GOOD DATA PRACTICE:

A GUIDE FOR BUSINESS TO CONSUMER INTERNET OF THINGS SERVICES FOR AUSTRALIA

Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia V1.0 November 2017

This Guide was developed by Workstream 3: Data Use, Access and Privacy of the IoT Alliance Australia (IoTAA) – http://www.iot.org.au/

Disclaimers

1) Notwithstanding anything contained in this Guide:

a) Internet of Things Alliance Australia (IoTAA) disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for any direct or indirect loss, damage, claim or liability any person may incur as a result of any:

i) reliance on or compliance with this Guide;

ii) inaccuracy or inappropriateness of this Guide; or

iii) inconsistency of this Guide with any law; and

b) IoTAA disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for ensuring compliance by any person with this Guide.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

TABLE OF CONTENTS

Introductory statement

The IoTAA publishes this Good Data Practice Guide to promote industry and consumer awareness as to good practice in dealing with data associated with provision of business to consumer (B2C) IoT services. Examples of B2C IoT services include applications for connected car, smart homes, wearable technology, quantified self, connected health, and 'smart appliances' that use Wi-Fi for remote monitoring or control such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators.

The IoTAA promotes consumer and industry awareness about good business practice in provision of IoT services and IoT devices to consumers. By building that awareness, we aim to assist both businesses and consumers to anticipate and address possible concerns before they occur. This Guide focusses upon measures that IoT providers can take to build trust and understanding amongst consumers about collection and uses of data in the course of provision of operation of IoT devices and provision of IoT services, protection of privacy and secure installation and operation of IoT devices.

This Guide is drafted principally to assist providers of IoT B2C devices and services to design fair and appropriate features and settings for privacy, security and accessibility into their products and services and to make available appropriate and readily understood guidance for consumers about their use. This Guide is also intended to assist the IoTAA and consumer organisations in developing general guidance for consumers about privacy protection and secure implementation and use of IoT devices and services.

This Guide supplements existing privacy and consumer laws. We try not to restate protections provided by those laws. Instead, we focus upon key practical ways in which providers of IoT B2C devices and services may implement good data handling practices and may assist consumers to understand and use IoT devices and services.

The IoTAA suggests that the principles for good data practices set out in the Guide are of general application in relation to IoT services and IoT devices regardless of industry sector or particular IoT application. We note that there are other initiatives underway within the workstreams of the IoTAA, and elsewhere in Australia and comparable jurisdictions, to formulate principles, guidelines or industry codes as to good IoT business practice for particular industry sectors and for specific IoT applications. We encourage these initiatives. We also support ongoing efforts to develop Australian and international standards that facilitate information security, interoperability of IoT devices and services, and consumer choice.

IoT services and devices are rapidly evolving. It is likely that this Guide will be a living document and adapt to address concerns as they emerge. We welcome ongoing input as we continue to develop this Guide.

Many individuals in the IoTAA, and in particular in IoTAA Workstream 3: Data Use, Access and Privacy, have contributed to the development of this Guide. We gratefully acknowledge their respective contributions. We also acknowledge the ongoing support given by employers of those individuals, including businesses, government agencies, consumer organisations and not-for-profits that facilitate those individuals' participation in the IoTAA. We also acknowledge valuable comments by other agencies and organisations. Of course, although this Guide represents the collective input and effort of many individuals within the IoTAA, the Guide does not reflect the views of any organisation or agency supporting the IoTAA, or particular individuals participating in IoTAA initiatives.

Peter Leonard
Chairman, Workstream 3: Data Use, Access and Privacy and Principal, Data Synergies

1. OBJECTIVES OF THIS GUIDE

The objectives of this Guide are to promote:

- take-up and acceptance by Australian consumers as purchasers and users of IoT services and devices, by promoting adoption of good industry practices by providers of IoT services and devices; and

- global expansion of Australian based IoT businesses, by stating principles which may be consistently applied in provision of IoT services to consumers in other countries, including in jurisdictions which do not provide an equivalent standard of consumer protection or information privacy as in Australia (while also noting that some jurisdictions may have additional or different requirements to the principles stated in this Guide).

