good coverage of NBIoT network now with the nationwide roll out by Telstra. This can be leveraged by enterprises to design new IoT solutions for clients across APAC.

- Terrestrial/ Fixed Broadband: The National Broadband Network (NBN) rollout has proved to be a challenging roll-out. Dissatisfied customers with high costs but poor services. Speeds are reportedly worse than the previous ADSL speeds. These issues need to be resolved quickly in order to maximize accessibility of fast internet access nation-wide which will help sustain the adoption of digital solutions and support the growth and development of Australia as a Digital Economy.

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

There are few ways opportunities for Australian government to look at accelerating the growth of Digital economy

- Ensuring the standards and infrastructure are well defined: There is some ambiguity around standards for new digital technologies especially on areas like AI, Block-chain, etc. The Australian government can bring together the various stakeholders/regulators to ensure transparency in discussions and to ensure that common standards are adopted. This can be a big push for enterprises wary of investing in new technologies without knowing the specific standards which they should conform to.

- Talent pool development: Effective curriculum development from the early stages leading to good STEM (Science, Technology, Engineering and Mathematics) programmes will be key to ensuring that our future Talent pool will have the necessary skills and capabilities to thrive in a global Digital Economy. Hence, developing the right infrastructure and knowledge at an early stage so the youngsters can start innovating and participate in the new age economy.

C. Standards and Regulation

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?

We believe the following technologies will create maximum opportunities for Australia and there should be a special focus on developing these technologies and developing the Standards & Regulation in these areas:

- Artificial Intelligence (AI): Australia should accelerate its positioning as an AI hub. We believe NZ is ahead of the curve and have various forums supported by government and a government body that is propelling AI development in the country. Australia needs clear standards around fail-safe design of autonomous AI driven systems. Autonomous systems that malfunction can potentially harm human users, society, and the environment. Fail-safe measures are essential to lower risks related to systems breaking down, and to provide developers clear instructions to stop systems which may been compromised. Standards along these lines provide a basis for developers to design these fail-safe systems to improve accountability.
- SDX (SDWAN, SDN, SDDC) – Software defined Technologies. Australia was way ahead in the adoption of SDN and Virtualization. Software Defined WAN and Software Defined Data centre will be big themes going forward.

The biggest challenge for Software defined technologies adoption is the clarity around data access and data control. Clear standards around Data access, control will be essential for enterprises to adopt Software defined based technologies in a faster manner.

- Blockchain - Sydney & Melbourne are already seen as Pioneers in the APAC Fintech landscape. We expect Blockchain use cases to go beyond Australia and there maybe use cases for Australian enterprises in Real estate, Healthcare, Logistics etc.
- However, current use case for Blockchain is limited to Crypto-currencies primarily in Australia .Important for RBA (Reserve Bank of Australia) to work with other agencies to define the regulatory implications of using Blockchain.

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?

The Australian government established the Digital Transformation Agency (DTA, previously the Digital Transformation Office) in 2015 to work with agencies to establish

digital standards to deliver a better experience for Australians. To a certain extent, some of DTA's original design was based on design standards adapted directly from GDS in the UK. Moving forward, there is a need for a transformation and Australia needs to look at new forms of Digital standards used in other countries. For example,

- Estonia: Digital standard governing use of X-road, a secure data exchange layer used by banks, other businesses, and public services alike – has a level of security and reliability that is unmatched around the world.

- UK: GDS has also played a central role in establishing digital standards to assess the quality of online services for citizens. Standardization of these services across various government agencies enabled uniformity of e-citizen services.

D. Trust, Confidence and Security

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

Digital transformation plays a critical role for today's government, however, its mindset, goals and long term plans should focus on building 'digital trust' among its citizens. It is not only imperative to have traditional technology solutions such as firewalls and user and access management controls. There is an urgent need to have a resilient leadership, culture, networks and change readiness to fight against cyber criminals and other malicious factors.

