10 December 2021

Attorney General's Department

Federal Government

Canberra

To whom it concerns:

Subject: IoTAA submission to the Online Privacy Bill and consultation Regulation Impact Statement

IoT Alliance Australia (IoTAA), https://iot.org.au/, 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 in Australia to improve our competitive advantage and benefit society.

IoTAA welcomes this opportunity to provide a response to the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the **OP Bill**), released for public comment in October 2021.

Key points

IoTAA strongly supports the current process for consultative review of the Privacy Act 1988, which requires a substantial overhaul. IoTAA will be making a detailed submission in response to the Discussion Paper.

The proposals in the Discussion Paper would apply to all regulated entities, not just limited sectors. This is appropriate. Advances in data analytics conducted at the level of individual transactors (whether or not identifiable) and their transactors, the shift to online transacting and use of geolocating internet access device, take-up of IoT (non-conventional internet enabled devices including personal wellness devices, smart speakers, TVs and other home automation devices), data labelling and rearchitecting of data platforms to enable data to be discoverable and more useful), have fuelled ever more sophisticated profiling of individuals. The Privacy Act needs to provide clear guardrails and enable a regulator to supervise implementation

by regulated entities across the economy, of data privacy by design and default and other appropriately privacy protective controls and safeguards, to address these challenges.

Support for Schedules 2 and 3, with some revision.

IoTAA supports enhancement of the range of regulatory powers and tools available to manage enforcement of the Privacy Act for all sectors, as addressed in Schedules 2 and 3 of the OP Bill. IoTAA has concerns as to the framing in the Exposure Draft of some of these changes. IoTAA has reviewed the Communications Alliance submission as to possible revisions to Schedules 2 and 3 of the OP Bill to address such concerns and endorses those proposals.

Propose that Schedule 1 not be included in the Bill or alternatively restrict classes of organisation covered.

However, we are concerned that the draft provisions in Schedule 1 of the OP Bill pre-empt development of appropriately crafted, substantial changes to the Privacy Act, as canvassed in the Discussion Paper. These changes are not yet developed and specified to a level of detail to provide sufficient clarity and certainty to guide OP organisations to develop an OP code. The list in section 26KC(2) of matters that must be addressed in an OP code would require OP organisations to guess and fill-out - effectively, to pre-empt - outcomes of the detailed drafting and balancing of the broad range of privacy controls, safeguards and incentives for minimisation in collection and handling of personal information relating to individuals, as canvassed in the Discussion Paper.

IoTAA therefore submits that Schedule 1 of the OP Bill should not be included in the bill.

Alternatively, IoTAA suggests that draft provisions of Schedule 1 of the OP Bill should be rescoped to require a more limited class of covered organisations to address how they give effect to requirements of current APPs, applying current definitions in the Privacy Act (including as to personal information and consent).

IoTAA submits that the OP code should cover acts and practices in collection and handling (including disclosures) of personal information relating to personally identifiable individuals where an activity is a covered activity or relevant information is directly or indirectly derived from conduct of an activity which is defined as a covered activity.

By contrast, under the Exposure Draft each OP organisation is covered and regulated for all their activities, not only provision of a service that led to them becoming within coverage. The only exception (outside exercise of Ministerial

discretion) is if section 26KC(9) is used by the code developer or the Commissioner to take out of coverage particular activities of a covered entity as specified by the code developer or the Commissioner respectively. This is a disproportionate response. It leads to clear inequity as between specialist entities and diversified entities. It also creates likelihood that a Code will not be agreed (because of diversity of interests and concerns of potentially covered entities) and therefore that the IC will determine a Code.

After the Bill receives Royal Assent, the OP code will need to be developed and registered within 12 months. There should be a staged (phased) approach to development of the code, so that industry is not pre-empted by intervention by the regulator because of unrealistic expectations as to how quickly a code may be developed. At the minimum, industry should be allowed a clear twelve months from enactment of the OP Act to finalise a final draft code for submission to the Commissioner for registration.

If Government and the legislature is concerned that industry development may be delayed or stall due to complexity and range of covered activities and covered entities, the best way to address that concern is to narrow the range of entities and activities to be covered, and to require the code to address only those matters where Government and the legislature require urgent attention.

More detailed comments

IoTAA is strongly supportive of government and the legislature delegating to industry participants a leading role in development of codes and best practice guidance as to how to implement legislated settings as to data privacy.

However, the reset envisaged by the Discussion Paper of legislated settings as to data privacy is not sufficiently elaborated by the OP Bill, or capable of being further elaborated in any revised OP Bill drafted in advance of the Discussion Paper reforms, to enable industry to now take on the heavy lifting of code development.

