

Parliament of Australia
Exposure Drafts of Australian Privacy Amendment Legislation

About Yahoo!7

A joint venture between Yahoo! Inc and the Seven Media Group, Yahoo!7 offers a range of content, navigation and information services to internet users in Australia. Yahoo!7 is focused on powering its communities of users, advertisers, publishers and developers by creating indispensable experiences based on trust. We welcome the opportunity to provide Yahoo!'s unique perspective on the current landscape in global privacy matters, where we draw on 15 years of experience delivering innovative features for our users, striving to ensure the highest level of responsible privacy protection along the way.

Inquiry Terms of Reference

The Senate has referred the exposure drafts of Australian Privacy Amendment Legislation to the Finance and Public Administration Legislation Committee for inquiry.

The Senate agreed that in undertaking this inquiry the committee may consider the exposure draft of the Australian Privacy Principles and the draft companion guides on the Australian privacy reforms and any other relevant documents tabled in the Senate or presented to the President by a senator when the Senate is not sitting.

Submission

Yahoo!7 welcomes the opportunity to participate in this inquiry by providing feedback on the first component of privacy law reform in Australia, the new Australian Privacy Principles. We have considered both the Exposure Draft of the Australian Privacy Principles and the draft companion guide to the Australian Privacy Principles and provide the following preliminary comments on selected sections of the Exposure Draft. Yahoo!7 looks forward to ongoing engagement on this text as public dialogue continues to account for internet technologies and their privacy implications for Australian users of global services.

Exposure Draft of the Australian Privacy Principles

Australian Privacy Principle 1

Point 4(g): We consider international data transfer and back up to be ubiquitous in the online services industry especially when you consider cloud computing phenomena. We are concerned that it may not be practical to require companies to specify which countries they transfer data to in their privacy policies and favour a simple disclosure obligation

which refers to international data transfer and back up more generally.

Australian Privacy Principle 2

We are concerned that the statement in point (1) is very broad. Yahoo!7 makes many services available to users who are both registered and unregistered. There is a core group of products and services that Yahoo!7 requires users register to use and we rely on this data to enforce the terms of use for each service and to assist law enforcement agencies when they are investigating crimes that involve one of our services. We do offer users the ability to interact with other users using a pseudonymous screen name, but maintain that it is necessary for users to be accountable for their use of our services. Companies operating ecommerce websites also have a clear need for users to authenticate their identity through the use of credit cards to pay for sales. We consider that a one size fits all solution is not practical for the diverse range of interactions taking place online and that context needs to dictate the appropriateness of allowing users to engage anonymously or to interact pseudonymously within these services. We would welcome some guidance from the Committee on these issues. How does the Committee envisage this choice being offered to individuals? How can service providers balance the need to allow individuals to engage anonymously whilst at the same time ensuring that appropriate information is retained in the event of abuse or misuse of the services?

Australian Privacy Principle 3

Yahoo!7 aggregates behavioural data relating to our users for the purposes of interest-based advertising. Interest-based advertising generally relies on information about web browsing behaviour, such as ads viewed, ads clicked, pages viewed, pages clicked, and/or search terms entered, to serve selected advertisements to a specific browser that will hopefully be more relevant to the user of that browser. Conceivably, certain sensitive topics could be gleaned from web browsing habits observed on a particular browser. It is important to emphasise that behavioural technology is based upon identifying a browser, rather than an individual user per se. As such, an IP address facilitates assignment of interest categories to a unique browser, using a browser cookie set for this purpose. We would argue that the fact that this information is not intended to be attributed to an individual precludes it from being considered sensitive information. Further, verified information about sensitive topics specific to an identified user, such as medical records, should be treated differently under the law than mere inferences based on web surfing interests presumed or associated with a browser, as might be the case if websurfing suggests a high interest in fitness or health-consciousness articles, for example. We welcome additional guidance from the Committee on this matter.

Australian Privacy Principle 4

Points (3) and (4): this provision seeks to shift liability for the original collection of personal information from the original collector to an entity who receives the information where it was “unsolicited.” It is unclear what is intended in the language suggesting a lack of solicitation. Is this intended to speak to policies for accidental receipt, contracted purchase or other? We are concerned that this is a challenging obligation to meet when the entity cannot secure the same consents as were provided to the original collector but has nonetheless obtained the information in a lawful and privacy abiding manner. There are many legitimate sources of personal information both in the public domain through government agencies and from private companies, however an entity receiving personal information from one of these sources may not be in a position to influence or control the

original collection of this information. We therefore ask whether it is reasonable to require the entity to either, (a) comply with APPs 5-13, (b) destroy the information, or (c) de-identify it.

Australian Privacy Principle 5

We commend the drafting of this principle and consider it to be a very pragmatic and flexible acknowledgment that the context around collection of personal information will be determinative of how and when notification is provided. In relation to points (i) and (j), we reiterate that international data transfer is the norm in the age of cloud computing. These disclosure obligations therefore need to be meaningful and actionable by users.

