IoT Alliance Australia

12 August 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 (IoTAA) to Issues Paper *Data Availability and Use*

Thank you for the opportunity to contribute to the development of the Productivity Commission's Public Inquiry as to *Data Availability and Use*.

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 Office of the Australian Information Commissioner (**OAIC**), the Australian Communications and Media Authority (**ACMA**), the Australian Competition and Consumer Commission (**ACCC**), the Department of Prime Minister and Cabinet 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 the development of this submission.

Key submissions

(a) Many new uses and applications of data rightly cause concerns for consumers as to excessive collection and use of personal information about individuals.

(b) The principles-based approach in Federal data privacy regulation (as embodied in the Australian Privacy Principles **(APP)** under the Australian *Privacy Act 1988 (Cth)* **(Act)** is adaptive to evolving applications of data that is personal information about individuals.

(c) The Act and the active administration of that Act by the OAIC seek to provide appropriate regulatory incentives to ensure that:

- through the requirements for privacy policies and collection notices provided to affected individuals, collection, use and disclosure of personal information about individuals is managed by certain entities, both government agencies and private sector organisations (**APP entities**) in an open and transparent way. As used in Section 24 of the *Australian Consumer Law* (**ACL**), a term is transparent if it is expressed in reasonably plain language, is legible, presented clearly and readily available to any party affected by the term;

- collection, use and disclosure of personal information is minimised to that which is reasonably necessary to give effect to an openly and transparently disclosed purpose and reasonably anticipated secondary purposes;

- each individual may access and correct any personal information held by any APP entity about that individual and seek assistance from the OAIC if that right of access is obstructed or delayed or refused; and

- for non-disclosed data analytics applications conducted by APP entities, before those applications are conducted, any relevant personal information is first reliably and verifiably de-identified. This de-identified information (if not manifestly anonymised such that the risk of re-identification is negligible) is protected by technical, operational and contractual safeguards to ensure that individuals will not subsequently be re-identified through any use or analysis of this de-identified information by any person or entity who may have access to this de-identified information.

(d) Notwithstanding these legislative requirements and the OAIC's administration and guidance, there remain concerns about whether these requirements are being met in practice. Privacy policies and collection notices can be not readily intelligible to consumers: indeed, some privacy advocates contend that this is often the aim of the drafters. Deployment of Internet of Things **(IoT)** devices may also limit consumers' convenient access to privacy policies, or hinder their opportunity to read privacy policies in full: sometimes there is either no, or no immediate, screen interface and sometimes functionality is mobile-only. Further, there is a concern that consumers generally do not understand data flows – or even that data flows are inherent in IoT deployment. Then there is the category of consumers or individuals who enter someone else's IoT-connected home or who drive a friend's car, whose data may also be collected as a result and without their knowledge and consent unless active further steps are taken to ensure that their consent is obtained or reasonably may be inferred.

(e) The right of individuals under the Act to access and correct personal information held by any APP entity about them (APP 12.1 and APP 13.1) inevitably leads to issues as to when information is no longer sufficiently related to an individual to *be personal information about that individual*. Perhaps surprisingly, this issue has not been the subject of judicial decisions in Australia and precedents under analogous statutes in other jurisdictions are very limited. Ambiguity as to the data fields or data sets that are sufficiently related to an identifiable individual to be personal information subject to a right of access by that individual is squarely in contention in the Full Federal Court in the Ben Grubb appeal (*Privacy Commissioner v Telstra Corporation Limited VID38/2016*) scheduled to be heard in the Full Federal Court in August 2016. This will be the first significant judicial determination of this question in Australia. It would be appropriate for the Productivity Commission to defer further consideration of the scope of personal information under the Act until the Full Federal Court publishes its reasons for decision following this appeal hearing.

(f) Consumers are concerned about collection and uses of personal information, but their concerns do not begin and end with data privacy. Many IoT applications require establishment and maintenance of trust between IoT service providers and other entities involved in the IoT service delivery chain as to proper, sensitive and transparent handling of information about affected individuals (whether or not personal information). That trust is partially facilitated by good privacy management, including appropriate transparency and understanding of information handling practices. Many consumers are now demanding greater transparency than has been expected of businesses to date as to diverse uses of data, for example, as to the pricing of services as offered to different customer segments or classes of users, or as to disclosures to law

enforcement agencies or private litigants. The need to establish and maintain trust will be an important constraint upon information handling practices of IoT service providers and other entities involved in the IoT service delivery chain. That trust depends on a clear understanding at the consumer level of data flows and handling practices, as well as knowledge of any breaches and the remedial action taken in response to such breaches.

