Australian Productivity Commission

NetApp MSS Contract Extension

NetApp®

TABLE OF CONTENTS

Contact information

NetApp Details			
Address	Unit 8, Level 1, 2 Brindabella Circuit, Canberra Airport, ACT 2609		
Contact Name	**Title**	**Telephone**	**Email**
Michael Steer	District Manager, Public Sector		

1 Introduction

NetApp welcomes the opportunity to contribute to the Productivity Commission's inquiry into Data Availability and Use.

NetApp understands that the Productivity Commission inquiry will investigate ways to improve the availability and use of public and private sector data. The Commission is required to:

- look at the benefits and costs of making public and private datasets more available;
- examine options for collection, sharing and release of data;
- identify ways consumers can use and benefit from access to data, particularly data about themselves; and,
- consider how to preserve individual privacy and control over data use.

NetApp's submission will focus on two key issues that underpin the inquiry's deliberations; namely data privacy/data protection and data security.

This reflects the particular global expertise that NetApp has developed in these matters through the activities of the company's Data Governance group. This is led by NetApp's Global Data Governance and Privacy Counsel, and Chief Privacy Officer.

NetApp's comments are based on the company's experiences in Australia, as well as in many overseas jurisdictions.

NetApp trusts that the Productivity Commission finds the following comments of interest. The company would be pleased to assist further, including providing further information or meeting with the Productivity Commission to elaborate on its responses.

2 About NetApp

Established in the United States in 1993, NetApp Inc is a global corporation that has grown through innovation to become one of the largest storage and data management providers in the world. NetApp provides software, systems and services to help organisations manage their data.

NetApp Inc is now a Fortune 500 company with annual revenues in excess of USD$6B with 12,000 employees in more than 150 offices worldwide. In Australia, NetApp Australia Pty Ltd employs more than 160 people with annual revenues in excess of A$200M.

NetApp Australia is a major supplier to the Federal government, to State and Territory governments, to the corporate sector and to education and the research community.

NetApp's primary focus is on data because we believe it is every organisation's most valuable asset. It needs to be well managed and stored securely, but data now also has to be mobile so that organisations can access and realize the value of their data and enable innovation.

At NetApp we have established a data governance organisation, led by the Global Data Governance and Privacy Counsel, and Chief Privacy Officer to address the critical issues of data access, availability, use and associated privacy, protection and security issues. This team has dual roles: not only does it seek to implement data privacy and sovereignty compliance solutions for NetApp, but it also engages with Data Protection Authorities (DPA) and law enforcement agencies worldwide. In its global role, the NetApp team has:

- created global policies, procedures and processes related to data privacy, cyber security, data breach management, cloud computing, and Big Data;
- developed data privacy training;
- actively participated in industry associations such as CompTia, Electronic Frontier Foundation and Storage Networking Industry Association (SNIA); and,

- been a partner with global data privacy councils including the EU Data Commission Privacy Advisory Board, APEC Cross Border Privacy Rules (CBPRs) Advisory Committee, etc.

In Attachment A, NetApp has provided further details on Ms Sheila Fitzpatrick, NetApp's Global Data Governance and Privacy Counsel, and Chief Privacy Officer.

3 Overview

Private or Public, data is any organisation's most valuable asset. Data can also be the source of great vulnerability. A data breach can significantly injure an organisation's brand and reputation as much as any charge of corruption, mismanagement of budgets, an oil spill or automotive recall.

Every day there is a front-page headline about a data breach, examples include Target, NSA PRISM, Sony, and U.S. Office of Personnel Management, to name a few.

As the Productivity Commission undertakes an inquiry on behalf of the Australian Government into the benefits and costs of options for increasing the availability of and improving the use of public and private sector data by individuals and organisations, it must address the key aspects of data governance. Compliance with the critical facets of data governance includes a detailed understanding of the significant and important requirements related to data privacy, data sovereignty and security.

NetApp agrees that the effective use of data is increasingly integral to the efficient functioning of any economy. As stated in the Productivity Commission's Issues Paper, improved availability of reliable data, combined with the tools to use it, is creating new economic opportunities. Increasing availability of data can facilitate development of new products and services, enhance consumer and business outcomes, better inform decision-making and policy development, and facilitate greater efficiency and innovation in the economy.

Data protection laws have been in place for decades. However, many organisations still resist the reality that they must comply with these laws, which require systems and processes to administer their compliance regulations. The conventional belief that focusing only on technology and security will meet all of the data governance obligations is actually detrimental to building an effective data availability and use program.

