30 ST MARY AXE
LONDON, EC1A 8EP
TEL +44 (0)20 7220 5700
FAX +44 (0)20 7220 5772

2200 PENNSYLVANIA AVENUE
WASHINGTON, DC 20037
TEL 202 955 1500
FAX 202 778 2201

26th July, 2016

RESPONSE TO THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER DRAFT BIG DATA AND PRIVACY PRINCIPLES GUIDE

1. BACKGROUND

This response is submitted by the Centre for Information Policy Leadership (the "CIPL"). Nothing it contains should be taken as representing the views of any individual CIPL member. CIPL strongly supports the focus given by the Office of the Australian Information Commissioner to Big Data analytics, and recognising the enormous societal and economic benefits that can flow from big data and advanced analytics. All CIPL members are global businesses, each of which is committed to using personal data responsibly. For this reason, CIPL chose to provide comments on the Draft Guide to Big Data and the Australian Privacy Principles (the "guide").

Big Data Today

In the modern information age of Big Data, the Internet of Things and cloud computing, new data-driven products and services are enabling scientific and societal developments at a rapid pace and are key drivers of economic growth. Our digital information society depends and thrives on the ability to generate, collect, aggregate, link and use information, including personal data, through increasingly complex technologies and global processes. Understanding how personal information is being used in this environment is becoming increasingly difficult if not impossible for the average person. Thus, expecting individuals to take an active role in deciding how their personal information is used in all instances is increasingly unrealistic.

Yet, data protection and privacy are important societal norms and in many countries are fundamental or constitutional rights. Individuals must have confidence and trust that their data is being used responsibly and its use is consistent with these norms and rights. Thus, where still possible within the world of Big Data, individuals must be empowered to make informed decisions that relate to the use of their personal data. Where individuals can no longer control each particular use of their personal information in this new environment, other protections and mechanisms must be put into place that create the necessary confidence and trust among the public and regulators that personal information is being used in a responsible and sustainable manner for purposes that are beneficial to individuals or society.

2. RESPONSE

CIPL welcomes the Commissioner's consideration of issues arising from Big Data in its draft guidance and welcomes the draft, which is in many aspects reasonable, considerate and well balanced. CIPL

congratulates the Commissioner for undertaking the task of producing regulatory guidance on the topic of big data, which can be used by privacy practitioners across the spectrum of organisations and which also has a capacity to influence the thinking of regulators and policymakers more broadly. This is especially important at the time when the topic of big data and analytics is being debated globally.

CIPL finds the following areas of draft guidance particularly helpful

- The recognition of anonymisation processes, privacy impact assessments and privacy by design as important practical measures which organsiations should engage in within Big Data processing and analytics.

- The focus on the reasonable expectations of individuals in regards to the use of their data;

- Highlighting the risk based framework approach as part of an organisation's Privacy Management Programme in addition to listing a number of high-level risks and mitigating actions organisations should be aware of when embarking on Big Data processing throughout its draft at relevant junctures in its guidance.

CIPL would like to make a number observations regarding certain aspects of issues raised within the draft guide specifically providing comment regarding collection and notice, privacy management frameworks, in addition to some potential additional areas of inclusion within the final guidance by Commissioner.

3. COMMISSIONER'S STIMULUS QUESTIONS

Are there any topics that you believe the draft guide should cover that have not been covered, or should be covered in greater detail?

CIPL finds the Commissioner's guide places too great an emphasis on user consent under APP 3 – Collecting Personal Information as a condition for processing personal data, and insufficient emphasis on the potential scope within the secondary use of data per APP 6 Use or Disclosure of Personal Information.

Reliance on consent

Even where consent in a single processing scenario theoretically appears to work (as currently exists under APP 3), it is doubtful that a repeated and frequent recourse to consent will be workable for individuals in the current information age, where big data and analytics will be performed constantly and automatically, by all types of organisations, on many devices and in all kinds of scenarios – in online, employment, customer, and government contexts.

CIPL believes that additional analysis by the Commission concerning when and how consent remains viable in the Big Data context and when it does not would be beneficial. Such further analysis would reveal that, increasingly and cumulatively, in many circumstances, consent may not be viable and cannot deliver the necessary and effective privacy protections for individuals. Where this is the case, we believe that alternative safeguards do exist that, nevertheless, maintain focus on the interests of the individual in delivering effective data protection.

CIPL would also like to note, that placing complete reliance on consent for Big Data processing places a greater burden on both the user and organisation in the moment of "consent". The single consent model increases pressure on the organisation's privacy policy to gather the scope of consent required for its Big Data processing. The organisation, in turn, is faced with a greater level of information it must deliver to

its users and educate them as to its meaning. The user is also faced with an even wider scope of asks contained within their "consent" in the click " yes" moment. While CIPL welcomes the acknowledgement within the draft guidance that many users do not read privacy policies prior to providing consent as a risk organisations should mitigate in its risk management of Big Data, the alternative options currently available to organisations to gather consent are limited.