This Guide seeks to achieve these objectives by:

- facilitating trust, by promoting mutual understanding between providers and consumers about the collection, handling, disclosure and security of personal information and other consumer data;

- facilitating a common understanding of good business practices for B2C IoT services and devices, including through stating principles for fair information handling and 'plain English' language for consumer-appropriate customer terms and notices, consumer disclosures and consents;

- promoting simplicity and clarity in terms of use, enabling consumers to better compare terms for provision of particular IoT services and devices;

- assisting service providers to ensure that consumers understand expectations that providers place upon them when consumers set up and use IoT services and devices, including by following good information security practices, by addressing implementation risks and by promoting disclosures by customers who implement an IoT service or device to other individuals that may be affected by use of that IoT service or device;

- stating good practice principles for handling data flows by various IoT service participants associated with provision of IoT services and devices. Many IoT services involve three or more entities in provision of an IoT service to an end user, with relevant data flows required between those entities. The data flows between participants are sometimes referred to as 'data ecosystems'. These good practice principles seek to facilitate a better understanding between participants in those data ecosystems as to the rights and expectations of consumers, participants and affected individuals;

- stating good practice principles as to disclosure to consumers on the potential provision of information derived from IoT services to law enforcement agencies, environmental and other relevant regulators, and insurers, loss adjusters or other third parties, so that IoT users (consumers and affected individuals) are aware of relevant obligations of IoT service providers.

2. HOW WE USE SOME TERMS AND ABOUT THE OPERATION OF THIS GUIDE

Terms

There is a confusing range of terms used about the Internet of Things. To simplify this Guide, we set out below how we use some words and phrases.

The **IoT** is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Each '**thing**' is uniquely identifiable through its embedded computing system, and may work within an IoT specific communications network, but also connects to and is able to interoperate within the existing Internet. 'Things', in the IoT sense, can refer to a wide variety of **IoT Devices**, including:

- familiar devices that become '**smart**' through being internet enabled with sensor or actuator devices,
- specialist collector devices such as drones and climate sensors, and smartphones, personal wellness devices and smart watches that collect and report sensed data and enable a user to actuate other IoT devices, and
- **virtual assistants** such as Cortana, Siri, Google Home and Alexa.

B2C IoT Services are services provided by business to consumer that enable use of an IoT Device to be controlled by a consumer or by a service provider on behalf of the consumer acquiring the service.

IoT Platforms are specialist IoT Devices and associated platform services that enable communication between a user, the Internet and other IoT Devices, but which are not the B2C IoT Service that the consumer acquires to control and use IoT Devices. An example of an IoT Platform is Google Nest smart home platform, which enables interconnectivity between a consumer and a variety of B2C IoT Devices (e.g. smart thermostats, security systems and baby monitors).

A provider of an IoT Service or IoT Device may or may not be an 'APP entity' regulated under the Privacy Act 1988 (C'th), including the Australian Privacy Principles (**APPs**), or an entity regulated under other relevant Australian laws (including State and Territory information privacy, information security, tracking and surveillance devices laws). We refer to these privacy related laws together as (**Australian**) **Privacy Laws.**

We refer to laws conferring protections and rights upon consumers in relation to products and services that they acquire or use as **Australian Consumer Laws**, so we do not limit use of that term to the Australian Consumer Law which forms part of the Competition and Consumer Act 2010 (C'th) and the fair trading laws in States and Territories.

We use the term **Provider(s)** in this Guide to refer to the broad class of providers in Australia of IoT Services (and their sub-contractors, such as data warehouses and data analytics service providers), and providers of IoT Devices, regardless of whether the relevant provider is regulated by Australian Privacy Laws.

In this Guide, a consumer contracting directly with a Provider for the provision of an IoT Service is referred to as a **Customer**.

As this Guide applies to a broader class of affected individuals and users than Customers, this Guide uses the term **Affected Individuals** to refer to persons within that broader class. The term 'Affected Individuals' includes (for example) end-users of IoT Services and IoT Devices that are permitted to use, or be observed by, an IoT Service or IoT Device that is implemented by a Customer who contracts with a relevant Provider.

This Guide is intended to apply in relation to collection and handling in Australia by a Provider of:

a) any information about Affected Individuals who are reasonably identifiable (being 'personal information' as regulated under Australian Privacy Laws), and

b) other information about Affected Individuals who are not reasonably identifiable but where the information might reasonably be regarded by Affected Individuals as 'private' because this information is domestic or confidential in nature.

As this Guide is intended to apply to a broader class of information than personal information as regulated under Australian Privacy Laws, we use the term **Relevant Information** in this Guide to refer to information within that broader class (both paragraphs (a) and (b) above).

We use the term **IoT Partners** to refer to entities that a Provider works with in order to provide an IoT Service to a Customer, but which does not directly deal with the Customer in relation to that IoT Service. Such partners in a Provider's data eco-system may include providers of data warehouses and cloud platforms, data analytics service providers, billing and carriage service providers, mobile app developers and app providers and providers of IoT sensor devices.