In Australia, as in many countries, the protection of personal information is not merely a regulatory requirement but a sovereign and inalienable right of every citizen. When viewed through this lens, the Australian Government's compliance with global data protection laws is both common sense and a fundamental requirement to being successful in today's economy.

Mindset is the key to the success in dealing with an issue the magnitude of global privacy legislation. Compliance is not ancillary to an organisation's outcomes. It must be 'how' an organisation conducts its business in integrated and indivisible ways from its operations.

Implementing a successful and effective compliance program requires a delicate balance between protecting the privacy rights of individuals and taking full advantage of new technologies such as cloud computing, mobile apps, and social media. The solution must embrace and reflect an organisation's corporate values and demonstrate commitment to the needs of citizens, employees, customers, and partners.

The stakes are high when collecting, processing, storing, hosting, sharing or transferring personal data, and the penalties are severe if the laws are not followed. A comprehensive data privacy program is not cheap or easy to develop and implement. It is not "plug-and-play." There is no "one size fits all" solution. Yet, when properly built and maintained, a data privacy program can provide comfort to citizens, consumers and other stakeholders to demonstrate that their interests are at the core of an organisation's operations.

4 Productivity Commission's Questions and NetApp's comments.

4.1 Questions On High Value Private Sector Data

NetApp is not in a position to answer the questions in this section. NetApp has no specific knowledge of the data sets that the private sector holds, but we would suggest that these are many and varied, and that determining what exists, how it can be used, and what value can be derived should be key objectives for this initiative. Many private sector organisations undoubtedly hold data sets which they collect as part of their business activities, but they are unlikely to have considered how such data might be used by researchers. Many organisations are only now beginning to explore what value they can themselves extract from the data they hold.

4.2 Questions On Access to Private Sector Data

PC Question

Are there any legislative or other impediments that may unnecessarily restrict the availability and use of private sector data? Should these impediments be reduced or removed?

NetApp Comment

Many data sets will have been collected after the individual providing the data has agreed to a set of terms and conditions that states that their information will not be shared. Private sector organisations would, understandably, be reluctant to make available data so collected.

If the data is personal information about an individual, the legislation should not be relaxed. The individual owns their personal data and should have control over what can or cannot be released publicly.

PC Question

What are the reasonable concerns that businesses have about increasing the availability of their data?

NetApp Comment

Businesses are concerned about competition, loss of their competitive advantage and loss of control. They are also concerned about the potential for reputational damage if they are perceived to have made data available inappropriately.

Companies are not going to share proprietary information or information that will put them at a competitive disadvantage, cause financial loss or unnecessary risk and exposure.

They want to control the flow of the data and decide what data they will or will not share.

They need to know what 'is in it for them' and what benefits they will gain from sharing data.

Companies are interested in sharing and obtaining information that will foster private and public sector cooperation; build partnerships; attract new business to Australia; improve technology; enhance business intelligence; combat cyber attacks; and expand the pool of available resources.

An example of this in the technology industry is that all companies have agreed to share data to an Industry Association regarding the volume and timing of business sales with the aim of understanding the total size of the industry, where each company is positioned in terms of market share and to highlight movements in those results.

PC Question

Should the collection, sharing and release of private sector data be standardised in some way? How could this be done and what would be the benefits and costs? What would standards that are 'fit for purpose' look like?

NetApp Comment

To standardise data, it first has to be classified by both the type of data (confidential restricted, confidential limited use, personal/sensitive, government classified, or public), and by the three categories of Big Data (raw data, incremental or value-added data, or commercial data).

Once the data has been classified, data handling standards can be attributed to the types of data with value derived and risks defined. Data handling standards exist in different jurisdictions and can be referenced to establish a standardised approach.

PC Question

Would such voluntary arrangements raise competition issues? How might this change if private sector information sharing were mandated? Is authorisation (under the Competition and Consumer Act 2010 (Cth)) relevant?

NetApp Comment

Voluntary sharing of information could raise competition issues, but more importantly it could enhance partnerships.

Mandatory sharing of data could create adversity and resistance, as well as mistrust of the intentions of the government. It could detract from the overall goal of growing business opportunities and investment in Australia.

NetApp understands that the intent of the Competition and Consumer Act is to control restrictive trade practices and monopolies, to protect consumers from unfair commercial practices, to promote efficiency and competition in business, to reduce prices and to protect all Australians from unfair practices. Accordingly, if the government sought to use the Act to authorize data sharing, it would need to define the categories of data, especially Big Data*, and provide a cohesive set of guidelines and principles that encourage cooperation as opposed to detracting from it by over regulating.

