24 January 2022

Attorney General's Department
Federal Government
Canberra

By email lodgement: PrivacyActReview@ag.gov.au@ag.gov.au

To whom it may concern:

Subject: IoTAA submission to the Consultation on Privacy Act Review Discussion Paper

IoT Alliance Australia (**IoTAA**), https://iot.org.au/ welcomes this opportunity to address issues raised in your Privacy Act Review Discussion Paper.

IoTAA is the peak Australian IoT industry body, with over 500 participating organisations and 1000 individual participants. We grow the Australian IoT eco-system, help build capability and good practice, advocate for policies that help accelerate adoption and "IoT for good" that is safe and secure IoT deployment and uses of Internet of Things (**IoT**) devices and services in Australia. Our mission is to accelerate the adoption of IoT to improve competitive advantage of Australia and benefit Australian society.

The data privacy challenges of IoT enabled services and applications

Many societally beneficial applications of smart devices and smart infrastructure are dependent upon legislative and regulatory settings being appropriate to permit responsible deployment and use of IoT devices, while also protecting data privacy of individuals.

Particular care needs to be taken to ensure that changes to the data privacy statute do not dampen innovation in development and rollout of IoT enabled products and services and thereby impede Australia deriving societal benefits from take-up of smart devices and deployment of smart infrastructure. These benefits can be achieved without compromising the need to ensure that individuals are not exposed to and suffer relevant privacy harms. Getting this balance right requires careful consideration of the interaction of different requirements and prohibitions, and associated limitations and exceptions, that together make up the data privacy statute.

We consent to publication of this submission.

We thank you for the opportunity to make this submission.

We are available to discuss our comments and to provide any clarifications that you may require.

Yours Sincerely,

Frank Zeichner

CEO, IoT Alliance Australia

www.iot.org.au

Level 6, 91 York Street

Sydney 2000

+61 408 233 762

Getting the framework right

IoTAA strongly supports the current process for consultative review of the Privacy Act 1988. The Act requires a substantial overhaul. The review provides an opportunity for AGD to assist the legislature to:

- address uncertainties as to operation of the Australian Privacy Act,
- ensure that the Privacy Act 1988 remains fit for purpose in protecting personal information of individuals, while also accommodating fair and respectful collection and use of data, including through use of IoT devices to provide IoT enabled services that benefit Australian society and the Australian economy,
- reduce friction of cross-border dealings, including for Australian businesses expanding globally, by improving alignment of the Australian Privacy Act with leading data privacy and data protection statutes in other jurisdictions.

Many entities regulated under Australian data privacy laws already conduct operations in multiple jurisdictions, or have ambitions to do so. If Australia elects to chart its own course, Australian entities may be forced to incur substantial, regulation-induced, costs in adapting data architectures, analytics processes and data handling practices, for cross-border dealings. Australian policymakers should exercise particular caution to avoid, wherever reasonably practicable, devising regulatory measures that lead to Australia-specific, regulation-induced, costs for Australian entities in cross-border dealings.

Protecting of personal information of individuals is necessary to ensure that individuals do not suffer privacy harms:

- through intrusive or unanticipated surveillance;
- through service providers collecting or sharing more information relating to activities of persons than is necessary and as individuals would reasonably expect to enable a particular service to be provided to them,

and to assure that service providers implement good practice in data governance and information security.

Reforming a legal principles-based, data privacy statute is particularly complex. Expansion of categories of information that is protected, and changes to requirements protecting that information, readily lead to unintended consequences. It is particularly hard to draft provisions that remain clear as to effect and intended operation notwithstanding (currently unforeseeable) developments in utilisation of technologies and data

analytics capabilities, and continuing expansion in data points relating to devices and humans.

Privacy Act fitness and appropriateness to protect consumer welfare

The notice and consent framework of existing data privacy protection does not work well to ensure consumer welfare in many IoT deployment scenarios. Notice and consent works best when these is a direct, proximate and contractual relationship between a consumer that elects to buy and use a product or service, the provider of that product or service, and collection and use of data relating to that individual's use of the product or service.

This is not the case for many IoT scenarios, both household and non-domestic. Many IoT enabled services are deployed in environments where there is no direct relationship between a person active in that environment and the provider of the service. For example, a home IoT device may be installed and used in a domestic environment where the person that installs the device, enables the IoT service and/or sees reports is not a person whose activities are monitored or reported upon. A device may be installed in a rental property, or a shared household, or outside a property but enabling observation of activity within a property. A person may suffer a harm through excessive and unreasonable surveillance, or as a result of a device actuating an outcome that is adverse to a person, without that person knowing that they were observed, In many such scenarios, giving of notice, or provision of informed consent, are not reasonably practicable.

The data privacy statute is generally not the most appropriate instrument to regulate such activities. Consumer protection statutes (such as the Australian Consumer Law and State and Territory fair trading statutes), or surveillance and tracking statutes, or new statutory schemes to regulate uses and applications of AI and automated decision-making, may be more fit for purpose to address such activities.