Operation of this Guide

This Guide does not, in any way, reduce each Provider's obligations to consumers under the Australian Consumer Law, Australian Privacy Laws and other laws and mandatory codes.

We suggest that it is good practice for Providers that are not APP entities to commit nonetheless to consumers to comply with Australian Privacy Laws, including the APPs, in relation to the provision of IoT services to consumers.

We also suggest that it is good practice for Providers to apply the principles in this Guide to provision of an IoT Service that is delivered by a Provider to consumers outside Australia where Providers collect or hold Relevant Information in Australia, regardless of where relevant consumers reside or use the IoT Service.

3. GOOD DATA PRACTICE PRINCIPLES

1. APPs and Consumer Protection Benchmark Principle

As a matter of law, each Provider must comply with:

(a) Australian Privacy Laws;

(b) Australian Consumer Laws; and

(c) other industry sector or application specific laws and codes that have mandatory operation in relation to that Provider.

It is noted that the APPs include requirements as to collection, handling and other use, disclosure (including outside Australia), retention and deletion or de-identification of personal information.

A Provider of IoT Services and IoT Devices should ensure that the Provider's terms of service, and other Provider originated statements and materials, do not imply in any way that those terms and other statements and materials, or the principles in this Guide, override or exclude the operation of Australian Privacy Laws and Australian Consumer Laws.

2. Accountability Principle

A Provider should exercise end-to-end accountability in relation to all flows of Relevant Information associated with provision of its IoT Service, including flows between the Provider and the Provider's IoT Partners.

A Provider should take such steps as are reasonable in the circumstances to ensure that its IoT Partners comply with this Guide. It will usually be reasonable in the circumstances for a Provider to ensure that its IoT Partners comply with this Guide where the Provider is reasonably able to direct and restrict the way in which Relevant Information is used, otherwise handled or disclosed, by an IoT Partner. In other words, in circumstances where Relevant Information remains within the effective control of the Provider.

For example, if an IoT Service is provided by means of a telecommunications carriage service provided by an unrelated telecommunications carriage service provider, or an IoT platform device provided by an unrelated device supplier, the Provider should be accountable in relation to acts and practices of that intermediary to the extent only that the Provider is reasonably able to direct and restrict the way in which that intermediary uses, handles or discloses that Relevant Information (whether that control is through a direct contract with that IoT Provider or otherwise practically able to be exercised).

Often, however, the Provider will either not be in a relevant contractual relationship with the intermediary (for example, where the Customer buys, installs and operates the IoT Platform device), or will be a taker of standard contract terms that are prescribed by a third party and not reasonably able to be negotiated (for example, some public cloud applications). In such circumstances, a Provider should take such reasonable steps to make the IoT Partner aware of and encourage the IoT Partner's compliance with this Guide, in order to facilitate and support good customer engagement and trust in the IoT Service.

Accountability encompasses a Provider:

a) making available information to Customers in a 'plain English', easy to read form;

b) applying Privacy by Design (**PbD**) and Security by Design (**SbD**) principles to handling Relevant Information (and not only 'personal information' within the meaning of the Privacy Act 1988 (C'th));

c) designing and specifying IoT Devices and IoT Services and associated customer support to take into account the needs of persons of limited capabilities or understanding, to build accessibility features into those products, and to accommodate alternative forms of interaction with those products, services and

customer support. Providers should broaden the range of consumers that can use IoT Devices and IoT Services safely, securely and autonomously to the extent reasonably and commercially practicable. This design principle is now frequently referred to as **Accessibility by Design**. Anticipating and addressing needs or requirements of consumers with disabilities or otherwise limited capabilities to use IoT devices delivers clear benefits for our society and is also likely to improve reach and take-up of services. Often relatively minor changes made during the design and specification phase will enable IoT Devices and IoT Services to be accessible by a broader cross-section of consumers. There are now useful and readily available materials available to Providers as to accessibility by design;

d) carrying out privacy impact assessments (**PIAs**) where necessary and desirable to do so, in order to assess the privacy impacts of a new IoT Service or Device or changes to an IoT Service or IoT Device, and to identify ways in which obligations under Australian Privacy Laws can be met and an IoT Service or an IoT Device supplied in accordance with the Principles in this Guide;