(g) Subject to reasonable concerns of Australians as to personal information or other sensitive information about them entering into the public domain, being shared inappropriately or otherwise being used in ways that that are not transparent, open and understood and agreed, data flows should be facilitated as promoting business efficiency and consumer welfare. Data analytics and uses of data through IoT applications will usually promote business efficiency and consumer welfare through any or all of:

- reduced costs from higher asset utilisation;
- higher labour productivity;
- lower waste and improved supply chain logistics;
- businesses gaining new customers from improved product experiences; and/or
- reducing the time to market for innovations.

(h) Many governments around the world, including the Federal government and State and Territory governments, have stated an intention to release public data sets wherever practicable. This commitment to open government data reflects policy that, because government data is collected at the expense of the public purse for the benefit of government in serving the public good, the default should be that this government data is released, non-exclusively and as 'open data'. The exceptions to this default rule might reasonably be if any of (1) detriments to consumers, or (2) detriments to national security or good government, or (3) breach of conditions of collection of that data, can reasonably be identified as associated with the release of a public data set.

(i) Benefits to the Australian economy through competitive commercial value-added applications and research uses of open government data are likely to significantly exceed any value that government might capture by itself seeking to derive rents from charging for public data, or by exclusive licensing to a single private sector provider. If government elects to value-add and commercialise government data either by itself or through an exclusive contracted provider, government should not provide disincentives to use of, or derive monopoly rent from, exploitation of a public good. In such circumstance government should make available the 'raw data' (from which that value-added application is developed by itself or exclusive contracted provider) on a non-exclusive basis, either for free or for charges that recover directly attributable costs of making that raw data available.

(j) Governments should also not be subject to disincentives that impede the release of government data sets such as open government data for commercial value-added applications and research uses. Although privacy concerns are often cited as the primary disincentive, there is increasing recognition that other possible liability exposures may need to be considered and appropriately mitigated to ensure that expansion in the range and depth of open government data sets is not impeded. Making data available for use in diverse and perhaps unanticipated applications creates legitimate concerns as to exposure to legal liability of data sources, including public sector entities, that capture, curate or make available that data. Many data sources will be

concerned that raw data may be incomplete, intermittently available or otherwise unreliable and accordingly unwilling to release that data without quality assurance or effective protection against legal liability. Improvements as to data quality, or at least a clear statement of qualifications as to data quality, are desirable, but concerns as to data quality should not unduly impede the release of government data sets. Governments should be encouraged to develop terms for release of open government data that state any known deficiencies or qualifications as to data quality of those data sets, but which do not expose government to liability in relation to subsequent value-added uses or applications of that government data. In addition, where the government uses data sets for the development of its own applications, transparent governance frameworks may be required to ensure that such use promotes rather than hinders private sector competition.

(k) There is also a significant prospect that concerns about loss of control of data (for instance, that data may be used by competitors or others adversely to the interests of a data source or data controller), or the information security of data that passes through the IoT service delivery chain, may significantly impede data sharing and provision of open IoT platforms and devices. Unless this concern is adequately addressed a likely outcome would be to advantage fully integrated IoT service providers, closing out opportunities for specialist or niche providers. This would likely be adverse to Australian start-ups and other Australian businesses in competing with vertically integrated global operators that can operate 'closed system' IoT services and therefore do not need to address the diverse issues associated with data sharing within the IoT service delivery chain. In other words, effective and predictable legal protection (in Australia and in other markets) that facilitates data sharing within the IoT service delivery chain is likely to be more important to Australian start-ups and other Australian businesses than to vertically integrated global operators that provide 'closed system' IoT services in Australia. As a corollary, assurances as to the predictable use of consumer data, will play a critical a role in generating consumer confidence and it will be important for smaller entities and start-ups to preserve this confidence by being able to reliably conform with and implement the APPs, to the same degree as the larger 'closed system' operators. Simplified but effective data management processes may facilitate uniform implementation across start-ups, small and large enterprises as well as 'closed system' operators.

(l) Another significant impediment to data sharing is lack of a common language or semantics for description of data and classification of data sets and their characteristics. Requirements for common terms to enable coordinated and integrated delivery of health services and interoperability of health information systems led to the health sector being relatively advanced in this area. SNOMED Clinical Terms is a systematically organized computer processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting. SNOMED CT coverage includes clinical findings, symptoms, diagnoses, procedures, body structures, organisms and other etiologies, substances, pharmaceuticals, devices and specimens. Integration of geo-spatial data sets has promoted standardisation of data classifications for geo-mapping. In many fields relevant to IoT, including smart cities and smart homes, the development of common terms and classifications is much less mature. That lack of maturity significantly impedes the 'discoverability' of data that is often key to sharing of data at reasonable cost. If a machine cannot readily 'see' the data by semantic searching, the data is of limited value – often the cost of translations or other activities to 'cleanse' the data and present it ready for semantic searching will be prohibitive of data sharing and data re-use. The *Enabling IoT for Australia* report[1] commissioned by IoTAA, points to data sharing as a critical enabler for industry innovation through the use of IoT technologies. Interoperability standards for sharing

