IoT Alliance Australia

26 July 2016

The Australian Privacy Commissioner
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

consultation@oaic.gov.au

Dear Commissioner,

Response of IoT Alliance Australia (IoTAA) to Consultation draft: *Guide to big data and the Australian Privacy Principles*

Thank you for the opportunity to contribute to the development of the OAIC's draft *Guide to big data and the Australian Privacy Principles*.

This is the submission of IoT Alliance Australia (**IoTAA**). IoTAA has a diverse membership and over 250 volunteers participate in its current workstreams, including valuable contributions from officers of the OAIC, the ACMA, the ACCC and other Federal and State Government departments, authorities and other agencies. While this submission has been prepared by the IoTAA Workstream 3 participants, it may not reflect the views of individual participants in IoTAA or (if applicable) their employers. The officers of the OAIC participating in our workstreams did not participate in development of this submission.

The draft Guide outlines key privacy requirements and encourages the implementation of the Privacy Management Framework. Taking this approach will embed 'privacy by design' in entities' culture, systems and initiatives from the design stage onwards. We would also support a 'security by design' culture in data collection and management.

Our interest in the draft Guide

IoT Alliance Australia was created in May 2015 (then called IoT Think Tank) as part of Communications Alliance. It was registered as a separate (not-for-profit) entity in July 2016 which is hosted by the University of Technology Sydney (**UTS**).

Our interest in the draft Guide arises from the essential role of data handling, data analysis and data sharing between multiple entities, in enabling deployment of the internet of things (**IoT**) services and managing IoT devices to enable those services to be provided.

As the OAIC will be aware, the IoT is the concept of basically connecting any device with an 'on' and 'off' switch to the Internet and/or to each other. This includes everything from vehicles, smartphones, thermostats, kettles, swimming pools, washing machines, headphones, lamps, wearable devices and so on. This also applies to remotely monitored components of machines, such as a jet engine of an airplane or an electricity network, or remotely operated machines such as mining and undersea vehicles. A key element of the IoT is usually

incorporation of sensor devices which may be either passive, monitoring and reporting as to conditions in a particular environment, or active (actuator) devices, involving remote operation of the device in response to the changing conditions in that environment. Frequently the IoT service will be in essence machine-to-machine (**M2M**), rather than human-to-machine, giving rise to concerns as to awareness of consumers and other affected individuals as to handling of personal information about them in the course of provision of such services. Some IoT consumer applications provide consumers with information that enables them to make actionable decisions based upon the analysed information (for example, to turn on an air-conditioner, or to buy chemicals required to treat a swimming pool). Other applications may fully control conditions in a particular environment without any active consumer intervention, and many foresee an automated contract scenario whereby M2M ordering occurs without human intervention. Of course, all such applications require significant data flows and data analysis, often enabled through sharing of particular data fields or data sets between multiple entities (for example, a data analytics services provider, a communications service provider, a device provider, a data warehouse operator, and so on). Applications require trust between consumers and other affected individuals as to proper and sensitive handling of information about them by IoT service providers and all other entities involved in the IoT service delivery chain that have access to information about them, including personal information. That trust is enabled by good privacy management, including appropriate transparency and understanding of information handling practices. Hence our interest in this draft Guide.

About IoTAA

IoTAA is the primary, and indeed, only IoT thought leadership industry body in Australia. Members are drawn from a wide cross-section of IoT service providers, vendors, consultants and suppliers as well as business, universities and consumer groups.

IoTAA aims to define the IoT eco-system, informing and enabling Australian companies to exploit the business opportunities afforded by IoT technology and services, increasing Australia's innovation, productivity and economy. Our key objectives are to:

- drive sound, evidence-based input from industry into appropriate policy and regulation for IoT in Australia;
- recognise, understand and drive the national growth strategy underpinned by IoT enabling technologies, across key sectors of the Australian economy where Australia enjoys a competitive advantage; and
- promote collaboration at all levels including (but not limited to) between industry and Government, across the SME community, start-ups and investors, between service providers and problem/opportunity owners.

There are six IoTAA workstreams that are run by some 250 volunteers who are part of IoTAA. The current six workstreams include the following areas.

1. Collaborative Australian IoT Industry
2. Smart Cities & Industries
3. Open Data & Privacy
4. Spectrum Availability & Licensing
5. Cyber Security & Network Resilience

6. IoT Start-Up Innovation

This submission has been prepared by IoTAA Workstream 3.

IoTAA response

Scope and coverage

The draft Guide outlines key privacy requirements and encourages the implementation of the Privacy Management Framework, noting that taking this approach will embed 'privacy by design' in entities' culture, systems and initiatives from the design stage onwards.