e) taking such steps as are reasonable in the circumstances to inform Affected Individuals as to any use, disclosure or handling of Relevant Information that is not likely to be within the reasonable expectations of Affected Individuals (noting, however, that the Provider will often not be in a position to ascertain Affected Individuals, or be able to directly inform them as to a relevant use, disclosure or handling of Relevant Information, and may therefore need to request the Customer to do so);

f) in addition to complying with Australian Privacy Laws, Australian Consumer Laws and any industry sector or application specific laws, taking such steps as are reasonable in the circumstances to inform Customers of an IoT Service as to:

    i. a Provider's reasonable expectations about good implementation of an IoT Device and an IoT Service, about device handling, device maintenance and data security and information handling practices that may reasonably be implemented by Customers, including to address and mitigate any known or anticipated vulnerabilities. Relevant information may include how to make appropriate security settings and recommendations as to notifications by the Customer to other Affected Individuals, etc. (as further discussed in the Consumer Empowerment Principle below);
    ii. any other vulnerabilities to continuing provision, quality or reliability of an IoT Device or an IoT Service that a Customer of the IoT Service or an Affected User might not reasonably anticipate and which are outside the reasonable control of the Provider. Examples of possible vulnerabilities include failure of power supply to a sensor device, unavailability of relevant data from a third party data source, unreliability of data, failure of an IoT platform device, mobile apps being turned off or not updated, any need for another app to be enabled, or for a smartphone to be on, for alerts to be received, and so on;

g) implementing reasonable steps to protect security of Relevant Information (including internal unauthorised access, improper use by sub-contractors and from external intrusions);

h) implementing processes and procedures for handling consumer complaints about IoT Services and IoT Devices, and guidance about those processes and procedures that can readily be understood by Customers. IoT Services are inherently complex and will be unfamiliar to many Customers. Customers may not readily understand the IoT supply chain or which entity should be responsible for which IoT device or service in the IoT supply chain. Providers should take reasonable steps to assist Customers to understand how their IoT Service fits in the IoT supply chain, and the appropriate scope of responsibility of the Provider in addressing complaints and concerns of Customers. In developing processes, procedures and guidance, Providers should have regard to good practice guides for handling consumer complaints in Australia, including the Communications Alliance Telecommunications Consumer Protections

(TCP) Code (which will have mandatory operation for Providers that are relevant telecommunications service providers) and Australian/New Zealand Standard AS/NZS 10002:2014, Guidelines for complaint management in organisations.

3. Customer Empowerment Principle

The Accountability Principle as outlined above addresses key responsibilities of a Provider in relation to an IoT Service or an IoT Device provided to Customers.

A Provider should not unfairly or unreasonably shift these responsibilities to Customers.

However, many aspects of provision of an IoT Service, and safe and secure use of an IoT Service by a Customer and any other Affected Individual, are outside the reasonable control of a Provider. Where a Provider reasonably and fairly expects a Customer to accept key responsibilities and to the extent that a Provider reasonably can, a Provider should ensure Customers understand these responsibilities, and are empowered to exercise them.

In determining the fairness of any allocation of responsibilities, it is reasonable to have regard to whether responsibilities placed upon Customers could reasonably have been addressed by the Provider in its standard offer of an IoT Service through implementation of such Privacy by Design (PbD) and Security by Design (SbD) architectures, processes and settings reasonable when the IoT Service was provided or last substantially upgraded or modified, having regard to the pricing for the IoT Service, then-known vulnerabilities and the general capabilities of IoT Devices and IoT Services at that time.

For example, Customers will often be responsible for:

a) set up of an IoT Service and IoT Devices, including configuration of appropriate security settings;

b) providing access to the Internet of an IoT Service, by configuration of appropriate security settings;

c) monitoring the safekeeping and operating environment of an IoT Device;

d) ensuring availability of reliable power supply or other external requirements to ensure that IoT Devices operate in accordance with their specifications; and

e) installing patches and updates.

As per the Accountability Principle, a Provider should take such steps as are reasonable in the circumstances to inform Customers as to good IoT Device handling, maintenance and data security and information handling practices that the Provider reasonably expects the Customer to implement. Such steps and practices may include (by way of examples) addressing and mitigating any known or anticipated vulnerabilities, recommendations as to security settings and recommendations as to notifications by the Customer to other Affected Individuals.

A Provider should ensure that any statement as to responsibilities of a Customer is in 'plain English', in a form that is reasonably prominent and transparent, and which empowers a Customer to make a sensible and properly informed decision as to safe set-up, safe use and reliable operation of an IoT Service or an IoT Device.

4. Cyber Protection Principle

A Provider should implement security by design in all IoT Devices and IoT Services.