In any event, a person may suffer a relevant surveillance harm, or adverse outcomes, through use of IoT derived data associated with that individual that is not information from which an individual is reasonably identifiable. It is not sensible to extend the definition of personal information under the Privacy Act to capture all data driven effects or outcomes that may be adverse to individuals. Among other reasons why not, such extension would remove regulatory incentives for product or service providers to minimise collection of personally identifying information to circumstances where collection and use of personally identifying information is necessary to provide a product or service.

Accordingly, we suggest that caution in changing the statute to expand categories of information that is protected as personal information, and changes to requirements protecting that information.

We support developments in other laws to the extent that those developments are necessary and proportionate to address surveillance and other harms to individuals that may arise in circumstances where personal information is not being used: that is, where the relevant data being collected, used or shared is not personally identifying information about or in relation to individuals.

We also support targeted and proportionate changes to the Privacy Act that have the effect of improving accountability of regulated entities and providing regulatory incentives for exercise of responsibility and restraint of regulated entities.

The respective role of industry standards and good practice guides, and regulation

In many IoT deployment scenarios today, deficiencies in data privacy management arise through lack of understanding of entities as to good practice in anonymisation and other privacy enhancing technologies and processes, rather than deliberate malfeasance by regulated entities.

A first priority in data privacy regulation should be to ensure that there are industry standards and good practice guides as to evolving good practice in governance and assurance of handling of personally identifying information.

Of course, some entities will not consistently and reliably implement good practice. Regulation will be required to cause these less motivated entities to their standards.

However, regulation should not supplant industry standards and good practice guides, because these may more readily revised and evolve over time, and can be targeted to address particular circumstances of product or service categories or types.

Making of Industry Codes

The Discussion Paper at 3.1 canvasses an amendment to the Act, to allow the IC to make an APP code on the direction or approval of the Attorney-General:

- where it is in the public interest to do so without first having to seek an industry code developer, and
- where there is unlikely to be an appropriate industry representative to develop the code.

Section 26C(3)(a) as now in force provides that an APP code may impose additional requirements to those imposed by one or more of the APPs, so long as the additional requirements are not contrary to, or inconsistent with, those principles.

Section 26G (Development of APP codes by the Commissioner) provides a limited control as to the Commissioner using code-making authority to expand coverage and requirements of the privacy statute. The IC may develop a code if (1) satisfied that to do so is in public interest, and then only if (2) the IC has requested (under subsection 26E(2)) a code developer to develop a code and the request has not been complied with, or the request has been complied with, but the IC has decided not to register, under section 26H, the APP code that was developed as requested.

A key current control over over-expansive coverage of codes is that codes are developed through consultations within an industry sector led by an industry code developer, and not imposed upon an industry sector by unilateral action by the IC.

That control is appropriate, regardless of whether or not that unilateral action is directed or approved by the Attorney-General. If the Information Commissioner was empowered to make an APP code of its own volition and on the Attorney-General's view of 'public interest', that code could add new requirements to those imposed by one or more of the APPs and otherwise impose substantial additional regulatory burdens upon APP entities. This would be an inappropriate delegation of quasi-legislative authority to the IC. The IC would be effectively unregulated by the Parliament, acting at the discretion of a Minister exercising that Minister's personal and political view as to the public interest.

The IC's powers of stepping in to determine a code should be appropriately qualified, reserve powers only exercisable where an industry code developer fails to develop a code after that industry code developer has been afforded a reasonable opportunity, and a reasonable timeframe, to do so.

As is clear from existing section 26C(3)(a), an APP code may impose additional requirements to those imposed by one or more of the APPs, limited only by the requirement that additional requirements are not contrary to, or inconsistent with, those principles. It would be an inappropriate delegation of quasi-legislative authority to the IC to enable this discretion to be exercised by the IC, unless:

- an industry sector has been afforded a reasonable opportunity, and a reasonable timeframe, to address a request by the IC for the industry sector to develop a code, and
- the relevant request states the nature of the additional requirements which the IC requests that industry sector to address in a code and why the IC considers those additional requirements to be in the public interest, such that the industry sector can be reasonably considered to be on notice as to the IC's expectations and grounds for those expectations.

A period of twelve months should be specified as a minimum period. Given the potential for the IC to develop a code if an industry sector does not develop a code, we consider it most unlikely that the industry sector would fail to nominate an appropriate industry representative to develop a code.

Addressing supply side multiparty data ecosystems

In many scenarios today where potentially identifying information is shared between entities today, there is poor or unclear allocation of roles and responsibilities to ensure good data privacy management across the data ecosystem. Many IoT deployments involve multiple entities sharing some data relating to provision of an IoT enabled service. We consider that introduction of a data controller-data processor restriction would:

- assist in ensuring that there is clarity as to which entity within a multiparty data ecosystem is responsible for controlling uses and disclosures of personally identifying information by other entities within that ecosystem, and
- lift levels of compliance by other entities within that ecosystem with reasonable expectations as to good data governance and assurance processes and practices.

Introduction of this distinction would also assist in ensuring that there is alignment between statement of purpose in collection and handling of personally identifying information, as given to the user of a product or service, and necessity and scope in how this information is handled across a multiparty supply side data ecosystem.