Some of the opportunities that exist for the Australian government to adopt are as below:

- Need for stringent data protection laws: To increase the community trust and confidence in digital adoption, the government can consider developing a national policy framework that aims to provide a legal and policy foundation, basis which a resilient cyber eco system can be built. Some inferences can be drawn from the EU's adoption of the General Data Protection Regulation (GDPR) that has strict implications for businesses and individuals across Europe. This regulation is to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

  In current times, it is important to develop a comprehensive law enforcement capability. An increased level of cooperation is needed between the private sector and the law enforcement agencies to better anticipate and respond to attacks. There should be sufficient funding in law enforcement capabilities for prosecuting cybercrime. Other areas for consideration include collaboration in cross-border legislation and continuous efforts between companies, governments and law enforcement agencies to fight cybercrimes.

- Government driven cybersecurity investment: A government that has been successful at digital adoption and building trust among its citizens is Estonia. It has invested heavily in the country's cybersecurity infrastructure and put a state of the art framework for cyber protection. Here the citizens own their data and have the right to

control access to their data. In case of health records, they can be decisive on giving access rights to doctors and choose not to give to certain individuals. In cases, where they are required to give their data by law, they can see who accessed their data. The citizens also enjoy the right to get support in investigating suspicious users.

Another example is of the Danish government that has announced an investment of DKK 100 million for a new national strategy for cyber and information security. The strategy, which will be valid for 2018-2020, will be formulated and developed in a cross-ministerial working group with representatives from 13 ministries.

- Increased thrust on cyber resilience: Some governments are appointing 'Tech Ambassadors' to discuss issues around data security and customer privacy with leading tech companies such as Google, Apple and Facebook. Denmark is the latest country to appoint a 'Digital Minister' to discuss data related issues and to digitally engage their citizens in everyday life. Past examples of such roles have been seen in the UK, France and Poland. These initiatives by the governments to have a strong cyber infrastructure and resilience policies in place will help increase the public confidence and boost digital adoption.

- Focus on citizen convenience: The Australian government needs to maintain a balance between security requirements and citizen convenience. Citizens will support the digital adoption if they are given an assurance of increased security measures being adopted to protect their private data. For example, if additional login questions or use of advanced technologies such as biometrics are used, it can help in developing an increased level of citizen trust. Regular security checks by the government will add further to their trust level.

- Drive citizen education and awareness on cybersecurity: Training and information campaigns can be run to help citizens to be more aware of the basics of cyber security as they can then contribute to protect their own interests from the various threats. Education on cyber wellness can be implemented as early as primary school, which will set the strong foundation of good cyber practices for the long term.

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

- Role of the government: In a digital economy, the government agencies aim to improve their citizen's digital experience by using more advanced technologies such as Internet of Things (IoT) and Big Data. This can improve data management techniques and build customer confidence in the future. It also needs to develop and enforce stringent data protection laws that can enable trust in the community and widen digital adoption. It needs to move away from traditional legacy databases and invest in educating the customer, build customer friendly websites and applications to enable better customer experience. The Australian government should consider mitigating any risks and enable a trustworthy yet seamless digital experience.

- Role of the business: Today, businesses are adopting digital technology and IoT to transform their business operations and achieve digital operational excellence. This

has created several opportunities for those that are quick to adopt digital innovations. As a result, they are now moving away from traditional methods of conducting business and becoming more agile, and are able to provide real time information to the informed and demanding customers. This can be seen as an opportunity to incorporate "security-by-design" in these digital initiatives to prevent possible cyber-attacks.

Companies such as Facebook, Google and Microsoft are using techniques based on Artificial Intelligence (AI) to train computers to respond faster to customers by understanding human language. This is also enabling complex decision making for businesses based on customers' preferences and responses. Thus, with more and more corporates adopting digital technology, they will re-invent their businesses and this will enable the digital economy to reach its full potential. The use of AI should also be incorporated to their security technologies to detect and respond faster and accurately towards cyber-attacks.

- Role of the individuals: In a digital world, customers expect seamless and personalized experience in their digital interactions. Hence, businesses and the government should design digital solutions to enable a smooth customer experience. Customers should become more aware of the latest digital offerings by keeping themselves updated through social media and other channels. They should make use of the digital platforms to benefit from savings in costs and time spent in physical interactions. While, the use of digital applications has almost become the norm today, customers should also be aware of the cyber threats it poses. They should use these applications with utmost care and be aware of phishing emails and websites that do not seem authentic. In a study done by Frost & Sullivan on Australian enterprises, almost 33% of Australian organizations surveyed experience phishing email attacks every month.