IoTAA strongly supports this approach and notes that the IoT requires facilitation of end-to-end privacy management across multiple entities and often with some sharing of information between an entity responsible for providing an IoT service and providers of platforms or devices used to capture relevant information and providers of passive sensors or actuator devices. Data sharing requires consideration as to data minimisation, in particular, as to where, when and why personal information is collected, used or disclosed in the course of provision of an IoT service, and as to transparency (including notice to affected individuals, which includes consumers) and accountability to affected individuals. Accountability requires:

- clear understanding of the extent of responsibility of each entity in the IoT service delivery chain for privacy management (including information security);
- one entity, usually the service provider to the consumer or other customer of a service, exercising responsibility for end-to-end privacy impact assessment and privacy management;
- third party providers being bound by the same obligations as initial data collectors;
- each party in the IoT service delivery chain ensuring that data is used and retained in accordance with the purpose for which it was collected.

Often the information flows required to provide an IoT service will not be in the high volume commonly associated with definitions of 'big data'. However, many 'big data' applications involve closely similar issues as to information management and sharing of information. Indeed, the draft Guide is really focused upon privacy concerns associated with data analytics services, not 'big data' as commonly understood. For this reason, we suggest that the draft Guide might more appropriately be stated to be a Guide in relation to data analytics and the Australian Privacy Principles. References throughout to 'big data' could be changed to be references to 'data analytics' and 'data analytics services'. This would more accurately reflect the broader remit and relevance of the draft Guide.

De-identified personal information and anonymised personal information

Key objectives of privacy management in provision of IoT services and other data analytics services should be:

- to minimise collection, use and disclosure of personal information to that reasonably required to enable provision of the service; and
- to ensure appropriate transparency to affected individuals of relevant collection, use and disclosure of personal information.

The draft Guide notes that personal information may be de-identified so that the information is no longer about an identifiable individual or an individual who is reasonably identifiable (s 6(1)). Data that has been successfully 'de-identified' is not personal information.

Unfortunately, there remains significant uncertainty as to the standard of risk mitigation required to effect 'de-identification' under the Privacy Act. This uncertainty impedes both development of data analytics services and use of de-identification techniques wherever possible. Continued uncertainty as to 'de-identification' processes and outcomes has potential to significantly impede take-up of IoT devices and IoT services, to the detriment of Australian consumers and the Australian economy.

The term 'de-identification' is sometimes used to refer to a *process* of de-identification, which involves a series of steps, considerations and possible outcomes. The term may also be used to refer to the *output* or *outcome* of a process, being removal of identifiable information such that re-identification of any individual from that information (alone or in combination with other available information) is no longer practicable. This conflicting use is often not a problem: usually when read in the context in which 'de-identification' is used, it should be clear in which sense the term is being used. However, confusion often arises where information is 'de-identified', using that term to mean that no individual is reasonably identifiable but only for so long as technical, operational and/or legal or contractual safeguards effectively protect the anonymisation of that information within the zone of permitted recipients of that information and the protection of that zone is to a standard which renders the risk of broader, less controlled distribution or availability of that information to be low or remote.

To put it another way, a de-identification process may lead to an outcome or output of de-identified information which is still not appropriate for release into the public domain as fully anonymised information (because the risk of re-identification of any individual would then be other than low or remote), but which is reliably and verifiably assured as to re-identification risk through ongoing implementation of appropriate privacy protective safeguards as determined by privacy risk assessment and deployed as 'privacy by design'. It is this level of protection that would enable many IoT services and other data analytics services to be provided in an assured privacy protective framework.

Unfortunately, the drafting of the Privacy Act predated modern data analytics de-identification techniques and as a result the Privacy Act appears to use 'de-identification' as an omnibus term which encompasses both de-identification and full anonymisation. However, this omnibus use does not preclude the OAIC from endeavouring to build a better business and community understanding of the distinction between these two concepts, in particular throughout the drafting of this Guide.

A key issue to note is that data identifiability is not binary. Data lies on a spectrum with multiple levels of characterisation. This is recognised by the Future of Privacy Forum, https://fpf.org/#, which usefully outlines a framework for seven data de-identification classes from Pseudonymous to Anonymous, depending on the presence of direct identifiers, indirect identifiers, and levels of safeguards and controls.

There are significant benefits for Australian consumers and for the Australian economy to be derived from the OAIC endeavouring to promote understanding of the distinction between de-identification and fully anonymised information as an output. Further, that understanding would be assisted by clear legal definitions, such that business may proceed with confidence in this regard.

Firstly, more extensive use of de-identification processes and of technical, operational and contractual safeguards to protect de-identified information, would be encouraged, thereby

stimulating better information management processes including data minimisation and reducing information security risks.

Secondly, end-to-end privacy management would be facilitated, by recognising that entities involved in a service delivery chain may agree safeguards that assure limited and controlled information sharing within those entities in the course of service delivery but preclude uses for other purposes or disclosures to any broader audience.

Thirdly, research activities by universities and other research institutions would be facilitated. Many research activities, particularly in relation to medical or health applications, require transaction level or individual level information to be available to researchers, but this information would be personally identifiable if disclosed to a broader audience or otherwise used outside the relevant safeguards.

For these reasons, we commend to the OAIC inclusion of further discussion in the draft Guide as to de-identification as an appropriate tool in processes for privacy management where information about individuals' transactions or activities is required to be shared but and broader distribution or misuse of that de-identified information could reasonably lead to re-identification of an individual that is the subject of that de-identified information.