A Provider should make it as easy as is reasonably practicable (having regard to the nature of the IoT Service or IoT Device and its price point) for Customers to:

a) understand the Customer's responsibilities in relation to security settings and updates;

b) implement security patches and updates; and

c) understand what security vulnerabilities will remain and how best to address these vulnerabilities (including through monitoring or implementation of third party security products).

A Provider should ensure that its IoT Partners develop and adopt appropriate security processes and practices, including:

a) taking appropriate measures to ensure the protection of consumer data from attack during storage and transmission;

b) ensuring, wherever possible, that over the lifecycle of products and services regular security updates are made available, but also recognising that many devices will operate without prompt installation of updates and therefore be vulnerable;

c) where reasonable and appropriate, deploying new software and hardware technologies relating to authentication, identification, and data access controls;

d) compliance with regulatory, product and service security certification requirements; and

e) development and implementation of strategies to preserve security and to limit reasonably anticipated loss or damage when data breaches or data corruption have occurred.

5. Customer Data Transparency Principle

A Provider should:

a) implement good information handling practices that meet reasonable expectations of consumers as to full and fair disclosure as to collection and uses of Relevant Information;

b) ensure that information is provided to consumers as to collection, uses and disclosures of Relevant Information; and

c) ensure that information provided to consumers is in 'plain English' and 'customer friendly' form, or as it is sometimes referred to, sufficiently 'transparent'. Information should be fairly disclosed with sufficient prominence (easy-to-find) and easy-to-understand (that is, provided in a way that makes it reasonably likely to be understood by a person of reasonable, but below average, literacy).

6. Data Minimisation Principle

Collection and handling of Relevant Information (including data flows between a Provider and the Provider's IoT Partners) should be minimised by a Provider to those collection and handling practices:

a) necessary for operation of an IoT Device provision of the IoT Service;

b) expressly permitted in relation to handling of personal information by relevant applicable privacy laws (including Australian Privacy Laws); and

c) expressly and transparently disclosed to the relevant Customer acquiring the IoT Device or IoT Service.

To the extent reasonably practicable:

a) Relevant Information should not be handled in identifying form but should be de-identified through the use of reliable and verifiable de-identification process and practices that are accepted as good industry practice;

b) de-identified information that is not fully anonymised (whether through aggregation or otherwise) should be handled in accordance with reliable and verifiable technical, operational, legal or other safeguards or controls reasonably required to ensure such information remains effectively, reliably and verifiably de-identified. The

appropriateness and likely effectiveness of such safeguards and controls should be evaluated applying data risk assessment and mitigation practices that are generally accepted as good industry practice;

c) de-identified information that is not fully anonymised (whether through aggregation or otherwise) should not be made available to any entity that might reasonably be anticipated as able to re-identify an individual, whether from the information itself or from combination with any other information that might reasonably be available to that entity.

However, and subject always to Australian Privacy Laws and Australian Consumer Laws, special arrangements may be applied in relation to appropriately controlled disclosures and uses of Relevant Information for research conducted under appropriately controlled conditions by accredited research organisations, in accordance with data risk assessment and mitigation practices generally accepted as good industry practice from time to time.

7. Customer Data Control Principle

A Provider should take reasonable steps (for example, in the relevant terms of service or privacy statement or privacy notice to Customers) to inform consumers as to rights of access to Relevant Information.

Limitations as to portability of Relevant Information should be clearly stated. To the extent reasonably practicable (having regard to the nature of the IoT Service or IoT Device and its price point), Customers should not be unduly impeded in exercising choice and in exercising an ability to switch between multiple providers of products and services.

Allocation of rights of confidentiality and any other intellectual property rights or proprietary rights (including ownership, where such rights arise) of data, including Relevant Information, may reasonably be specified in terms of service for a particular IoT Service. However, such allocation should be expressed in terms that comply with the Customer Data Transparency Principle above. In particular, provisions as to ownership of data should not confuse or undermine clarity as to rights of access by Customers and Affected Individuals to Relevant Information about them collected during provision of an IoT Service.

Customers should be properly informed in accordance with Australian Privacy Laws, Australian Consumer Laws and good transparency practice as to possible uses and disclosures that may be made of Relevant Information that would not reasonably be anticipated by Customers, such as disclosures to insurers and loss adjusters.