**** Big Data -** is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.*[1]

PC Question

Who should have the ownership rights to data that is generated by individuals but collected by businesses? For which data does unclear ownership inhibit its availability and use?

NetApp Comment

Individuals should always remain the owner of their own personal data regardless of who collects it. Unless the personal data is required for a legitimate legal requirement, individuals remain the data owners.

Businesses are the data stewards and should be allowed to use the data if they are transparent about the collection, use and sharing and obtain the explicit consent of the individual. Businesses should have the right to use the data in aggregated, anonymized or statistical format without consent provided the data cannot be tied back to a specific individual.

---

[1] http://www.gartner.com/it-glossary/big-data/

4.3 Questions On Privacy Protection

PC Question

What types of data and data applications (public sector and private sector) pose the greatest concerns for privacy protection?

NetApp Comment

Two data classifications would pose the greatest threat in terms of data protection: Confidential Restricted Data and Personal Data.

Confidential Restricted Data is the "crown jewels" of an organization that if exposed to unauthorized access could result in substantial harm to the organization. Personal Data is any piece of information that is identifiable to a person or can identify a person either directly or indirectly, and if exposed to unauthorized access can result in harm to the individual. These data types require additional attention and concern before sharing broadly.

Personal data would require the consent of the individual and a thorough and detailed vetting of the parties to which the data would be released for data protection compliance mechanisms and frameworks.

The data applications that pose the greatest risk if exposed publicly without going through a compliance and vetting process would be HR, financial, product development, internal investigations, law enforcement, and product development applications.

PC Question

How can individuals' and businesses' confidence and trust in the way data is used be maintained and enhanced?

NetApp Comment

Confidence and trust is built through transparency. Organisations need to be clear, explicit and transparent about:

- what data they are collecting;
- what they are doing with the data and why;
- who will have access to the data and why;
- how the data will be protected from unauthorized access and use;
- how long the data will be maintained;
- how will the data be destroyed;
- what recourse an individual has if his/her personal data is misused or shared with unauthorized individuals;
- how and individual can opt out of having his/her data shared publicly;
- how an individual can have their data corrected or removed; and,
- the technology solutions implemented to manage the data. As part of the technology solution, organisations need to thoroughly vet their technology partners and suppliers from a data privacy compliance perspective and not just a security point of view. All vendors provide security, but very few will talk about privacy compliance.

PC Question

What weight should be given to privacy protection relative to the benefits of greater data availability and use, particularly given the rate of change in the capabilities of technology?

NetApp Comment

Technology is critical to the growth of any industry, but it still cannot trump privacy laws.

Good technology should take into account not only security, but privacy as well. Privacy by design should be a key consideration before building and implementing any new technology.

If a technology decision only benefits the government and not the citizens, it is not a viable solution. Privacy considerations should not be tossed aside due to cost, flexibility and scalability of a technical solution. The fundamental right to privacy of any individual must factor into the planning process. By conducting detailed Privacy Impact Assessments (PIAs), the government, and other organisations, can balance the needs to comply with data protection laws while embracing new technologies such as the cloud, Internet of Things (IoT), smart cities, etc.

PC Question

Are further changes to the privacy-related policy framework needed? What are these specific changes and how would they improve outcomes? Have such approaches been tried in other jurisdictions?

NetApp Comment

The privacy policy framework needs to include requirements related to transparency, notification, consent and disclosure.

Part of the framework should include a mandatory requirement to conduct Privacy Impact Assessments (PIAs) prior to implementing any new technology that impacts personal data. This will force organisations, including government entities, to address privacy upfront and not just look at security. Security is only one component of privacy.

By implementing these changes, individuals will gain confidence that their personal data is being treated in a fair, legal, and transparent manner.

These frameworks have been implemented in several jurisdictions in Europe, Canada, Hong Kong, New Zealand, Switzerland, and other countries, and have proven to be successful.

PC Question

How could coordination across the different jurisdictions in regard to privacy protection and legislation be improved?

NetApp Comment

Coordination between jurisdictions would allow for the "lessons learned" scenarios.

Countries that have been successful in enforcing data protection legislation and guidelines that allow for the implementation of new technology, while protecting the fundamental right to privacy of every individual, can share the processes they embrace to ensure success.

Rather than sharing information, many jurisdictions automatically form an opinion that privacy laws are an impediment to doing business. That attitude leads to a stalemate where nothing gets solved and conflict continues. Instead, countries should share what they've done, how they've done it, and the benefits achieved not only for the government, but for the citizens as well.

PC Question

How effective are existing approaches to 'confidentialisation' and data security in facilitating data sharing while protecting privacy?