This acknowledgement by the Commissioner on the lack of engagement by users with privacy policies acknowledges the wider issue that a downward pressure on privacy policies to be a valley of processing permissions is not feasible for organisations who in many cases will not be certain of the detailed types Big Data processing it will carry out. Widely drawn or heavily detailed privacy notices also do not serve the users best interests in terms of providing transparency of how organisations use the data collected. If reliance on the initial consent gathered is not feasible from a technological point of view or desirable from the perspective of user engagement and transparency, then organisations will need to rely on secondary processing permissions as provided under APP 6.

APP 6 and Secondary Processing

The Commissioner's acknowledgement that most Big Data processing by organisations will fall under the processing exception within APP 6 Use or Disclosure of Personal Information highlights the reality faced by most organisations using Big Data and advanced analytics. While relying on consent to secondary processing is welcomed, CIPL believes the scope provided within this principle is not sufficiently wide enough for organisations and users to benefit from the full capability that Big Data can and will deliver in the future.

Organisations relying on the use of secondary processing consent must meet the criteria where the Big Data processing is related to the primary purpose of processing and also be the reasonable expectations of the user. This two-limb consent risks stifling the potential of Big Data where the use case may not be directly related to the initial data collection or analysis yet provide real user and organisational benefits. CIPL has explored the concept of consent, secondary processing and Big Data analytics in greater detail in the following white paper:

Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/big_data_and_analytics-seeking_foundations_for_effective_privacy_guidance__discussion_document_february_2013_.pdf

Compliance with APP 6 also requires the user to be "reasonably informed" of the additional data processing uses an organisation has in mind. Compliance with this could require including additional data uses within the privacy policy language (which could be vaguely worded or specifically listed, neither of which option benefits the user or organisation). However, as mentioned earlier long or heavily worded privacy policies place an undue burden on the user to read and understand extensive privacy policies at the consent moment. Alternatively, the organisation could be expected to seek additional just-in-time or contextual consents to ensure its processing meets the standard of APP 6, which could prove logistically impossible in terms of informing users when required.

Both scenarios potentially place the APP 6 exception under potential pressure in terms of Big Data processing. The guidance recognises that businesses will rely in the main on APP 6 to carry out Big Data processing. While APP 6 is suitable for more traditional forms of analytics and processing, it does not provide the necessary scope for the potential of Big Data to be explored or harnessed by organisations or end users.

In line with the fact that the APP's were designed to be technology neutral the Commissioner should consider expanding its principles to include the concept of "Legitimate Interest Processing" as a valid ground for Big Data processing. The "legitimate interest ground" for processing is a principle found within the EU Data Protection Directive as well as the new EU General Data Protection Regulation whereby organisations have permission to process data on the grounds that the processing falls within the legitimate interests of the organisation or a third party. This right to process based on legitimate interest is tempered by, or balanced against, any countervailing interests or fundamental freedoms of the user requiring protection. This concept provides a fair balancing of rights and value exchange for both the organisation and the consumer. An organisation is provided with the flexibility to process data, but must balance its legitimate organisational need to continue to understand and evolve its own business against respecting the rights and privacy of its users and customers. An organisation must be able to demonstrate and evidence this balancing of business needs and consumer rights through its risk management programmes and frameworks.

Legitimate Interest As a Ground for Data Processing

Legitimate interest processing is likely to become an increasingly important ground for data processing in the era of Big Data, as it can:

- Facilitate data collection, use, sharing and disclosure in circumstances where consent is not feasible, practicable or effective.

- Enable uses of information for new purposes, beyond the original purposes at the time of collection, provided such uses are not harmful to individuals and appropriate safeguards are implemented.

- Stay consistent with organisational accountability, pursuant to which organisations implement safeguards in the entire lifecycle of information, from collection to use, sharing and destruction.

- Ensure the protection of individuals' privacy, while allowing organisations and society at large to pursue the benefits of new technologies, products and services.

As such, further work by the Commissioner on this subject should be undertaken to explore the potential use of this principle within the context of Big Data. The inclusion of legitimate interest processing within the final guide has the potential to deliver a number of benefits:

- It will respect and ensure the privacy of individuals in a transparent and balanced manner.

- It will ensure the APP Principles' aim of remaining technology neutral and relevant.

- It will provide the data ecosystem with scope and permission to legitimately explore the potential uses and benefits of Big Data in a manner that is consistent with individuals' privacy.

