IoT Alliance Australia

12 December 2016

Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra City ACT 2601

www.pc.gov.au/current/data-access

Dear Commissioners,

Response of IoT Alliance Australia to *Draft report as to Data Availability and Use*

Thank you for the opportunity to contribute to the development of the Commission's *Draft report as to Data Availability and Use: October 2016* as released on 3 November 2016.

About IoTAA

This is the further submission of IoT Alliance Australia (**IoTAA**). As the Commission will know, IoTAA submitted in relation to the Issues paper: submission 188. We have not repeated comments in that earlier submission.

IoTAA is the peak Australian Internet of Things (**IoT**) body, with a diverse membership over 180 companies and 360 participating volunteers from members. See further www.iot.org.au.

The association is a registered not-for-profit entity currently hosted by the University of Technology Sydney (UTS).

IOTAA's vision is to empower industry to grow Australia's competitive advantage through IoT. IOTAA's purpose is to accelerate IoT innovation and adoption by:

- activating and supporting collaboration across industry, government, research and communities
- promoting enabling, evidence-based policy and regulation
- identifying strategic opportunities for economic growth and social benefit

There are currently six IoTAA workstreams, covering 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

While this submission has been prepared by participants in the IoTAA Open Data and Privacy workstream (workstream 3), this submission may not reflect the views of individual participants in IoTAA or (if applicable) their employers. The officers of PM&C, the OAIC and the ACCC participating in our workstreams did not participate in the development of this submission.

We first make some general comments in relation to the Draft Report, before turning to consider the proposed Comprehensive Right in more detail.

Generally

(a) We support the Commission's emphasis upon consumer trust as a key attribute of the social contract between individuals (consumers and citizens) and businesses and governments that enables use and limited sharing of information about individuals. Consumer trust is integral to adoption of IoT-enabling technologies and services and therefore to achievement of the benefits to society that are expected to flow from uptake of IoT services. Maintenance of consumer trust is rightly identified by the Commission as an economic priority: indeed, perhaps the most important factor to achieving efficiencies within the Australian economy through increasing availability and use of data, including information about individuals. Consumer trust is also rightly a consumer protection issue. Businesses and government should be held to account when they do not handle information about individuals in accordance with reasonable expectations of consumers based upon the nature of the relevant services and what businesses and governments have said that they will do, or not do.

(b) Regulatory intervention in support of availability of information about consumers may be required in particular sectors of the economy where markets fail and consumers cannot exert pressure to ensure availability of information about their transactions to enable price comparisons and reasonably facilitate switching of service providers. However, we are not aware of evidence of economy wide market failure of service providers failing to respond to consumer pressure for availability of information about their transactions, such as might then require economy wide regulatory remediation.

(c) At its core, collection, handling and availability of information about identifiable individuals and their personal activities is an issue of information privacy, already addressed through rights of individuals to access personal information about them. Often access to personal information (as already required by Australian Privacy Principle 12 and the subject of detailed guidance by the Australian Privacy Commissioner) requires careful handling of an access request in a manner that is sensitive to privacy or security concerns of other individuals (for example, holders of joint accounts or guarantors of accounts), and that also addresses legitimate concerns of the alleged subject of the access request (for example, where an estranged spouse is seeking to obtain details about their ex-partner's location or activities).

(d) The Australian Privacy Principle 12 right of individuals to access personal information about them is not often exercised. However, the right is broadly drafted and interpreted by the Australian Privacy Commissioner and simple and easy to exercise. If the access rights afforded by Australian Privacy Principle 12 are perceived by the Commission to be inadequate, such perceived inadequacies could readily be addressed by selective and targeted statutory or regulatory intervention: an example of selective and targeted strengthening of privacy laws is afforded by the recent *Privacy Amendment (Reidentification Offence) Bill* 2016. If the concern of the Commission is that resources or enforcement powers of the Australian Privacy Commissioner are inadequate to ensure effective enforcement of individuals' rights to information, those regulatory resources should be adjusted, consistent with the benefits to the Australian economy that the Productivity Commission sees as flowing from improved data availability and use. If privacy rights and enforcement powers as so

expanded are insufficient to address sector specific or service specific failure of service providers to respond to consumer pressure for availability of information about their transactions, then consumer protection provisions of Australian Consumer Law, including as to unfair contract terms and unconscionable conduct, might then be invoked by the Australian Competition and Consumer Commission. In short, alternative and more targeted interventions could address key issues that the Commission identifies as requiring the economy wide, broadly drafted Comprehensive Right.