NetApp Comment

One of the challenges we continually observe is the focus on security and not on privacy. Both are indeed critical, but if you only focus on security, you will miss one of the most critical components.

Before addressing security, you must deal with the data privacy component. Encrypting data you never should have collected in the first place, or shared to begin with, will not help you meet your privacy obligations or gain the trust of people. You must conduct a Privacy Impact Assessment that helps focus on what data you need, why you need it, what it will be used for, what laws protect it, what restrictions guide it, who will have access to it and why, where it will be stored and for how long, who you will share it with, and how it will benefit the individual.

Once you address the privacy implications, you can develop policies and procedures that reflect a data privacy compliance approach and build a security infrastructure that protects such data from unauthorised access and use.

PC Question

What lessons from overseas jurisdictions can Australia learn from regarding the use of individuals' and businesses' data, particularly in regard to protecting privacy and commercially sensitive or commercially valuable information?

NetApp Comment

Australia should definitely look at the way the EU, Canada, Hong Kong, New Zealand have managed to balance the fundamental right to privacy with the ability to embrace new technology. These jurisdictions have some of the most restrictive data privacy regimes in the world with harsh penalties, yet have been able to embrace new opportunities delivered by new technology.

PC Question

What are the benefits and costs of allowing an individual to request deletion of personal information about themselves? In what circumstances and for what types of information should this apply?

NetApp Comment

Allowing an individual to request the deletion of certain types of personal data puts control of personal data back into the hands of the data subject and helps foster trust and transparency.

Data that is no longer needed to manage the relationship, is no longer needed for the purpose for which it was collected, has no legal retention period, and is not under a legal hold should be deleted if requested by the data subject. Cost savings can be realized by deleting data that is no longer needed. The cost of not deleting data when it is no longer needed can be more expensive than maintaining it, especially if there is litigation. The cost of electronic discovery can be extremely high.

However, there are also technical challenges in locating and deleting one record from a larger set: the correct record must be deleted, implying a compliance requirement, the rest of the data set must not be corrupted, and there will be costs associated with performing the

tasks. This subject has been addressed in detail in papers such as “The Economics of the Right to be Forgotten” (Byung-Cheol Kim and Jin Yeub Kim, March 2015).[2]

PC Question

What competing interests (such as the public interest) or practical requirements would indicate that the ability to request deletion should not apply?

NetApp Comment

There are several factors to be considered, including which type of record is the subject of the request:

1. permanent/vital records required for legal purposes and business continuity; and
2. temporary records required for a limited period of time that have no legal retention requirement and are not needed for business continuity.

Permanent or vital records have a legal retention period that must be followed and therefore could prohibit the deletion of such information. Temporary records have no business value and are meant to be superseded by new records and therefore should be deleted when they are no longer needed, or upon request.

A clear and explicit records retention policy along with a records retention and destruction schedule should be implemented as part of this project.

As stated in the previous answer, there are costs associated with selective data deletion, and these can be difficult to quantify.

As part of its response to the European Court of Justice’s “Right to be forgotten” ruling, Google requested public comment and evidence to the following issues[3]:

- Are there any procedural issues raised by the case (eg responsibilities of search engines, data protection authorities, publishers, individuals)?
- What is the nature and delineation of a public figure's right to privacy?
- How should we differentiate content that is in the public interest from content that is not?
- Does the public have a right to information about the nature, volume, outcome of removal requests made to search engines?
- What is the public's right to information when it comes to reviews of professional or consumer services? Or criminal histories?
- Should individuals be able to request removal of links to information published by a government?
- Do publishers of content have a right to information about requests to remove it from search?

While these questions are to some extent specific to requirement to remove access to information from a search engine, they do bear consideration in the context of this initiative.

4.4 Questions On Other Restrictions

PC Question

Having regard to current legislation and practice, are further protocols or other measures required to facilitate the disclosure and use of data about individuals while protecting privacy interests? What form should any such protocols or other measures take?

---

[2] http://econ.msu.edu/seminars/docs/Byung-Cheol%20Kim.pdf
[3] https://services.google.com/fb/forms/advisorycouncilcomments/

NetApp Comment

Yes, additional protocols are required to facilitate the disclosure and use of data about individuals. Since this data is considered personal and is protected under country-specific data protection laws, the protocols should include transparent notifications, explicit consents, Data Privacy Agreements (DPA) between the transferring and receiving entities, vetting of technology providers who will provide the infrastructure to capture, store and share the data.

PC Question

Is there need for a more uniform treatment of commercial-in-confidence data held by the Australian Government and state and territory governments?