[1] Available at http://www.commsalliance.com.au/Documents/Publications-by-Topic/IoT.

data are a key enabler for data sharing and provide an opportunity for Australia to take a lead in selected industry sectors, particularly through promoting use of commonly accepted terminology and data classification standards that are also accepted internationally. Promoting data discoverability would facilitate market entry by Australian IoT service providers and assist their international competitiveness. Promoting data discoverability does not require any regulatory decision as to whether IoT devices and services should be open or proprietary. Rather, common terminologies and data classifications will facilitate both open and proprietary devices and systems, by facilitating data sharing where persons that curate that data elect to allow data sharing. Often data discoverability may be promoted without direct regulatory intervention. For example, the Hypercat PAS 212 published by the British Standards Institute specifies a means to automate the discovery of data resources, without either the client or server having to be written to be explicitly compatible with each other. Some tenders for major urban development projects conducted by British government authorities have mandated use of Hypercat PAS 212 for urban precincts, to facilitate smart city interoperability of sensor devices and services. We commend consideration of such creative approaches to promotion of data discoverability.

(m) Data sets collected or curated by businesses are already subject to the operation of the *Australian Competition and Consumer Act 2010* including the ACL, as well as the Act and sector specific laws such as those statutes addressing health information. Provisions of the *Australian Competition and Consumer Act 2010* (as that Act may be amended following recent relevant reviews) are appropriate to address concerns as to anti-competitive conduct in relation to handling of data, including exclusive dealing and other refusals to supply, and in IoT applications. However, consideration needs to be given as to whether the ACL needs revision to address IoT, particularly give the fundamental role of characterisation as either 'goods' or 'services' in determining which consumer rights arise, and which remedies are available, under the ACL. IoT services and the data flows that enable those services do not readily fit within traditional classification as goods or services. Workstream 3 *Open Data and Privacy* of the IoTAA has a project underway to consider how consumer protection laws may need to change in order to appropriately address IoT services.

(n) Australian copyright law provides very limited protection for databases and for computer-generated works, which fails to recognise or encourage intellectual and commercial investment in these types of works. In a digital context, databases and compilations are increasingly created through the joint efforts of multiple contributors, and the use of (new) technologies. A failure to protect commercially valuable works which are substantially computer-generated (as opposed to being the direct product of human effort) fails to recognise the use and adaptation of new technologies, and is a disincentive to the creation and dissemination of these works. Misappropriation of these works by third parties can cause significant damage to the owner of the works.

(o) Limitation in the scope of copyright protection for databases and for computer-generated works may not, however, be a significant impediment to the development of data-driven businesses and 'data assets' in Australia provided that other areas of law continue to develop to afford appropriate protection to non-proprietary assets in the form of trade secrets, including databases of business information that have the necessary character of confidence to qualify for protection under Australian law as confidential information.

(p) In some other jurisdictions, protection of databases and computer generated works has been addressed by a sui generis legislation (for example, *Directive 1996/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases*). While experience with these statutory rights suggests that careful

consideration needs to be given to their interpretation and application (which is the same for any new legislation), there is scope in Australian to consider similar laws.

(q) Further, there is a growing international trend towards developing trade secret law to supplement copyright and patent laws. By way of example, on 27 May 2016 the Council of the European Union approved the Commission's proposal on the Directive on trade secrets as amended by the European Parliament in March 2016: see further https://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en, and compare the *Uniform Trade Secrets Act* (UTSA) and the *Defend Trade Secrets Act* of 2016. Starting from quite divergent approaches to protection of confidential information in common law countries and varying trade secret theories of protection in civil law jurisdictions, there is now broad congruence in approach and a common recognition in advanced industrialised economies that statutory reform is necessary to protect creativity in the digital age. In Australia, the important role of the law of confidential information in protecting valuable business information should be better recognised and supported through:

- specification of circumstances in which access might be provided to consumers or others to 'slivers' of information from within the database; and

- statutory clarification that information which is not known to the public and which therefore has the necessary character of confidence may be shared between entities (for example, the various entities in an IoT supply chain) in circumstances where the information is protected against disclosure through verifiably reliable implementation of technical, operational and contractual safeguards without the database itself losing the necessary character of confidence that is required to continue to be protected as trade secret (confidential information).

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.