Expanding the APP principles to include legitimate interest processing should also be considered alongside the additional safeguard of the risk-based approach to privacy (the Commissioner's guidance makes references to risk management and risk-based decision making in its sections pertaining to Privacy by Design, Privacy Management Frameworks and Privacy Impact Assessments).

The Risk Based Approach to Big Data Processing

CIPL wishes to underline the importance of a risk-based approach to privacy. CIPL believes that the Commissioner should place greater emphasis within its final guidance on the role of risk and that it should investigate the further use and value of a risk-based approach and its methodology in the Big Data context prior to issuing a final guidance text.

Risk assessments, alongside the legitimate interest grounds for processing, place the responsibility for data protection on the organisation rather than the individual in appropriate circumstances. Risk assessments are inherently linked to organisational accountability and are an integral component of what accountable organisations can and must do.

Organisations are in a unique position to assess and understand the impact of their proposed information use. Thus, they should be allowed and required to use tools and frameworks to assess the potential risks and harms of their proposed information uses on individuals in a given context, implement appropriate safeguards based on these assessments, weigh any residual risk against the benefits of the proposed processing and then make responsible decisions about whether and how to proceed with the proposed processing, taking full accountability for their actions (or inaction) both vis-a-vis individuals and privacy regulators.

Privacy risk assessments can help accountable organisations determine whether and how to proceed with proposed information uses, based on potential risks and harms (both material and intangible) they may cause to individuals. Risk assessment is an integral part of devising robust information security measures and implementing privacy by design. While risk assessment should be performed in connection with all processing activities, they are uniquely suited to enable responsible data use decisions in the context of Big Data for the following reasons:

a. Understanding the likelihood and potential severity of harms to individuals that may result from proposed information uses in big data context allows organisations to understand the impact of their actions and to devise appropriate and targeted mitigations and controls, including addressing any concerns from individuals. It also facilitates weighing any residual risk of harms, after mitigations have been implemented, against the countervailing benefits of the proposed use.

b. Privacy-risk assessments place the burden of privacy protection on the organisation. They are especially useful in big data situations where individual control and consent may not be viable or effective due to the absence of direct interaction with the individual (e.g., if the data has been de-identified, or in case of interconnected devices emitting personal data), or due to the repeated frequency of the information processing, or increased complexity of processing.

c. Because risk assessments focus on the risks to individuals (rather than solely on the organisational risks) and seek to remove or limit such risks as much as possible (or to identify uses that should not be pursued), the individual remains at the center of focus even in the absence of individual consent.

d. A risk-based approach can calibrate applicable legal requirements to specific big data contexts and allows for flexibility in interpretation of data privacy principles, which ensures that they stand the test of time. Thus, the risk-based approach is not an alternative to principles-based privacy protection, nor does it replace or supersede such requirements. It simply allows for interpretation and contextualisation, emphasising privacy protection measures that are more appropriate to the context at hand.

e. The risk-based approach and risk assessment can be useful in determining the compatibility of a subsequent or new purpose when determining compliance with the purpose limitation principle. For

example, if having performed a risk assessment, an organisation determines that a subsequent or new big data processing would have a great likelihood of causing significant risks of harms to individuals, the organisation may conclude that such subsequent or new processing is not compatible with the original purpose (and vice versa).

f. Risk assessments also reduce inefficient deployment of organisational resources by allowing organisations to prioritise their privacy controls according to the likelihood and severity of harm associated with a proposed data use. Such prioritisation is likely to contribute to the overall effectiveness of internal privacy management programs (a principle that is reinforced by the Commissioners itself in its own Privacy Management Framework Guidelines and referenced in the Big Data Draft Guidance).

It also allows for a more holistic approach to information governance and data privacy, ensuring that data privacy shifts from being perceived as an obstacle, to being a business enabler in data driven business processes and the big data world.

A crucial issue with privacy risk assessments is how to identify and agree on the nature, classification and quantification of privacy risks. To provide effective protection, the risk-based approach takes an inclusive approach to harm. It does not only seek to identify and evaluate tangible harms such as bodily injury, financial and other economic harms and loss of liberty, but also considers intangible harms such as reputational harm, embarrassment and discrimination and stigmatisation. The issues relating to Big Data, consent, risk management and transparency raised by this consultation align well with recent and ongoing work by CIPL and which is discussed in greater detail in the following white papers and articles. For a more detailed discussion, please see the resources available via the links below

Papers

Three Solutions for Protecting Privacy in a World of Big Data

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/three_solutions_for_protecting_privacy_in_a_world_of_big_data__executive_summary_december_2015_.pdf

The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

The Role of Risk Management

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf

Articles

Empowering Individuals Beyond Consent

https://iapp.org/news/a/empowering-individuals-beyond-consent/

Transparency and the Future of Driverless Privacy

https://iapp.org/news/a/transparency-and-the-future-of-driverless-privacy/

Are there any topics that you believe the draft guide should cover that have not been covered or should be covered in greater detail?