As the Discussion Paper recognises, legislated reforms need to be carefully crafted. The impact of possible legislated responses needs to be considered 'in the whole', developed considering how individual changes will operate together as a package of measures. Careful consideration and balancing of legislated settings are required to address the breadth and range of issues arising from diverse activities of entities that collect and use information relating to individuals for good or bad 'singling out' (differentiated treatment) of individuals. The Discussion Paper, and not the OP Bill, envisages a revised

Privacy Act drafted following careful consideration and balancing of a package of measures.

The Discussion Paper, rightly and sensibly, envisages a fundamental shift in the Privacy Act, addressing the key issue of 'the illusion of choice'. Regulation today focusses upon creating transparency (through privacy disclosures) for citizens, to enable citizens to exercise choice. As now almost universally acknowledged, choice is often impractical, and usually made difficult to exercise. 'Notice and consent fatigue' is real.

However, to enable shift in the focus of regulation away from consumer choice and towards requiring more responsible practices and greater accountability of regulated entities, regulated entities require sufficient certainty (clarity and predictability) as to what good data privacy practice looks like.

Any OP code developed by social media providers, data brokers and online platforms is unlikely to enter into operation significantly before finalisation and passage of a comprehensive package of Privacy Act reforms as envisaged by the Discussion Paper. The OP code would then require substantial overhaul to address further or changed requirements of that revised Privacy Act. This duplication of effort will waste money and human resources across over 500 organisations, by the Government's own (conservative) estimate, impacted by these reforms.

The list in section 26KC(2) of matters that must be addressed in an OP code pre-empts, overlaps and sometimes contradicts the following key elements of the reforms canvassed in the Discussion Paper:

- A definition for consent which elaborates the required elements differently as to detail from proposed s.26KC(2)(e) in this OP Bill.
- A requirement that notices under APP 5 must be clear, current and understandable, differs in detail to proposed s.26KC(2)(g) of this OP Bill. In particular, the OP Bill also appear to shift the balance between transparency through privacy policies and transparency through APP 5 privacy (collection) notices in a way which is directly contrary to the proposal in the Discussion Paper to reduce complexity and 'noise' of APP 5 notices.
- A right to object to (opt-out from) use or disclosure is analogous to proposed s.26KC(2)(h) in this Bill, but envisaged to be drafted to include appropriate, reasonable bases for exceptions from an opt-out option (i.e., carve-downs for reasonably anticipated or compatible uses or legitimate uses or interests), as compared to the most uncertain scoping of "such steps as are reasonable in the circumstances".

- The circumstances in which parents or guardians will need to consent on behalf of children aged under 16, analogous to proposed s.26KC(6)(b) in this Bill, but with revision of the Privacy Act likely to be after (and therefore informed by) finalisation of the current efforts of many industry participants and at least five industry associations to develop an Age Verification Implementation Roadmap for online safety, which is scheduled to be presented to Government in December 2022.
- A requirement to ensure that collection, use and disclosure of personal information is 'fair and reasonable', and where that information is about children it must be in 'the best interests of the child', analogous to proposed s.26KC(6)(e)-(f) in this OP Bill, but yet to be elaborated.

The Discussion Paper says that the Online Privacy Bill "addresses the unique and pressing privacy challenges posed by social media and online platforms".

We disagree with the characterisation that privacy challenges posed by social media and online platforms are unique or sufficiently different to other sectors as to make it now sensible or appropriate for the legislature to require those sectors to address those challenges now, separately, and ahead of legislated economy-wide reforms.

We disagree that the need to address relevant "challenges posed by social media and online platforms" is so pressing that it today makes sense to require over 500 organisations, by the Government's own (conservative) estimate, to expend substantial money and devote human resources to trying to guess and pre-empt future privacy reforms.

To the extent that protection of children and other vulnerable persons is a pressing and time sensitive concern, the current detailed work of many industry participants and at least five industry associations, working with and supervised by the eSafety Commissioner, including evaluation and design of age assurance and age verification measures, should be prioritised. Diversion of responses from that effort may be counterproductive.

Indeed, the age assurance and verification measures envisaged by the OP Bill are likely to lead to the perverse policy outcome of covered entities being required to collect more personal information relating to individuals, directly contrary to appropriately privacy by design, legislated settings, as canvassed in the Discussion Paper. For example, obtaining consent from, or providing notification(s) to all household members, including minors, who use a smart speaker. We note that age of internet users could only be assured by collecting more personal information about most individuals regardless of their age, to work out whether they then need to be subject to even more privacy intrusive collection of personal information through age verification.

There is therefore a very real risk that fast-tracking the OP Bill leads to worse outcomes for many affected individuals than the more balanced package of age assurance mechanisms and protected guardrails for services attractive to children, as envisaged by the Discussion Paper.

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