Our interest in the in the Commission's Inquiry

IoTAA's interest in the Commission's Inquiry arises because management of data handling and data analysis, and of data sharing between business entities, will be a core issue in provision of most of IoT (also known as the Internet of Everything) services. Data management is also critical in operation of IoT communications platforms and the sensor, communication, control and reporting devices used in IoT services. Diverse data capture, multiple data flows and substantial value-add by data analytics are at the essence of IoT services.

Hence IoTAA's interest in:

- rewarding value-added activities that utilise and value-add to data inputs, by development of intellectual property law, contract law and consumer protection law in a way that equitably balances protection to create economic incentives for further innovation, competitive market entry and consumer interests;

- ensuring that consumer welfare is enhanced while promoting a diversity of IoT services;

- promoting data quality and network and information security, reliability and trust;

- increasing the availability and range of public sector data that is released for value-adding applications and for research and experimentation;

- stimulating data sharing between businesses, and between businesses and consumers on terms, that are fair, transparent and understood; and

- facilitating Australian IoT services to reach global markets, by endeavouring to ensure that services developed from the Australian market can readily be offered in other markets, ideally operated, further developed and supported from Australia.

What is the IoT?

The IoT is the concept of gathering data from any number of sensors connected to the internet, analysing that data and acting on the information gleaned from that data. Sensors can come in many forms and can be used to sense a wide range of physical things. Physical sensors measure and enable reporting as to such characteristics as movement, temperature, moisture, altitude, salinity, presence or absence of particular chemical elements or compounds, characteristics and many other physical properties. Sensors may also interwork with social media tools such as Facebook, Twitter and Linkedin.

IoT devices include everything from vehicles, smartphones, thermostats, kettles, swimming pools, washing machines, headphones, lamps, wearable devices and so on – hence the alternative moniker for the IoT is *the Internet of Everything*. The IoT also refers to remote monitoring of components of machines, such as a jet engine of an airplane or an electricity network, and remote operation of machines, such as mining vehicles or undersea craft.

A key element of many IoT services is incorporation of sensor devices. These sensors may either be passive devices that monitor and report over the Internet as to conditions in a particular environment, or active (actuator) devices change conditions in that environment.

Frequently an IoT service will be machine-to-machine **(M2M)**, rather than human-to-machine. This absence of direct human involvement may lead to concerns as to awareness of affected individuals as to ongoing collection and 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, 'smart home' applications to turn on an air-conditioner, to turn off a pool filter or to order chemicals required to treat a swimming pool). Other applications may fully control and adjust to the conditions in a particular environment without any active consumer intervention (for example, smart home applications that respond to an extreme weather event by automatically activating sprinklers, closing curtains, turning off non-essential electrical appliances and turning on an air-conditioner that services a pet area).

IoT has been much hyped. IoT is probably near the peak of the now familiar technology hype cycle predicted by Gartner (*Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor*, 18 August 2015, www.gartner.com). That noted, a report released by Macquarie Equities in July 2016 and entitled *I Robot, Who can win from digital disruption*, identifies "four mega trends" that have the largest potential to disrupt the Australian corporate landscape over the next decade, being virtual reality, wearables, big data and IoT. Cisco Systems estimates that IoT will increase US corporate profits by 21 per cent in the next eight years, derived through reduced costs from higher asset utilisation, higher labour productivity, lower waste and improved supply chain logistics, new customers from improved product experiences and reducing the time to market for innovations. Macquarie Equities also suggest that due to the increasingly rapid business impact of technological change, the opportunity cost of businesses being slow to adopt technologies will rise exponentially.

There is no doubt that technological factors are converging to escalate the pace of IoT deployment. These factors include:

- as to sensors, rapid reductions in cost consumption coupled with improvements in capacity, durability, robustness and power efficiency;

- improvements in communications technologies between sensors and hubs and control devices, including 'meshed networks' and other improvements in bandwidth utilisation and reliability;

- improvements in encryption and other technologies to protect security of data both at rest and in transit;

- rapid uptake of smartphones, enabling near ubiquity of availability (subject to mobile network and wifi coverage) of a relatively low cost and globally standardised device which enables both insights to be delivered to users and the smartphone used as an actuator device. For example, many businesses such as logistics providers and couriers have swapped out proprietary terminals used to communicate between base and field providers for smartphone base applications which provide similar capabilities but at significant lesser cost and which also enable interworking with consumers and customers for real time reporting as to movement of items in transit;

- rollout of cloud based data warehouses and cloud based analytics platform services, enabling interconnectivity and low cost set-up and tear-down of data sources and analytics capabilities; and

- rollout of broadband and narrowband networks and IoT platforms and hub devices that support third party IoT services. Many low cost IoT smart home applications require access to an IoT hub device, such as a Google Nest device, provisioned by a third party such as a consumer. Smart city precincts require open data standards and interfaces that enable interworking of various proprietary networks such as building climate control systems, lift systems, street lighting, movement sensors and so on. Smart services to smart cars (other than those 'built-into' the car and proprietary to the manufacturer) require the make and model of smart car to present an open interface and to be smart enough. An agricultural IoT service delivering insights to a farmer's smartphone is of little value if the farmer does not have in-field mobile phone coverage, or if on-farm sensors cannot cope with the harsh Australian environment and also reliably communicate with each other.