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

- Handle data in compliance: The government needs to handle the personal data collected according to the data protection law. For instance, only the required data should be collected and it should be collected by fair means, with the individual's consent, be kept secure and be used for meaningful purposes. Consumers should be made aware of who is accessing their data. The government must ensure that the customer data is by no means sold, rented or exchanged to other parties without their prior consent.

- Maintain data security accountability: The Australian government should ensure that government IT employees and management understand their responsibilities. The various types of data collected should be classified so that employees understand the differences. Some data is critical and should remain confidential and within the company. While other types of data can be made public and shared externally.

- Draft policy around acceptable use: There should be clear definitions that talk about acceptable use of data. In addition, consumers should sign an Acceptable User Policy so that the government can take the necessary disciplinary action if needed.

- Ensure control over technological resources: It is very important that system logs are monitored, proper system and process audit checks are conducted to identify and mitigate potential risks. Technology resources such as photocopiers, printers, scanners, laptops and smartphones are cleaned before their disposal as they store copies of information that has been photocopied, printed or scanned. Identity theft could occur if the information is leaked.

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

Small businesses often face challenges related to capital funding and technological know-how and lag behind in cyber security adoption. Some of the key barriers faced by them include:

- Lack of management support: Cybersecurity does not remain a top priority for the management of small businesses as they scale and grow. With other more immediate demands from other business issues, Cyber-security takes a back seat. Most small businesses do not have a comprehensive IT policy that covers cybersecurity. There is no representation of dedicated technology specialist or involvement of the C-level executives on the management board in matters relating to cybersecurity.

- Limited budget for IT expenditure: Small businesses find it difficult to justify the investment needed for cybersecurity solutions, especially, when such funds can be used for other purposes. Unlike bigger enterprises, they do not have the required budgets to outsource their IT needs to a managed service provider. These businesses often overlook cyber insurance as they assume it to be for larger companies, as those businesses are the most frequent targets of hackers.

- No clear IT policies and IT resources in place: Employees are allowed to bring their personal devices to office and these small businesses do not have any control over these devices. These devices could often have malware or might otherwise allow an outside party to gain access to their network, and hence information could be leaked. Further, employees often conduct business transactions on smartphones and employees click on phishing emails or download from unknown sources that can lead to hacking and data breach. Employees may be unaware of these threats and it is important to keep them updated with the latest cybersecurity practices.

  Small businesses do not have qualified, dedicated cybersecurity professionals to help them in case of any sudden threats. Further, cybersecurity has become a major issue for them only in last few years.

- Evolving technologies pose a challenge: Another barrier to the adoption of cybersecurity is the continuous evolution of technologies. Small businesses are unsure of where to invest and which solutions will be best for the data protection of their firm.

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

The Australian government and the private sector can be effective in mitigating cyber related threats if they can come together to address the concerns of businesses, government stakeholders and consumers. Some of the key measures they can take are stated below:

- Disclosure guidelines: The government needs to ensure that the private sector should disclose all significant cybersecurity risks and incidents to the investors. Even though the companies would agree to comply, sometimes they may be reluctant to disclose information about a breach, as it could lead to damage in market value, reputation, or clients' trust. Loss of intellectual property is the most serious outcome of a security incident to organizations surveyed in Australia, followed by reputational loss.

- Annual audit checks: The government can conduct annual cybersecurity audits at various private companies to ensure that they are conducting their businesses in a cyber secure environment and are following all the protocols to avoid data thefts. For instance, the Kenyan ministry of information, communication and technology signed a memorandum of understanding with the Information Security Audits and Control Association (ISACA) with plans to conduct regular ICT audits. Other activities carried under this agreement will include training of law enforcement officers about information security and sharing threat intelligence with private sector companies.

- Incentives for cybersecurity adoption: A number of incentives can be introduced to the private sector for adopting stringent cyber security practices. For instance, federal grants, legal protection and cybersecurity insurance can be given to companies that invest additional money in cyber secure practices.

- Educating the customer: Both the government and the private sector can come together to educate the customers on following safe digital practices that can reduce the probability of data breaches. Gamification using cyber security topics can also help interest customers to learn and be guarded against possible attacks. The government can take initiative to introduce cyber security related courses at the university level and conduct R&D with the private sector to meet the future technological needs.

