Title:	Responses for Australia Digital Economy Consultation Paper
Author:	Mark Micallef Vice President, Asia Pacific & Japan
Organization:	Cloudera

Data Sharing

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

To perform successfully in a digital economy, Australian enterprises and public-sector bodies must prioritise the roll-out of infrastructure that will support fast, scalable, and secure data management and analysis. As communication platforms continue to evolve and generate massive volumes of data, we can continually expect diverse data points available for capture, storage, and analysis. With large volumes of sensitive data being generated, infrastructure that supports authentication, authorization, data protection, and governance is also essential for enterprise environments. A modern data hub allows for the fast, fluid, and secure actioning of high-volume data sets, avoiding the siloes that occur with traditional data warehousing.

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

As the NBN continues to roll out across the country and telecommunications service providers upgrade their mobile data platforms, the ability to harness that increased data flow will provide greater opportunities to analyse and gain deep insights into online behaviours. Implementing big data analytics solutions that are capable of handling and analysing this increased data flow will open a host of new ways to look at data sets across the spectrum of possibilities – from national security to health, retail marketing, customer analysis, and much more.

Cybersecurity

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

Both public and private sector organisations value the trust of their citizens and customers respectively, so the ability to manage their data safely and securely is vital. That means having infrastructure and policies in place that demand the secure transaction of data – regardless of where it is being accessed from.

The general public needs to know that governments and private companies hold their data very tightly and do not look to leverage it for anything other than expanding the greater good

of customer service or to solve community-wide problems. People also need to know that cyber threats are taken seriously across all organisations. With the right technology in place and a demonstration that big data can be used for improved services, greater trust can be established across the board.

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

    Large entities such as government bodies and private enterprises must take a lead role in not just securing an individual's data, but also in educating their stakeholders about where that data comes from, how it is stored, and the value it brings. Via transparency and education, greater trust will be built and individuals will also be empowered to be data-driven in this digitised economy.

    It is necessary for government departments to prepare for a wide spectrum of possible scenarios – including data breaches. This needs to be acted out on a broad playing-field, covering as many potential breach-points and scenarios as possible.
    The same can be said for the private sector – enterprises must be responsible for any and all data that is collected by them.

    Individuals should also take it upon themselves to absorb available knowledge on data privacy issues and policies so that they can gain full control of their personal data. The entire community has a part to play, but also much to gain from the digital economy.

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

    A national policy needs to be backed up by in-house policies and data needs to be secured at every level of a department or enterprise. While data analysis was, until recently, the responsibility of the IT department, data plans now reside right across the enterprise and government spectrums, from accounts through to marketing, sales, and human resources. Consumers have the right to know that their data is secure if they choose to share it with an entity. They also have a right to choose whether an entity is collecting their data and for what purpose.

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

    While big data creates a vast array of opportunities for enterprises, including small businesses, it also produces issues in governing that data. Many small businesses currently lack teams with the right skillsets to fully leverage on big data and analytics, securely. Many are hesitant to explore big data initiatives because they believe that it requires major investments in security, hardware, and software.

Small businesses can start by taking baby steps towards leveraging and securing their big data. They can focus their efforts on a few business-critical sets of data to solve specific business challenges, giving administrators a few specific data sets to protect from cyber-threats, rather than a plethora of data right across the enterprise spectrum. Small businesses may also consider creating a small interdisciplinary team to experiment with extracting business value from data – which has the benefit of consolidating data operations into one focus group, making security easier to deploy and administer.

Furthermore, software, services, and infrastructure can now be delivered over the cloud, making them even more attainable and scalable, while increasing the security measures available to a small or mid-sized organisation. Cloud-delivered infrastructure can help SMEs take advantage of more sophisticated IT operations, which previously might not have been accessible to them due to high costs of operations and up-front investments.

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

Government and private organisations need to ensure confidentiality, integrity, and availability underpin all business-consumer interactions. A modern data hub can be used to form the basis of this trust, with data stored securely, with high availability, scalability and fluidity.

Beyond the technology, government-led open data initiatives will also allow for a more inclusive governance and greater transparency as well as continue the push for the digitalisation of enterprises.

#End#