Challenges of IoT

The opportunities afforded by IoT for the Australian economy come with risks and challenges, many novel and requiring development of new business models, law and new forms of contract.

Challenges

Often third party supplied devices will be integral to the service delivery chain. For example, a smart home application may communicate with service providers by means of the Google Nest platform as bought and installed by the consumer and with the householder by an app on the householder's smartphone or tablet. The variety of device and service options may lead to issues as to responsibility for failure in provision of a service caused by failure of third party supplied devices or communications platforms and carriage services.

Data errors or omissions or breakdowns may also lead to incorrect decisions being made by relying upon data analysis that is correctly conducted but using data that is adversely affected by data errors or outages. Because sensing may rely upon proper operation of third party devices and some operating issues will not be capable of remote detection, the reliability of IoT services may be adversely affected by data quality issues of which the IoT service provider is unaware, even if the IoT service provider exercises all reasonable diligence in real-time monitoring of service quality.

Clearly, data quality is important to ensure that IoT services provided using data are reliable and accurate. Many IoT applications will draw upon one or more external data sources to bring together various data inputs for analysis and outputs that either 'autonomously' make actuating decisions or that present a dashboard of analysed information that enables a human user to make an actionable decision. Making data available for diverse applications creates legitimate concerns as to legal liability for data sources, including public sector entities, that capture, curate or make available that data. Many data sources will be concerned that raw data may be incomplete, intermittently available or otherwise unreliable and accordingly unwilling to release that data without quality assurance.

Traditional forms of contracting have changed in the context of IoT-enabled devices which comprise multiple components and which are often provided by multiple suppliers in a rapidly expanding supply chain. Consumers often face myriad terms and conditions in numerous documents, usually on a website that may not be readily accessible. As such 'new forms of contract' may be appropriate and ACL interpretations may need to change: the definition of 'product' may need to expand; 'unfair contractual terms' may need to become tighter. Alternatively, acceptable model contracts may need to be constructed or other simpler ways to communicate disclosures to consumers may need to be devised.

Risks

Particular concerns arise where data may be used in applications that are beyond the contemplation of the data source: for example, where meteorological predictions are used to make machine-driven decisions as to climate control in factory farms. Similarly, providers of IoT communications platforms may be concerned that these platforms may be used for high availability, high risk exposure applications of which they are unaware. Concern as to legal exposure may impede government agencies or businesses from making decisions to release data for potential uses that are not controlled or managed by the data source. Concern as to exposure that may arise through data capture and availability may also impede prospective users of IoT services from making available their data for use in those services. For example, a farmer may be concerned as to the prospective use by environmental activists or environmental regulators of on-farm data that the farmer contributes to an IoT service, or by commodity brokers or traders to gain an informational advantage in price negotiations with the farmer.

Concerns as to data quality and potential legal liability arising out of reliance by IoT service providers or end users upon that data are particularly likely to impede release of data sets by government agencies. As mentioned above, many governments around the world have stated a commitment to release public data wherever practicable, implementing policy that public data should be a public good. However, open government data will be impeded unless liability exposures, as may arise from data quality issues or reliance by users, are appropriately assessed and mitigated. Many applications of government data may not be anticipated by the government agency that captures, curates or makes available that data. Uses often involve creative combination and comparison of multiple data sources by a data user that creates and manages an IoT service. Consider an agricultural IoT service that enables a farmer to make actionable decisions by means of a 'dashboard' report that provides analysed data outputs ('insights') on the farmer's smartphone. This service may combine data from field sensors measuring moisture content in soil and on plants, meteorological data provided by the Bureau of Meteorology, soil maps and river hydrological data from State agriculture agencies, and on-farm soil analyses by agronomy service providers, all mapped onto geo-spatial maps that combine public sector licensed geo-spatial data with third party corporate value-adds which enable annotations and other value-added features and functions. Failures or other errors in any of these data sets may compromise the information base and quality of analysed data outputs.