To the extent reasonably practicable, and having regard to the desirability of keeping terms of service and other statements and notices to Customers as straightforward as reasonably practicable, Customers should be informed by a Provider in general terms about potential provision of Relevant Information derived from an IoT Service or an IoT Device to law enforcement agencies, environmental authorities and other relevant regulators, so that IoT users are aware of such obligations on IoT Providers and any negative externalities that may flow from availability and use of Relevant Information.

Where information as handled by a Provider or its IoT Partners ceases to be Relevant Information through appropriate de-identification, but is then provided to a third party (for example, a law enforcement agency) that may reasonably be anticipated to have the capability to re-identify an individual that is an Affected Individual, this information should be regarded as Relevant Information for that disclosure.

Any disclosure of Relevant Information should only be made by a Provider to the extent that a Provider considers that the disclosure is required, authorised or otherwise mandated by law (e.g. court subpoena or other legal compulsion) or is otherwise expressly permitted by operation of the relevant terms of service or other statement or notice to Customers.

A Provider should maintain a log of disclosures of Relevant Information as required, authorised or otherwise mandated by law and conform with good transparency reporting practices as to such disclosures.

4. BACKGROUND

The intended audience for this Guide

Communications to consumers as to matters within the subject matter of this Guide will need to be succinct and readily understood.

This Guide is not intended to be the communication(s) to consumers that must be an essential part of implementation of this Guide. This Guide is a statement of expectations as to developing good industry practice in design and implementation of B2C IoT services and IoT devices, in sufficient detail to be of practical use by individual IoT service providers and consumer advocacy organisations.

What are IoT services and IoT devices?

The IoT is the infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

IoT devices include everything from connected vehicles, smartphones, thermostats, kettles, swimming pools, washing machines, headphones, lamps, wearable devices and so on.

There are many different types of IoT applications and services, but a key element of many IoT services is incorporation of sensor devices. These sensors may be passive devices that monitor and report over the Internet as to conditions in an environment, or active (actuator) devices that change conditions in that environment.

Some IoT consumer applications provide consumers with information that enables the consumer to make actionable decisions based upon the analysed information. For example, 'smart home' applications may turn on an air-conditioner, turn off a pool filter, or autonomously order pool chemicals when the dispenser runs out.

Other applications may fully control and self-adjust in response to changes in an environment without any active consumer intervention. For example, smart home applications 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.

Increasingly over time, IoT services will be machine-to-machine, rather than human-to-machine. Absence of direct human intervention may lead to concerns as to awareness of affected individuals in relation to ongoing collection and handling of personal information about them during provision of such services. This may particularly be the case where the affected individual is not directly involved in ordering or commissioning installation of the IoT service. For example, an IoT security monitoring application installed in a rental apartment may have been commissioned by the landlord, and the tenant and any invitee to the apartment may be unaware of the terms of provision of the IoT security service and any collection and handling of information about them enabled by that application.

IoT services and other data driven services

All new B2C data driven services raise concerns about consumer protection and uses of data about consumers. Some key concerns about IoT services are shared with social networking services, search engines, sharing economy services and price comparison services.

However, relevant characteristics of many B2C IoT services raise novel consumer concerns. These characteristics include:

- **multiple parties and separation of parties**: Often IoT services will be purchased by consumers separately from IoT platforms and sensor devices. Often these services will be set-up by consumers themselves, using separately acquired reporting or actuation devices and smartphones and mobile apps. Some consumers may not understand how to make appropriate data and security settings to reduce security vulnerabilities

and other risks. This Guide suggests how consumers may be assisted to make appropriate data and security settings.

B2C IoT services often will be implemented in homes or other shared use environments where an activity that is monitored or reported on using an IoT device is an activity of a person (an **affected individual**) who is other than the consumer purchasing the IoT device or IoT service. This leads to concerns as to whether affected individuals will know about collection and use of information about their activities.

On the provider side, data will often pass through multiple parties (e.g. the service provider and its sub-contractors such as cloud platform service providers, data warehouses and billing service providers) working together in a 'data ecosystem' to provide the full features and functionality of a service. This supply-side characteristic creates a need for a Provider to manage IoT data partners to ensure that end-to-end provision of an IoT service addresses confidentiality, privacy and information security vulnerabilities. Steps to address these vulnerabilities include good data privacy and security by design, minimisation of data flows associated with IoT services and IoT devices, and transparency as to collection, uses and disclosures of consumer data.

- **reach:** Many B2C IoT services reach into homes and other domestic, sometimes intimate environments, and enable observations and inferences as to private behaviour that otherwise are not possible. Even where collected data may not be demonstrably about an identifiable individual (and therefore its use and collection regulated by privacy law), there will be reasonable expectations of some consumers as to full and fair disclosure as to collection and uses of data about their activities.