Accountability, purpose and necessity

Relevant changes to the Act should also include clarification of how regulated entities should evaluate necessity to achieve a purpose, and how regulated entities should provide appropriate transparency as to purpose and other matters required to be addressed in privacy policies and notices. The statute should provide appropriate guardrails to ensure that:

- collection and handling (including disclosure) of personal information is:
  - only as necessary and reasonably proportionate to give effect to a clearly stated purpose (as stated in a published and reasonably prominent privacy statement) and directly related secondary purposes, or
  - only as affected individuals may reasonably expect, with reasonable expectations informed by acts or practices specified in the statute as permitted legitimate uses or compatible uses, or

otherwise in compliance with an industry code registered by the regulator, or a class exemption made by the regulator,

- otherwise, that information relating to individuals is not collected or handled in personally identifying form, or that personally identifying information is transformed so that this data becomes not personally identifying because this data is reliably deidentified and then used or disclosed only as effectively anonymised information.

Deidentification, pseudonymisation and anonymisation

It is critically important for this reform process to get right how the privacy statute addresses deidentification, across the spectrum from pseudonymisation to full anonymisation.

Many societally beneficial applications of data relating to citizens depend upon use of controlled and safeguarded data analytics environments within which individual level (transaction and transactor) data may be linked and analysed with appropriate assurance of privacy and security by default and design, both for the handling of data isolated within the controlled data environment, and outputs released from those controls.

'Deidentification' as a term is commonly used to refer to a spectrum, from:

(1) removal of direct identifiers, but indirect identifiers remain within associated information that might be used to effect identifiability. This might be referred to as 'pseudonymised information', to

(2) removal of both direct or indirect identifiers, but although the associated information is not of itself sufficient to effect identifiability, other information available elsewhere might be used to effect identifiability, and accordingly the information is only protected against identifiability if effectively isolated (through effective controls and safeguards) from that other information that otherwise (were the information not so isolated and protected) might be used to effect identifiability. This might be referred to as 'controlled deidentified information', to

(3) removal of all potentially identifying information, so that information may be released into an uncontrolled environment where third party identification attacks are possible. This might be referred to as 'uncontrolled deidentified information'.

If an entity demonstrably (reliably and verifiably) disables itself from capability to associate online data with an individual through technical means (i.e., through masking, anonymity, differential privacy, privacy-preserving machine learning and synthetic data, as well as through data transformations such as aggregation) and environmental (operational, contractual and other) conditions (controls, safeguards and guardrails), such that individuals are not

identifiable by any means reasonably likely to be used (i.e., the risk of harm to an individual of identification is sufficiently remote), the information is and should remain regarded as effectively or functionally anonymised (deidentified) and not be regulated as personal information.

It is not possible in practice to ensure that most consumer data is anonymised to the point where reidentification can be assured to be impossible over time: other data sources may become available that facilitate pattern or mosaic identification attacks, or technical processes for identification attacks may involve, in ways that cannot reasonably be anticipated by a regulated entity. For this reason, state of the art analyses of anonymisation technologies and techniques draw a distinction between 'functional anonymisation' (also sometimes called 'effective anonymisation'), and 'complete anonymization' (also sometimes called 'full anonymisation') (viz., anonymisation assured as pervasively reliable over time). Many experts consider that complete (full) anonymisation is not possible in practice for most consumer data.

If "anonymisation" is to replace "deidentification" as the relevant statutory term, it needs to be clear:

(1) that the standard remains 'functional (effective) anonymisation', where individuals are not identifiable by any means reasonably likely to be used - i.e., the risk of reidentification is sufficiently remote; as compared to full anonymisation (where individuals cannot be identified by any conceivable means);

(2) that in assessment of whether information is functionally (effectively) anonymised, account is to be had of both (a) the nature of the data, and (b) the data situation (data environment), in particular having regard to security and access controls and other controls and safeguards applied to a data processing environment in which that data is handled. It follows that a particular data set may be regarded as functionally (effectively) anonymised when handled within a controlled data situation (data environment), but not functionally (effectively) anonymised when released 'into the wild' (viz., into an uncontrolled data situation (data environment);

(3) what is the standard for assessment of residual (after implementation of mitigations) reidentification risk. The appropriate standard is "very low" or "sufficiently remote". The appropriate standard is not (as the Discussion Paper suggests) "extremely remote or hypothetical", which appears to equate to complete (full) anonymisation, which does not reflect state of the art analyses of technologies and techniques for reasonably practicable anonymisation.

In summary, an entity may handle deidentified information within a controlled data situation (data environment) that should not be regarded as personal information to the extent that this information remains within that

environment, but outputs from that controlled environment must be separately assessed as to identifiability risk if and when those outputs are released from relevant controls.

In each case, the standard for assessment should be "very low" or "sufficiently remote".

The outcome from application of that assessment is likely to be different when (1) the relevant information is for release into an uncontrolled environment, as compared to (2) the relevant information is effectively controlled.