(e) Our view that collection, handling and availability of information about identifiable individuals and their personal activities should be addressed as an issue of information privacy is not a view which the IoTAA has formed based upon a sanguine view of the operation of privacy law today. We also support the Commission's view that information asymmetry between businesses and governments and individuals as to uses of information about individuals needs to be addressed if consumer trust is to be nurtured and sustained. The current 'notice and consent' framework of privacy laws is under challenge as a result of many factors, including an increasing number of participants in most service delivery eco-systems, cross-jurisdictional service delivery and development of a click-through culture as services proliferate and terms and conditions (including as to collection, uses and disclosures of information about individuals) become more complex. The work program of IoTAA Workstream 3 includes exploring ways to reduce information asymmetry between service providers and individuals through use of standardised and simplified notifications as to collection, use and disclosure of information about individuals. Measures currently under consideration include 'just in time' notifications as to unusual features of data collection or use and simplification of terms and conditions through uses of standard terminology and by reference to principles based codes that address commonly accepted collections, uses and disclosures inherent to particular industry sectors or applications. Targeted notification would specifically address and highlight for consumer attention any unusual features of information handling and disclosure that a customer might not reasonably anticipate as associated with a particular service or application.

(f) We agree with the Commission's preliminary view that there is no demonstrable public interest for the government to intervene as to the pricing of data sets by private sector data custodians.

(g) We also agree with the Commission's preliminary view that there is a demonstrable public interest in policy measures to stimulate release of data sets by Australian Government agencies, including measures to address concerns of government data custodians as to exposure to re-identification attacks, reputational risk and legal liability as might arise through undue or unwarranted reliance upon data by data users (such as service providers) where data is released without assurances as to data quality or reliability or continuity of supply. Government agencies should be provided with appropriate incentives and protections to ensure that release of data sets is not unduly impeded by such concerns. We concur with the Commission's preliminary view Government agencies should generally release data as a publicly funded resource at marginal cost of preparation for release and with minimal value add.

(h) We also support a regulatory framework which permits data linkage projects (whether using public sector data sets or private sector data sets) where data can be linked in appropriately controlled 'Privacy by Design' frameworks, including through anonymised transactor matches conducted by trusted third parties under technical, operational and contractual safeguards that are reliable and verifiable and where the data collector and data custodian remains accountable to individuals in relation to maintenance and effectiveness of these safeguards. Ethical and social concerns as to data linkages are best addressed through ethics committees or other 'customer advocate' initiatives which ensure that possible concerns of individuals about uses of

information derived from personally identifying information are anticipated and considered in the design and specification phase of data linkage projects.

Comprehensive Right

(i) We agree with the Commission that the proposed Comprehensive Right should not be a general instrument of competition policy and regulation. As the Commission notes, Part IV of the Competition and Consumer Act 2010 and Part IIIA and the various other access regimes are the appropriate vehicles for competition regulation.

(j) However, we note the Commission's view that the data transfer aspect of the Comprehensive Right is seen by the Commission "as an integral part of facilitating competition in markets and reducing barriers to market entry. It will also, like the power to opt out, improve consumers' ability to control their data and so should serve to lift confidence over time that they too – along with governments and businesses – can choose how and when to use their own data." [at page 348] To the extent that "facilitating competition in markets and reducing barriers to market entry" is accepted as a legitimate objective of creation of the Comprehensive Right, the right should be assessed having regard to the extent to which such benefits are likely to be achieved and the attendant costs. The scope and ambit of operation (by industry sector and by application) of the Comprehensive Right should be determined having regard to anticipated consumer benefit properly assessed and weighted against the costs to business in implementing the Comprehensive Right in relation to their services and applications. The benefits, and those costs, will vary significantly sector by sector and over time, depending upon such factors, including development of agreed data discoverability ontologies and data interface standards by sector and by application. These developments will be either led, or at least heavily influenced by global developments over which Australia may have little influence. Costs and benefits therefore need to be assessed at a more granular level than economy wide.