  The Guide seeks to encourage good data handling practices regardless of whether the relevant data is regulated by privacy law. We set out principles for good information handling practices to meet reasonable expectations of consumers as to full and fair disclosure as to collection, uses and disclosures of data about activities of consumers and to ensure that information provided to consumers is easily understood.

- **undue reliance upon consumers to understand and mitigate risks**: Consumers may place undue reliance upon reliability and availability of an IoT service. Consumers may also not be aware of the extent to which reliability and availability of the service may be affected by factors outside the IoT service provider's control.

  IoT service providers may assume that consumers will anticipate, monitor and mitigate risks. A provider may expect that consumers are making appropriate security and privacy settings, updating software with security patches, and ensuring that devices are appropriately located and monitored. However, consumers may not understand that these matters are their responsibility or how to do these things.

  This Guide is intended to assist IoT service providers and IoT device providers in achieving an appropriate and reasonable allocation of risk and responsibility between provider and consumer, including through ensuring that communications with consumers about risks, and responsibilities for mitigation of risks, are appropriately easy to read.

- **IoT security concerns**: Standards, protocols and protections as to IoT device security are still developing.

  In this early stage of rollout of IoT services and development of security standards, poor security by design, poor implementation, poor coordination or misunderstanding as to respective responsibilities of provider and user, may lead to unacceptable security vulnerabilities.

Interaction of this Guide with Australian Privacy Laws and Australian Consumer Laws

This Guide supplements Australian Privacy Laws and Australian Consumer Laws.

Nothing in this Guide is intended to create any new legally binding commitments or to be advice about legal requirements. This Guide does not operate in any way other than in line with and subject to Privacy Laws and Consumer Laws in effect from time to time. All Principles set out in this Guide are to be interpreted as operating in addition to, and always subject to, Privacy Laws and Consumer Laws. Privacy Laws and Consumer Laws will operate together with and unaffected by this Guide.

This Guide is not intended to apply to Relevant Information that has been reliably and verifiably de-identified (including in accordance with relevant de-identification guidance from the Australian Privacy Commissioner), whether through aggregation or data de-identification practices that are accepted as good industry practice from time to time, but only for so long as:

a) any technical, operational, legal or other safeguards or controls reasonably required to ensure such information remains effectively, reliably and verifiably de-identified are applied in accordance with data risk assessment and mitigation practices accepted as good industry practice from time to time;

b) this de-identified information is not made available to any entity that might reasonably be anticipated as able to re-identify an individual, whether from the information itself or from combination with any other information that might reasonably be available to that entity;

c) a Provider implements good information handling practices that meet reasonable expectations of consumers as to full and fair disclosure as to collection and uses of consumer data; and

d) a Provider ensures that clear and understandable information is provided to consumers as to collection, uses and disclosures of consumer data.

How does this Guide fit together with standards, codes and other guides?

There are many initiatives underway in Australia, and in comparable jurisdictions, to formulate principles, guidelines or industry codes as to good industry practice in provision of various types of IoT and other data driven services. Initiatives include industry self-regulation schemes for business applications of data analytics and application specific statements of principles. There have been recent initiatives in comparable jurisdictions addressing IoT related services as diverse as agricultural IoT services, offer of telematic car insurance and personal assistant IoT services that record human speech.

This Guide does not address particular IoT applications, instead taking a more general, economy-wide approach. Particular sectors (e.g. smart cities street infrastructure, smart buildings, agriculture) and applications (e.g. personal health, connected vehicles, surveillance devices, drones) are likely to require supplementation of this Guide with additional codes or principles developed to address a particular use or specific risks associated with that use. We encourage development of application specific initiatives to address features and concerns of particular applications.

We also support efforts in development of international and Australian standards. At the date of first publication of this Guide, relevant international standards have not developed to the stage where they can usefully inform the drafting of this Guide. This Guide will be updated following adoption of any relevant international standards about B2C IoT services and devices.