E. Building on Australia's areas of competitive strength

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

Australia lacks an innovation culture like the Silicon Valley and Israel. The challenge we see is that Australian enterprises have not approached the idea of how to make Australia an Innovation hub well. There are only less than 5 Fintech companies that have garnered global attention. Australia lacks an innovation culture and is behind the US,

Israel and even NZ in many ways. How do you create a global Center of Excellence (CoE) for Fintech, AI and Cyber-security? These are areas for Australia to think about.

STEM development - Australia has a STEM (Science Technology, Engineering and Mathematics) decay curve with a concern on the talent pool for existing and next generation technologies. One of the big challenges is training and development available for students to steer their careers towards Digital Technology.

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

The key challenges we see with reference to Australian adoption for Digital Transformation:

- Multiple standards and Adherence: The standards can be simplified and adherence can be made a streamlined process
- Aging Infrastructure
- Talent: Hiring the right talent is a lot more expensive in Australia

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

At Frost & Sullivan, we have been bracing for Digital Transformation in a big way and to look at how we can enhance our products/service offerings leveraging on the capabilities of technologies for competitiveness. Externally, we have been advising our clients on how they should go about this journey.

Some of the things we have been focused on with reference to our clients and internal operations include:

- Digital engagement platform – We have created a Digital platform where we engage with our clients for their Advisory services. This means all the Reports we publish are available in Digital format which can be used by clients in various ways
- Digital tools to enable Customer Digital Transformation – We have worked with various Public sector and private clients where we have developed tools for real time monitoring (crime statistics, citizen feedback , consumer sentiments, etc)
- Internal digital tools – We have been a big advocate of using digital to increase internal collaboration across our 40 offices worldwide

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

- Scaling of businesses faster: Globalization/ expansion of enterprises happening at a rapid pace. So it is necessary for Australian enterprises to take a global view with reference to Digital Technologies. Cloud based technologies will be key to scale faster in the global landscape. In addition, incentives for SMEs adopting Digital tools can be a big driver to push the adoption. For example, the Singapore government successfully launched the SME Go Digital program to incentivize the SMEs.
- Growing Managed Services: Demand for enterprise services increasing across the board. So Australian enterprises need to tap into this global demand .Managed Services is a big growth opportunity, so Australia needs to ensure that it is aligned in

the best possible manner globally to deliver. Use of Digital Technologies across multiple verticals (e.g. Banking, Logistics, and Retail) can be a big driver.

- Customer experience management: Many paths to future growth for Australian enterprises especially for SMEs but customer-centricity will be key and they need to ensure the customer experience is digital and experiential.

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?

Some of the areas we feel Australian SMES have an opportunity to embrace innovations to unlock value:

- Engagement platform: Enhancing customer experience for SMEs is still a big challenge. In the 2015 survey, Australian enterprises stand at a CEI score of 3.45 compared to regional average of 3.8. (Source: Frost & Sullivan CEI Index, 2015). A big factor was customer engagement or the lack of it. Hence, sustained engagements with customers using Digital Platforms will be a big way forward for Australian SMEs to increase their customer centricity.
- Innovation platform: Australian enterprises should be open to the idea of opening the innovation ecosystem to their partners and customers.

  This can potentially be achieved in 3 ways:
  - Co-innovation – opening up the innovation ecosystem to new companies in the ecosystem (existing clients, partners, etc)
  - Co-creation – defining next generation ideas and opening up those ideas for contributing to new ecosystem partners
  - Crowd-sharing – open to sharing the platform with larger ecosystem players (app developers, new customers, etc)

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?

Key growth industries where Australia should be tapping into

- Data Analytics: Analytics is a big opportunity both for internal operation management as well as to target new revenue streams for Australian enterprises
- SDX (SDWAN, SDN, and SDDC): Software defined Technologies. Australia was way ahead in the adoption of SDN and Virtualization. Software Defined WAN and Software Defined Data centre will be big themes
- AI: Artificial intelligence esp. AI driven autonomous systems will be a key growth industry
- Cyber security & Physical security development: Australia is considered ahead of the curve in both Cyber-security and Physical security (Biometric access, Physical surveillance) aspect. Australian enterprises should be aggressive in promoting these to other geographies/ regions making Australia the hub for Security related industries.