CIPL would like to highlight two areas that should be reviewed in greater detail by the Commissioner as part of its draft consultation - transparency and context of data use.

Transparency as a Big Data Enabler

The draft guidance advises organisations to act in a transparent manner with their customers to build trust and avoid being "creepy" in support of its guidance under APP 7 and direct marketing. CIPL believes that transparency is not simply a tool that should be used for direct marketing with customers but is another enabling tool within the risk management suite that can be used by data driven organisations engaging in Big Data processing.

Under many data protecting regimes, transparency has been conflated with notice. In a world of big data, remote sensing and other technological developments, meaningful notice is increasingly difficult to provide, which is a point noted in the draft Commissioners Guidance.

Moreover, privacy notices and consents have been used so widely, that even when they may be valuable, they are often ignored by a public suffering from legal notice fatigue. Fortunately, there are many other ways to provide meaningful transparency and individual participation through surrogates, technologies, dashboards, access and the like. The content of transparency tools will also be impacted and influenced by risk management considerations (the importance of the content of privacy policies and notices as transparency tools is noted by the Commission within the draft when it references revising an organisations privacy frameworks as part of its Big Data risk management).

The greater the risk, the more transparent and more meaningful privacy notices and other transparency tools should be. Additionally, in the context of Big Data and analytics where consent may not be practicable, effective or required (due to secondary purpose processing, for example), transparency will increasingly have to be reconceptualized from mere notice (as the basis for consent) to a broader explanation of the value exchange between individuals who provide their data and organisations that use it, alongside explanations as to how organisations protect data from misuse and individuals from harms based on an appropriate risk assessment. Developing transparency along these lines and building it into the risk management culture of an organisation across all of its data processing activities engenders greater trust and willingness to share data on the part of users, thereby enabling an enhanced ability by accountable organisations to use data effectively as well as general progress in developing and applying technologies like Big Data in a safe and transparent manner for everyone in the data sharing ecosystem. Using tools such as transparency is an appropriate method to supplement and support the APP principles to ensure they remain relevant and technology neutral as a supporter and enabler of Big Data.

The Commissioner should place a renewed focus on context and data use in its final guidance text
There is often a compelling reason for personal data to be disclosed, collected or created. Assessing the risk to individuals posed by those data almost always requires knowing the context in which they will be used. Data used in one context or for one purpose or subject to one set of protections may be both beneficial and desirable, while the same data used in a different context or for another purpose or without appropriate protections may be both dangerous and undesirable. The final Big Data guidance should include advice to organisations to focus on the actual uses of Big Data and less on its collection and analysis as part of its privacy management frameworks and programmes. Risk management is essential to assessing the potential for both negative and positive impacts of a proposed use of personal data, identifying appropriate privacy protection tools and ultimately determining which uses should be

permitted. This does not take away or undermine the value of understanding risks at the time of data collection, but it is more appropriate to focus on the whole life cycle of data (which the Commissioner's Draft Guidance seeks to achieve as one of its aims) — from its collection to its various uses and applications and the risks and benefits that attach to those in context

4 PRESENTATION OF THE FINAL COMMISSION GUIDANCE

To ensure maximum utility and scope of its Guidance, the CIPL suggests that the final text from the Commission should consider the following recommendations

- The guidance text would benefit from some examples of Big Data processing scenarios for organisations to illustrate the advice provided. This would be particularly beneficial for guidance relating to secondary processing within APP 6 and Direct Marketing APP 7 and Quality of personal information under APP 10

- The final text should also focus as a core aim of the guidance to include reference examples of tools for compliance, summarised in a simple visual table alongside the interpretation of its key APP principles and existing guidance that is referenced within the text such as the Privacy Management Framework.

- The Commissioner should consider including guidance on transparency within its final text as a tool to facilitate and enable Big Data processing and move away from the traditional reliance on privacy policies and consent mechanisms the value of which the Commissioner itself notes are undermined by Big Data processing.

- A final section could include other best practices, relevant business context relating to all APP principles referenced with the guide alongside the more aspirational, yet still important parts of the guidance.

Thank you very much for considering CIPL's comments. If you require further information, please do not hesitate to contact Bojana Bellamy, President, Centre for Information Policy Leadership bbellamy@hunton.comor Markus Heyder, Vice President and Senior Policy Counselor, Centre for Information Policy Leadership mheyder@hunton.com
.