NetApp comment

Yes, the best approach is always to adopt the most restrictive requirements and adapt the program to meet those. By doing so, you can develop one uniform and consistent process and policy for the collection, use, processing, sharing, transfer and storage of personal information. Trying to manage multiple processes and policies instead of one consistent one is next to impossible. By building a framework based on the most restrictive privacy laws, you can meet your obligations no matter what jurisdiction the data is coming from or flowing to.

PC Question

Are there merits in codifying the treatment and classification of business data for privacy or security purposes? What would this mean in practice?

NetApp Comment

Data Classification is one of the most critical first steps prior to embarking on this data availability and use program. You need to understand what data you have access to and classify it based on the type of data it is and the level of protection it requires from both a privacy and security perspective. A successful program cannot be implemented without first completing a detailed classification effort.

4.5 Questions On Data Security

PC Question

Are security measures for public sector data too prescriptive? Do they need to be more flexible to adapt to changing circumstances and technologies?

NetApp Comment

Security measures need to be flexible based on the type of data involved. Different data classifications are going to require different levels of security. There is no "one size fits all" solution. New technology such as the cloud is going to require new security measures. The digital age is different from traditional data processing. Old security measures do not meet the needs of today's digital world.

PC Question

How do data security measures interact with the Privacy Act?

NetApp Comment

It is important to recognise that security and privacy, although intertwined, are not the same thing.

Privacy is the legal and regulatory aspects of the collection, use, access to, sharing, storing, transfer of personal data. Security is the fortress that protects that data from unauthorised

access and use. If organisations only looks at security, they are missing the most critical component.

Addressing privacy compliance up front as part of the design and planning process will allow organisations to take advantage of new technology. Privacy Impact Assessments (PIAs) must be conducted before even looking at the security aspects. Once the privacy considerations have been met, security will not be an obstacle to embracing new technology. Security will be an enabler to ensure personal data is protected no matter where it rests.

PC Question

How should the risks and consequences of public sector and private sector data breaches be assessed and managed? Is data breach notification an appropriate and sufficient response?

NetApp Comment

Once again this goes back to data classifications. Consequences of data breaches must be assessed and managed based on the type of data that was exposed or infiltrated. Questions that need to be considered include:

- Would the public entity or private sector company be harmed by the exposure of the data;
- Is the data the "crown jewels" of the company that if accessed without permission could do substantial harm to the company;
- Would access to data concerning the government lead to national security concerns;
- Would an individual whose personal data is impacted by a breach be harmed;
- What constitutes harm.

These questions have to be answered as part of this initiative. Data breach notification may not be sufficient if national security is at risk. Private citizens may not take comfort in knowing that, if their financial information is stolen, the only remediation they will receive is a notification of the data breach.

Data breach remediation plans need to be assessed and defined based on the data classifications.

Attachment A

Ms Sheila Fitzpatrick

Global Data Governance and Privacy Counsel, and Chief Privacy Officer

NetApp Inc.

Sheila is NetApp's Global Data Governance and Privacy Counsel, and Chief Privacy Officer based in our headquarters in Sunnyvale, California.

Sheila FitzPatrick has over thirty years' experience as an international data protection attorney. Sheila is considered one of the world's leading experts in data privacy laws and works closely with the US Government, Council of the European Union, country-specific data protection agencies in Europe, Asia/Pacific, and The Americas, as well as National Works Councils, European Works Councils and Law Enforcement Agencies.

Sheila provides expertise and hands-on experience in the areas of global data protection compliance, data sovereignty, cyber-security regulations and obligations, legal issues associated with cloud computing and big data, data breach compliance and management, and records management. Sheila has been recognized by Data Protection Authorities (DPAs) around the world for her depth of comprehension and commitment to data protection laws.

Sheila speaks regularly at global conferences and panel discussions focused on data privacy, cyber security and cloud computing. Sheila sits on many external councils and is currently the Vice-Chair of CompTIA/TechAmerica' s Privacy and Cybersecurity Committees and is actively involved in their Big Data and Cloud Computing Subcommittees.

Sheila holds strategic seats on "by invitation only" committees including the European Union Data Protection Advisory Council, the Asia Pacific Data Protection Framework Advisory Board, the Latin American Data Privacy Forum, the SNIA Privacy Council, the Canadian PIPEDA Advisory Board, and the ANZ Privacy and Cybersecurity Advisory Group.

Sheila holds undergraduate and law degrees from Santa Clara University in Santa Clara, CA, an MBA from Syracuse University in Syracuse, NY, and a law degree from Trinity College in Dublin, Ireland.

~End of Document~