There are certain areas where the global standards/directions are still not clear. So Australian enterprises should follow a wait and watch approach but be able to follow and act fast once the opportunities are clearer:

- Blockchain: Sydney & Melbourne are already seen as Pioneers in the APAC Fintech landscape. Australian enterprises especially Fintech companies can play a big role in the global Blockchain landscape in developing new 'Use Cases' beyond conventional Financial services applications we see today. But the regulations around the use of Blockchain in industries like Healthcare may need to be amended to support such initiatives.
- IoT services: 5G will push the business case for Australian enterprises further in verticals like Automotive, Energy, etc. Australian enterprises should be looking at being part of new associations like 5GAA (5G Automotive Association) to see how they can tap into cross industry opportunities. Australian enterprises should be ready to tap onto this opportunity as the standards evolve.

F. Empowering all Australians through digital skills and inclusion

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?

Empowering Australians should be the mandate of the Australian government in ensuring that the country has the right set of digital skills to tackle today's challenges and fulfill future skills demand. As technology evolves at a rapid rate, the subsequent disruption and impact on businesses and the economy will follow a similar pace. It is necessary for various education institutions, vocational and skills training institutions to infuse technology concepts and digital aspects into existing curriculum. This would apply for all segments, starting from early childhood education and primary schools, to universities and vocational institutes for young adults. Subjects such as basic coding, robotics and foundation application of technologies can be simplified and integrated into the education and skills training system to suit the respective learning groups. This has been successfully achieved in other countries such as Finland and Sweden. Other economies such as Singapore and Hong Kong are in advanced stages of integrating digital curriculum into their education and skills training systems.

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?

Key segments of the population who may have challenges bridging the 'digital divide' in Australia would be senior citizens and citizens who have limited access to digital technology due to their existing living and work environment. In the case of senior citizens, focus may be on the provisioning of silver friendly devices (e.g. elderly friendly digital information booths, large font pin pads), enhanced accessibility options and intuitive digital user interfaces. These would require a **national guideline or standard** for product/service providers to adhere to, specifically focusing on the abilities and limitations of the silver generation and their lifestyle.

For citizens who have limited access or exposure to digital technology, there are opportunities for the Australian government to reach out to this segment through community efforts and collaboration with businesses. Community forums, education roadshows and skills training can be organized at state level to increase exposure and enhance the technology savvy-ness of attendees. This will ride on existing education and outreach efforts available today. Partnerships with businesses may be made by providing skills training to specific job roles within an organization and collaboratively funded by both private businesses as well as the government. As the scope of each job evolves and the use of digital tools increases, it is necessary to ensure that workers in these roles are properly trained in these tools to reduce aversion to technology and improve understanding of the benefits it brings. Similar to the 'SkillsFuture' training fund provided by the Singapore government, such a fund at the national or state level will bring tremendous benefits to help bridge the digital divide between different segments of the population.

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

Technology has become ingrained into our lives and the average day for an urban person revolves around technology. To a large extent, this is facilitated by the portability and connectivity of technology (e.g. mobile devices) and increased our reliance on such devices/technology to organize our personal and work engagements. We are also seeing growing instances of individuals who have become emotionally attached to the mobile screen, and in many cases, resulting in a lower preference for direct human interaction. Many of us have become a slave to technology, rather than a master. A critical role which governments and grassroots organizations need to play is to ensure that we do not lose the human touch/factor in communications and a deep-rooted understanding must be ingrained in our young that technology is only a tool. Such messaging can only come through education and promotion campaigns.

The use of digital technology may also be a strong positive enabler to promote existing cultures and practices. As the modern society embrace technology in all aspects, digital technology has the ability to capture the attention of a large group of audience. Interactive programmes/platforms will further enhance the attractiveness of the content/message being shared. For example, QR codes have become a prevalent form of initiating the conversation between individuals and the content shared. In future, other forms of communications can be enabled through AR/VR, AI, IOT and any other digital technology which can provide the type of interactivity that will capture and enhance citizens' appreciation and understanding of cultural norms and communications.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact us: Start the discussion