(k) We note that the Commission deliberately distinguishes the proposed Comprehensive Right from individuals' rights in privacy and accordingly does not see the Comprehensive Right as an implementation of any recognised human right. The Commission suggest that the Comprehensive Right would be an entirely new statutory creation and should be evaluated as such. We have above expressed our view that collection, handling and availability of information about identifiable individuals and their personal activities should generally be addressed an issue of information privacy, not requiring creation of a new statutory Comprehensive Right.

(l) Most (if not all) of the data sets identified by the Commission as to be "consumer data' are "personal information" under the Privacy Act. To the extent that uncertainty remains at the boundary of the definition of "personal information" as to the point beyond which an individual ceases to be 'reasonably identifiable', that same uncertainty arises at the boundary of the definition of 'consumer data' and cannot readily be stated as a general principle and then addressed by statutory drafting. In any event, judicial guidance as to this point may be expected when the appeal decision of the Full Federal Court in *Privacy Commissioner v Telstra Corporation Limited* (VID38/2016) is handed down over the next few months.

(m) The most likely point at which significant additional costs would be incurred by businesses as a result of implementation of the Comprehensive Right would be in creating data management and data governance to facilitate a right of transfer of consumer data. These costs will be much higher if the outer boundaries of data that is subject to the Comprehensive Right do not match the boundaries of personal information as required to be managed by APP entities in accordance with the Privacy

Act. If the boundaries are not closely aligned, the Comprehensive Right will require an overlay of compliance frameworks and processes additional to existing APP compliance frameworks and processes.

(n) Further, the point at which information about uses of devices, networks or systems ceases to be information about operation of the devices, networks or systems by a (reasonably identifiable) individual regulated as "personal information" and then becomes de-identified information should be the same for any proposed new right in relation to consumer data (whether a new Comprehensive Right under consumer law or an extension of existing privacy law) and for privacy laws. Any difference between the demarcation point for a consumer right and for privacy rights will create burdensome compliance costs and uncertainties for businesses and government in data management and data governance. Any difference would also be likely to lead to confusion of consumers.

(o) The Comprehensive Right is presented by the Commission as necessary to maintain consumer trust in services and applications that are increasing collections and uses of data about identifiable consumers, by giving individuals transparency as to, and power over, data held on them. The Commission does not explore the extensive right of individuals to access personal information about them as afforded by Australian Privacy Principle 12 or comment as to why that power is deficient or otherwise inadequate. It is correct that the right to access personal information does not explicitly include a right of portability of personal information that an individual has provided to an APP entity.

(p) If the Commission remains of the view that an economy wide right of data portability should be provided to individuals, we commend for the Commission's consideration and comparison of Articles 2 and 20 and Recital 68 of the new EU *General Data Protection Regulation* (EU 2016/679) at Articles 2 and 20 and Recital 68. The effect of these requirements will allow individuals to obtain and reuse personal information about them which is personal information that they have provided to a data controller (in Australian terms, an APP entity that collects or otherwise controls the handling of personal information about individuals). Information provided to a data controller appears intended to include transaction records: detailed guidance as to the operation of this new requirement is expected to be released over the next few months. Data required to be made available must be made available in a structured, commonly used and machine-readable format. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. The individual also has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. If the access rights afforded by Australian Privacy Principle 12 are perceived to be inadequate, a corresponding 'right' could be created as an additional Australian Privacy Principle. Principles based privacy regulation allows for flexibility and adaptability of data portability by sector or by application. The Privacy Act also facilitates creation of industry codes by relevant APP entities.

(q) To the extent that a service provider uses its trade secret or otherwise proprietary data analytics techniques and technologies to value-add or transform data significantly beyond basic compilation of transactional data or activity data, this significantly value-added or transformed data should not be regarded as Consumer Data. To allow a consumer to appropriate these value-adds and enhancements that are the intellectual property of the service provider merely because the value-adds relate to that individual does not make that appropriation justifiable. In any event, the Privacy Act already protects affected individuals by requiring destruction or deidentification of information about individuals where retention of that information is no longer required within the stated proposes for its collection and use or otherwise required by law.

(r) To the extent that a service provider generates network management and other traffic management or other operational data about uses of devices, networks or systems in the course of provision of services to consumers, that data should be treated as technical and proprietary information separate and apart from the transactional and related information, for all aspects of the Comprehensive Right. In other words, technical or other service delivery or customer fulfilment data not directly relevant to the individual's transactional record should not be subject to any Comprehensive Right. This information is about '*how*' a service is provided to the consumer, not the '*what*', being consumer data that the Commission envisages might be required to be made available within the Consumer Right in each of its aspects.