IoT providers will also need to consider the impact of privacy laws. Where activities of persons with access to data about individuals are not appropriately controlled through deployment of reliable contractual, operational and technical safeguards, release of data that has been de-identified but not fully anonymised (and which therefore remains vulnerable to concerted re-identification attack through combination of the data with other data) may lead to individuals becoming reasonably identifiable. In such cases any disclosure of this de-identified information could be classed as a release of personal information.

For businesses, there are additional risks. Many of these risks relate to a fundamental issue, being that currently in Australia and many other jurisdictions legal recognition and legal protection of proprietary rights in data is somewhat uncertain and may not be fully effective to enable appropriate control over downstream uses of data. More specifically, the still developing equitable doctrines as to protection of trade secrets or confidential information may not be adequate to protect sharing of 'commercial-in-confidence' data as required for many IoT services, particularly where an IoT service provider is not vertically integrated and relies upon other entities to provide some elements of an IoT service within the IoT service delivery chain.

Particular business risks include that:

- contractual protections as to uses and disclosures of data may not be enforceable against third parties (that is, persons that are not parties to the contract with the data source), particularly given the ability of service providers to move data to jurisdictions which have inadequate contract law systems and enforcement frameworks;

- limited or controlled release of data to facilitate research purposes or for experimentation may compromise entitlement of the data source to protection on the basis that this data is confidential (trade secret) information;

- loss of control of data may directly and adversely affect the business of the data source: for example, data may be used by competitors to more effectively target the data source's products, services or customers;

- IoT service delivery chains and inter-working of IoT services with IoT communications services and devices, particularly services and devices supplied or managed by third parties, may create security vulnerabilities and weak points at which data may be compromised or intercepted; and

- regulators or litigants may obtain access to the data for uses potentially adverse to the business.

While IoT services are becoming more complex and diverse, product lifecycles shortening and the number and range of participants in the IoT service delivery ecosystem increasing, businesses and consumers are demanding simpler forms of contract and more readily understandable operation of consumer protection laws. IoT businesses need predictable operation of intellectual property laws and competition regulation and availability of suitable radio communications spectrum for low powered devices in Australia and other markets that those businesses service.

Problems of legal protection of data and databases

Copyright

Copyright is a proprietary right affording the strongest legal protection to copyright works. For copyright to subsist in a work that falls within the categories described in Part III of the *Copyright Act 1968 (Cth)* (**Copyright Act**) – literary, dramatic, musical and artistic works – the work must be original. The concept of originality has long been regarded as closely correlated with the notion of authorship, which is central to the statutory protection conferred under the Copyright Act. However, as neither 'original' nor 'author' is defined in the Copyright Act, the meaning of the terms is only found in judicial decisions.

The traditional concept of authorship was based upon the creation of a work by an individual author or by two or more persons who collaboratively produce a jointly authored work in which the contribution of each author is not separable from that of the others. Further, the effort in creating the original work related to the creation of the work itself, and not the creation of the preconditions which enabled the work to be created.

These concepts have been challenged by the data driven economy in three fundamental ways.

First, a computer output is now often created by a computer executing a program where a human issues an instruction that causes the program to be run but does not himself or herself exercise any creativity in generating that computer output (a 'computer-generated' output). There is no human author in traditional terms.

Second, the human and financial effort in creating the program and establish the processing environment that enables another human to cause the computer to execute the instruction is protected through copyright protection of the program, but often not the data inputs or the data outputs from operation of that program (unless those outputs are arranged into a particular form of presentation, and then with copyright protracting that presentation but not the output data itself).

Third, the principal ongoing human effort has shifted to decisions as to data structure and formats and 'sweat' in data capture and cleansing preparatory to inputting transformation ready input data to the computing environment where the human instructs the computer program to execute to deliver the 'computer-generated' output.

It is in this context that the two principal Australian cases relevant to copyright in compilations and databases fell for consideration. These cases are the decision of the High Court of Australia in *IceTV Pty Ltd v Nine Network Australia Pty Ltd*[2] ***(IceTV)*** and the subsequent decision of the Full Federal Court in *Telstra Corporation Limited v Phone Directories Company Pty Ltd*[3] ***(Phone Directories)***. Prior to these cases many Australian lawyers interpreted the Australian cases as following a common law approach often referred to as the 'sweat of the brow' doctrine, under which the requirement of originality could be satisfied as a result of the application of skill, labour or judgment. For example, in 2002 in *Desktop Marketing Systems Pty Ltd v Telstra Corporation Ltd*[4], another case concerning telephone directories, Sackville J summarised the authority:

> "The course of authority in the United Kingdom and Australia recognises that originality in a factual compilation may lie in the labour and expense involved in collecting the information recorded in the work, as distinct from the 'creative' exercise of skill or judgment, or the application of intellectual effort."[5]