5. USEFUL REFERENCES

Abou-Zahra, Shadi, Judy Brewer, and Michael Cooper, *Web Standards to Enable an Accessible and Inclusive Internet of Things (IoT)*, Proceedings of the 14th Web for All Conference, W4A 2017, April 2-4, 2017, Perth, Western Australia (available at https://dspace.mit.edu/handle/1721.1/107831#files-area)

Australian Computer Society, Data Sharing Frameworks: Technical White Paper, October 2017 (available through www.acs.org.au)

American Farm Bureau, Privacy and Security Principles for Farm Data (http://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data)

Alliance of Automobile Manufacturers, *Automotive Privacy Principles*

Australian/New Zealand Standard AS/NZS 10002:2014*, Guidelines for complaint management in organisations*

Communications Alliance, *Telecommunications Consumer Protections (TCP) Code*

Consumer Electronics Association, *Guiding Principles on the Privacy and Security of Personal Wellness Data*

Consumers International, Connection and Protection in the Digital Age: The Internet of Things and challenges for consumer protection, April 2016 (http://www.consumersinternational.org/news-and-media/news/2016/04/new-report-internet-of-things/)

Data Governance Australia, *Code of Practice* (http://datagovernanceaus.com.au/dga-code-of-practice/)

Earlence Fernandes, Amir Rahmati, Kevin Eykholt, Atul Prakash, *Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?*, May 2017 (https://arxiv.org/abs/1705.08522v1)

Future of Privacy Forum*, Infographic: Data and the Connected Car* Version 1.0 (https://fpf.org/2017/06/29/infographic-data-connected-car-version-1-0/)

Future of Privacy Forum, *Always on: Privacy Implications of Microphone-Enabled Devices* (https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf)

Future of Privacy Forum, *Shedding Light on Smart City Privacy* (https://fpf.org/2017/03/30/smart-cities/)

Future of Privacy Forum, *Best Practices for Consumer Wearables and Wellness Apps and Devices* (https://fpf.org/2016/08/17/future-privacy-forum-releases-best-practices-consumer-wearables-wellness-apps-devices/)

Gov UK, *Data Science Ethical Framework Guidance* (https://www.gov.uk/government/publications/data-science-ethical-framework)

IEEE Internet of Things (IoT) Initiative, materials available at http://iot.ieee.org/

Information Commissioner's Office (UK), *Data sharing code of practice – ICO* (https://ico.org.uk/media/for-organisations/.../data_sharing_code_of_practice.pdf)

Information Commissioner's Office (UK), *Big data, artificial intelligence, machine learning and data protection* (available through https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/)

IoTAA Security Guideline V1.0 23 February 2017 (available through http://www.iot.org.au/resources/)

National Automobile Dealers Association and the Future of Privacy Forum, *Personal Data in Your Car* (https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf)

NIST Special Publication (SP) 800-160, *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*

Online Trust Alliance, IoT Security & Privacy Trust Framework v2.5, June 2017 (https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf)

Office of the Australian Information Commissioner (OAIC), *Privacy shortcomings of Internet of Things businesses revealed* (https://www.oaic.gov.au/media-and-speeches/news/privacy-shortcomings-of-internet-of-things-businesses-revealed)

OAIC, *What is personal information?* (https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information)

OAIC, *Privacy business resource 4, De-identification of data and information*, (https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information)

OAIC*, Privacy management framework: enabling compliance and encouraging good practice* (https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework)

OAIC, *Guide to undertaking privacy impact assessments* (https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments)

OAIC, *Guide to securing personal information* (https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information)

OAIC and CSIRO Data61, *De-identification Decision-Making Framework* (http://data61.csiro.au/en/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework)

Online Trust Alliance, Jan 2017, *IoT Trust Framework* (https://otalliance.org/initiatives/internet-things)

Privacy Commissioner of Canada, *The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments* (https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/02_05_d_72_iot/)

Tech UK, *Trust in an Internet of Things World* (https://www.techuk.org/insights/news/item/10031-iot-trust-principles)

US Department of Homeland Security, *Strategic Principles for Securing the Internet of Things* (available through https://www.dhs.gov/securingtheIoT)

W3C Accessibility Task Force, *Web of Things* and associated materials available at https://www.w3.org/WAI/APA/wiki/Web_of_Things.

ABOUT IOT Alliance Australia, (IoTAA)

The vision of IoTAA is to empower industry to grow Australia's competitive advantage through IoT.

IoTAA has 650 members from approximately 330 organisations across its seven workstreams. The workstreams are focused on:

- Collaboration
- Smart industries and cities
- Data use, access and privacy
- Spectrum availability and licensing
- Cyber security and network resilience
- IoT start-up Innovation; and
- Platforms and Interoperability.

IoTAA was incorporated as a not-for-profit entity in July 2016, emerging from the Communications Alliance IoT Think Tank, established in 2015.

IoTAA is hosted and supported by the University of Technology, Sydney (UTS) at its Broadway Campus in Sydney.

http://www.iot.org.au/