We also recommend that the Guide includes three points of clarification in relation to de-identification processes:

- Consistently with treatment of aggregation and other processes where information ceases to be about an identifiable information, a process of de-identification of personal information which transforms that information to a point where the risk of re-identification of any individual in the course of subsequent use or disclosure of that information is low or remote should not be n act or practice in relation to personal information. This might include both de-identification subject to appropriate safeguards and full anonymisation. It would follow that this act or practice should not require notification to relevant individuals where information about their activities or transactions has either been effectively de-identified by being subject to reliable and verifiable safeguards, or fully anonymised. This approach would also be consistent with emerging international academic consensus as to anonymisation and also the extensive judicial analysis of broadly analogous provisions in the United Kingdom, notably Mr Justice Cranston in The Queen on the Application of Department of Health v Information Commissioner [2011] EWHC 1430 (admin) applying the House of Lords decision in Common Services Agency v Scottish Information Commissioner [2008] UKHL 47.

- Any information management that is implemented through safeguards rather than full anonymisation should require an assessment of the risk that these safeguards will not be effective, whether through internal malpractice (or carelessness) or external intrusions. The same standard of assessment of re-identification risk should apply in reaction to such possible occurrences as applies in relation to assessment of re-identification risk for determination of whether information has been fully anonymised.

Privacy statements, policies and collection notices

A key issue for all APP entities in complying with the Privacy Act is how to get the balance right between transparency and understanding of consumers and fulsome disclosure. As the OAIC recognises, sometimes 'less is more' if less text promotes better understanding of consumers by highlighting important or unusual privacy impacts of a particular service rather than more text cataloguing all privacy impacts however insignificant or commonly understood and by sheer density obscuring important or unusual privacy impacts.

Perhaps nowhere is this issue more stark than for IoT services to consumers. Many consumers will subscribe for these services through click-throughs on mobile phones or other consumer-friendly mechanisms. The utility of a privacy statement in such a context, where length or complexity is significant, is cause for consideration.

As the OAIC has already noted in its *Guidance to the Australian Privacy Principles*, there is significant overlap between what must be included in an APP 5 privacy notice and what is required for inclusion in an APP privacy policy. This was partly because privacy notices were intended to be service specific and provide more immediate and therefore impactful notice to a consumer than the more general information as might be included in a privacy policy. However, with widespread adoption of click-throughs to facilitate consumer convenience, an emerging question is whether privacy notices may provide more impactful notice to a consumer than service specific information as might be included in a privacy policy, which both consumers and privacy advocates can read at their leisure and compare with privacy policies of other entities providing similar services.

The draft Guide notes that APP 5 requires an entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. An entity must take reasonable steps before, at the time of collection, or as soon as practicable after it collects personal information. The guide goes on to state that an APP 5 privacy notice is different to an APP privacy policy. "A privacy notice should provide specific information relevant to a particular collection of personal information. The purpose of the privacy notice is to provide an individual with enough relevant information to make an informed decision about whether to provide their personal information to an entity. While an APP privacy policy is more general in nature about the entity's information handling practices it should generally not be used as a substitute for an APP 5 privacy notice."

While we understand the traditional rationale for this approach and we understand the statutory interpretation underpinning it, we query whether it is a necessary interpretation of APP 5 and further whether this interpretation effects the best outcome for consumers.

As the draft Guide already notes, "Privacy notices have a big job to do. They need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multi-layered and user centric privacy notices. Innovative approaches to privacy notices can be adopted, for example 'just-in-time' notices, video notices and privacy dashboards. Where possible privacy notices should be multi-layered and user centric to assist with readability and navigability. This means that brief notices are provided which are supplemented by longer notices. The timing of notices can also occur more dynamically to ensure information is given in context, at the right time, in a way that is easy to read."

We suggest that the draft Guide should take cognizance of the following likely facts:

- many, probably most, consumers will not read beyond click-throughs or ever get to the more fulsome layers of multi-layered privacy notices;

- consumers are more likely to review service specific terms in a privacy policy that is available well before first use and which has more enduring accessibility and availability than terms on a smartphone made available when first signing up for or accessing a service;

- current practices as to privacy disclosure and transparency of consumer-information practices, lack consistency.

Accordingly, we suggest that the Guide should recognise that appropriate privacy notice under APP 5 might be through expansion of an APP 1 privacy policy. Such expansion of an APP 1 privacy policy would include service specific coverage where this is consistent with achieving the objective of APP 5 to achieve transparency of privacy impacts arising from provision of a particular service to consumers.

We trust that these comments are of assistance to the OAIC in its further review of the draft Guide.

Should you wish to discuss any aspect of this submission, kindly contact Peter Leonard of Gilbert and Tobin as the coordinator of IoTAA Workstream 3 (*Open Data & Privacy*) and he will coordinate our further input.

Yours sincerely,

John Stanton

Chair Executive Council
IoT Alliance Australia