In *Data Access Corporation v Powerflex Services Pty Ltd*[6] the High Court of Australia held that a compression table in the plaintiff's Dataflex computer program, which had been produced with another computer program written by the plaintiff, was an original literary work protected by copyright. To create the Dataflex Huffman compression table, the plaintiff had first written a program that applied the Huffman algorithm to a database file which provided a representative sample of data for standard compressions. The High Court held that the Dataflex Huffman compression table was an original literary work produced by an author, stating:

> "The skill and judgment employed by Dataflex was perhaps more directed to writing the program setting out the Huffman algorithm and applying this program to a representative sample of data than to composing the bit strings in the Huffman table. Nevertheless, the standard Dataflex Huffman table emanates from Dataflex as a result of substantial skill and judgment. That being so ... the standard Dataflex Huffman table constituted an original literary work."[7]

These cases were regarded as supporting the relevance of labour, as contrasted to creative or intellectual input, to satisfying the originality test and further demonstrating the relevance of preparatory steps and intellectual effort in determining whether subsequent and related activity qualified for copyright protection.

---

[2] *IceTV Pty Ltd v Nine Network Australia Pty Ltd* (2009) 239 CLR 458; [2009] HCA 14

[3] *Telstra Corporation Limited v Phone Directories Company Pty Ltd* [2010] FCAFC 149

[4] 2002) 119 FCR 491

[5] At [407]

[6] [1999] HCA 49

[7] At [122]

In *IceTV* the High Court of Australia considered copyright in Channel Nine's Weekly Schedules of time and title of television programming. The Full Federal Court had been willing to take into account the skill and labour in the making of the programming decisions that were then reduced to the time and title and then that the time and title data was the "centrepiece" of the Weekly Schedules and so amounted to a substantial part of a copyright work. This reasoning was rejected in the High Court. French CJ, Crennan and Kiefel JJ found that there was insufficient originality in the arrangement of the time and title information for that to amount to a substantial part. Gummow, Hayne and Heydon JJ found that the originality of the Weekly Schedules lay in the selection and presentation of the time and title information together with additional program information and synopses as a composite whole. The preparatory work involved in producing the time and title information was not relevant to substantiality and accordingly there was left only "the extremely modest skill and labour" in setting down the programs already selected.

The *Phone Directories* case required the Full Federal Court to apply *IceTV* to the White Pages and Yellow Pages directories. The Full Court rejecting Telstra's submissions that "industrious collection" sufficed for originality.

As stated by Keane CJ:

> "The dicta in *IceTV* shift the focus of inquiry away from a concern with the protection of the interests of a party who has contributed labour and expense to the production of a work, to the 'particular form of expression' which is said to constitute an original literary work, and to the requirement of the Act 'that the work originates with an author or joint authors from some independent intellectual effort'."[8]

Information about the name and address of a particular telephone subscriber is merely factual in nature and is not an original creation of the person who takes a note of these details from the subscriber.[9] The form of the directories did not originate with the individuals who engaged the mechanical processes to produce the compilation.[10] As the White Pages and Yellow Pages were "not compiled by individuals but by the automated processes of the Genesis Computer System", they could not be considered as originating from an individual or group of individuals.[11] Copyright could not subsist in the directories because they were produced by a "computerised process of storing, selecting, ordering and arranging the data to produce the directories in the form in which they were published".[12] Yates J reached the same conclusion but was willing to accept that the Genesis system was transformative of the data and not a "mere tool utilised by employees" for the purpose of selection, ordering and arrangement of information to produce each compilation in the White Pages and Yellow Pages.[13] The activities carried out by the Genesis system would have amounted to authorship if carried out by humans, but in this case they were not the activities of human authors for copyright purposes.[14]

In summary, the requirement for relevant human intellectual effort in determining the specific form of transformation of the data, as distinct from instructing a program to execute a routine and predetermined transformation routine, appears relatively well settled on the current state of Australian copyright law. However, the required level of human intellectual effort or

[8] 2010] FCAFC 149 at [58] citing *Walter v Lane* [1900] AC 539 at 554 and *Sands & McDougall Proprietary Limited v Robinson* [1917] HCA 14; (1917) 23 CLR 49 at 54-55

[9] Keane CJ at [59]

[10] Keane CJ at [59]

[11] Keane CJ at [89] and [90]

[12] Keane CJ at [7] and at [96]

[13] Yates J at [166]-[167]

[14] Yates J at [166]-[167]

creativity should not be overstated. In a recent March 2016 Full Federal Court decision in *JR Consulting & Drafting Pty Limited v Cummings* [2016] FCAFC 20, the Court stated:

> "It may be that the observations in *IceTV* concerning the statutory conception of authorial contribution sufficient to render a work "original" under the Act, have the effect of "raising the bar" on the threshold skill, labour and judgement an author must contribute so as to render a work an original work. However, it should be remembered that French CJ, Crennan and Kiefel JJ affirmed the orthodoxy of the early formulation of Isaacs J; noted that "too much" has been made in the context of subsistence of the kind of skill and labour which must be expended; and noted that the requirement of the Act is "only" that the work "originates" with an author (or joint authors) from "some independent intellectual effort", a view consistent with the observations of Gleeson CJ, McHugh, Gummow and Hayne JJ in *Data Access v Powerflex*."[15]

In summary, under current Australian copyright law electronic data of itself is no more than a collection of information. It is the selection, structure and organisation of electronic data into a database that may qualify for copyright protection. The underlying data as accessible through that database generally remains unprotected by copyright although the same information as selected, structured or organised in a database may well be protected by copyright (subject to finding human authors and originality). What is being recognised and protected as a copyright work is the fruit of intellectual endeavour of humans in selecting, structuring or organising data/information into a database and not the underlying data.

In these circumstances, Australia's intellectual property regime is not currently suited to protecting database rights, which are of both intellectual and commercial value to Australian businesses, and of (significant) interest to those who misappropriate the information they contain for nefarious purposes. Further, whilst the developing law of confidential information (**CI**) go some way to addressing protection concerns for database owners, this judge-made law as it stands fails to adequately address broader issues such as incentives to invest in, create and develop new (database) technologies, including storage, access and dissemination technologies. There is a role for government to review CI laws, in conjunction with sui generis protections and incentives to adequately protect database rights, rights related to the development of new (digital) technologies, and to encourage future digital research and development.

Confidential Information

Australian law confers rights on legal entities and in relation to 'property'. 'Property' is legally recognised subject matter of rights of legal entities. Of course, legal entities have many other valuable rights that are not rights 'in and to property' as traditionally understood. Most relevantly, equitable doctrines in relation to confidential information have been developed to protect information as commercially valuable and confidential (trade secret) but which information does not fall within accepted species of property. (Noting, however, that theses doctrines may equally be applied to subject matter that is 'property', the key point being that the right is created regardless of whether the subject matter protected by that right is property or not.) So we now talk about trade secret information being 'protected' by 'the law of confidential information' within the class of 'intellectual property', when in fact:

- there is no such law (instead there are equitable doctrines 'fastening on the conscience of the wrongdoer');
- the subject matter may or may not be property; and

[15] [2016] FCAFC 20 at [285]

- the protection is not of the subject matter itself, but rather against the inequity of the wrongdoer deriving any benefit or advantage from that that they knew or should have known that they should not have.

In other words, 'property' is used in Australian law in various ways to describe a range of legal and equitable estates and interests, corporeal and incorporeal. As Gummow J stated in *Yanner v Eaton*:

> "Equity brings particular sophistications to the subject. The degree of protection afforded by equity to confidential information makes it appropriate to describe it as having a proprietary character, but that is not because property is the basis upon which protection is given; rather this is because of the effect of that protection."[16]

A database to be protectable as confidential information must have the necessary quality of confidence. This involves objective and subjective elements. A subjective element is whether preservation of the confidentiality of the information is of substantial concern to the plaintiff. This can be established to adducing evidence demonstrating efforts that courts of equity expect a plaintiff to have taken to preserve the confidentiality of the information that the plaintiff claims is a valuable trade secret. An objective element is that the information must be of a kind that warrants protection. If data has become part of the public domain, as a result the data is not confidential to the plaintiff and is not a secret, however much the plaintiff considers this data to be valuable and confidential. However, some parts of the secret may be in the public domain, and data or information may have circulation within a controlled and limited section of the public under conditions as to confidentiality and retain a commercial-in-confidence character. A trade secret may be as to the way that parts are structured, aggregated, combined or used, or of the aggregation itself. So an accessible database may be protected if the access is controlled and limited such that the combined accesses do not have the character of making the database broadly available.

The important role of the law of confidential information in protecting valuable business information should be better recognised and supported through:

- specification of circumstances in which access might be provided to consumers or others to 'slivers' of information from within the database; and

- information that is not known to the public and which therefore has the necessary character of confidence may be shared between entities (for example, the various entities in an IoT supply chain) in circumstances where the information is protected against disclosure through verifiably reliable implementation of technical, operational and contractual safeguards;

without the database itself losing the necessary character of confidence that is required to continue to be protected as trade secret under the law of confidential information.

We trust that these comments are of assistance to the Productivity Commission in its further consideration of this reference.

[16] *Yanner v Eaton* (1999) 201 CLR 351, 388–9.

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