(s) The right to consumer data should also be time limited, both for administrative simplicity and to ensure that personally identifying data is not required to be retained for longer than it really needs to be maintained to service any identified consumer need. We suggest that 12 full months back records from date of request generally should suffice.

(t) To illustrate how the above suggest principles might apply, we provide (as attached) a case study of a Fitness and Wellness IoT Service. We would be happy to expand upon this case study, or provide other case studies, if this would assist the Commission's deliberations.

(u) In summary, our view is that any right to transfer of Consumer Data should not:

- undermine incentives for services providers to innovate by value-adding in service feature and functionality and improving personalisation of services by data analytics and data transformations, whether information remains personally identifying or not;
- facilitate free riding by less innovative service providers upon innovations by first movers;
- unfairly appropriate, or otherwise undermine, trade secrets and other intellectual property of first movers;
- extend beyond information provided by an individual and information as to transactions of the individual;
- apply to small businesses, except to the extent that particular applications or services (e.g. patient records are expressly considered as requiring conferral of the right and then brought within the right);
- require provision of identifying data (such as technical, service delivery and fulfilment) and value added proprietary information that goes beyond transactional records relating to a sensible period (say, 12 months);
- require provision of information other than in its native format or a commonly used, structured and machine-readable format;
- override contracts as negotiated or otherwise actively agreed between individuals and service providers (accepting that non-transparent terms of 'I agree' click-through contracts should not be allowed to circumvent basic rights).

(v) IoTAA strongly supports standards, data ontologies and other data sharing initiatives that promote data discoverability and safe interworking of IoT devices. Such initiatives, when properly designed and implemented, should promote availability and uptake of IoT services, to the benefit of consumers. For example, IoTAA actively supports uptake

of the HyperCat protocol for smart city devices and its likely extension through further standards development into smart buildings. However, standards and codes for data sharing are likely to be highly sector specific, or application specific, and driven by unpredictable global and technology developments. Australian regulation should not inadvertently impede the ability of Australian IoT service innovators by imposing standards or other requirements that are significantly out of step with international developments.

(w) IoTAA notes that there may be perceived consumer benefits in consumers "having a copy of data about them provided to an entity that is not a competitor (for example, provision of medical records to a life insurance company or provision of utility payment information to a credit provider), or authorise a third party to transfer it on their behalf". Again, the extent of benefit must be weighed against additional costs, including externalities of impeding innovative and possible competition.

(x) There is an unexplored assumption underlying the Commission's proposed statement of the Comprehensive Right that the definition of Consumer Data for dealing with the aspect of data transfer should be the same as the aspects of the right of consumers being able to stop collection of, or access and edit, Consumer Data.

We submit that this assumption needs to be unpacked and examined.

(y) Costs of implementation of the data transfer aspect of the Comprehensive Right are likely to be substantial: indeed, huge if API-based availability was mandated. The costs will be proportionally greater for smaller businesses including new innovative start-ups. These costs should not be imposed as an economy wide burden: benefits should be reasonably assessed sector by sector, or application class by application class.

(z) If a Comprehensive Right is to be imposed, it should be imposed only following a proper process of independent evaluation and public consultation on the basis of sector by sector, or application class by application class, with implementation then by declaration as required sector by sector, or application class by application class, and then with review and re-determination or sunset provisions. For example, emerging global standards or industry sector practices may render obsolete past determinations.

(aa) Reflecting that costs of implementation of the data transfer aspect of the Comprehensive Right are likely to be substantial and that those costs will be proportionally greater for smaller businesses including new innovative start-ups, any process of independent evaluation and public consultation such encompass consideration of thresholds or other criteria for determining which entities within a particular industry sector or application class should be subject to the Comprehensive Right. Any determination might reasonably be subject to class exemptions.

(bb) The Comprehensive Right, if it is to be created, should be conferred upon individuals. The right relates to trust of individuals in the handling of their data,. It would not be appropriate to confer the right upon the broader class that includes businesses that are deemed consumers under the Australian Consumer Law.

We trust that these comments are of assistance to the Commission in its inquiry and drafting of the Final Report.

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