Australian Privacy Principle 6

No comment

Australian Privacy Principle 7

No comment

Australian Privacy Principle 8

As we are part of a multinational company, we read this Principle relating to the cross border disclosure of personal information with great interest. As mentioned above, we consider cross border disclosures of personal information to be ordinary in the course of online business and we favour implementing accountability for the handling of personal information across borders through self regulatory codes and cooperative instruments. Whilst we appreciate the need to provide information and reassurance to users in relation to cross border transfers, we consider any reliance on distinctions between borders to be unrealistic.

Australian Privacy Principle 9

No comment

Australian Privacy Principle 10

No comment

Australian Privacy Principle 11

Point (2)(b): Yahoo!7 broadly agrees with the flexibility in approach articulated within this principle, however we would like to suggest that the touchstone for the decision around whether personal information needs to be retained refer to “legitimate business purposes” rather than by referring to purposes under Division 5 of the Australian Privacy Principles.

Australian Privacy Principle 12

No comment

Australian Privacy Principle 13

We are strongly supportive of this Principle, which recognizes that the timing and nature of consent will require flexibility in approach.

Part B – Other relevant provisions

Personal information definition: we consider that the concept of ‘information’ is sufficiently broad to encompass ‘opinion’ and request that references to “opinion” be removed from this definition. We also ask that the words “by an entity” be added to the opening sentence of this definition as a person may be reasonably identifiable to one entity but not to another. By way of example, an IP address could be considered personal information by an ISP as they are capable of reasonably identifying the person to whom that IP address resolves back to. An online services provider who does not offer Internet access will not be able to use an IP address to identify a person. We also

consider the reference to “material form” in part (b) of this definition to be confusing given the many different forms that information can take in the electronic information age.

Record definition: we could not find any references to “records” within the Exposure Draft.

Sensitive information definition: we would like to highlight how difficult it has been for other jurisdictions to arrive at a sensible definition of sensitive information intended to apply to internet contexts while avoiding risk of over breadth. We note at the outset that the definition of personal information (on which sensitive information is based) is broad in that it includes information which is true or not. We repeat the same feedback we provided in relation to the personal information definition suggesting the deletion of references to “opinion.” We ask that the Government consider a distinction be made between information which a person has declared (e.g. through ABS statistics) and information that is inferred or extrapolated from a person’s online behaviour. We consider that information that has been declared may fall within the definition of sensitive information, subject to consent levels appropriate to sensitive data. However, inferences about interests are neither sufficiently precise nor specific to a user to create the risks of harms traditionally associated with truly sensitive data. We are also concerned by the inclusion of “political opinions,” as distinguished from the more common “political affiliations” within this definition. Restricting the former might adversely impact freedom of expression, whereas categorisation of the latter as sensitive information (if declared by an identifiable data subject) could more likely be viewed as “speech-protective.” We note alternately that if a person has made a political comment within a public domain, we do not think this should be treated as sensitive information. We also consider the category of “philosophical beliefs” to be too broad in this context. Would the Committee consider someone visiting a website extolling the virtues of tai chi to be indicative of a philosophical belief? With respect to the inclusion of “sexual orientation,” we suggest that the Committee consider the breadth of this notion and determine what specificity could be added to provide needed guidance for practitioners. Traditionally the view that Lesbian, Gay, Bisexual or Transgender status (LGBT) may be considered sensitive, whereas heterosexual orientation might be deemed less sensitive information in Australia. Including a reference to “health information” is also concerningly broad. While we completely understand and agree that medical records should be treated as sensitive, but what about whether a person has a gym membership? We urge the Committee to revisit these categorizations with great rigor as they are likely to significantly shape many business practices and the current definitions do not provide the clarity that would normally be sought from provisions triggering affirmative consents to collection of specific types or categories of sensitive information

Draft Companion Guide to the Australian Privacy Principles

Interaction with State and Territory Laws. We note that one of the intentions in reforming Australia’s privacy laws was to streamline and harmonise legal obligations in this area yet Section 3 of the existing Privacy Act will remain in the new Privacy Act. Section 3 of the existing Privacy Act allows any State or Territory to implement laws as long as they can co-exist with the overarching Privacy Act framework. This introduces a

level of uncertainty for Yahoo!7 as we were hoping to operate under a single unified privacy regulation framework . In addition the inclusion of this provision in the new Privacy Act increases the burden on organisations like ours who are seeking to comply with all applicable laws by requiring that we research State and Territory laws in addition to the national Privacy Act whenever we are collecting, disclosing or using personal information.

Definition of personal information. The addition of the concept of “identification” within the definition of personal information introduces a degree of legal uncertainty. We appreciate that this increases consistency with international privacy laws but we urge the Committee to consider this issue further and provide clarification on the practical scope and effect of this change.

Contact

Please address any questions regarding this submission to:

Samantha Yorke
Legal Director Asia Pacific
Yahoo! Australia and New Zealand
Levels 2 & 3
Pier 8/9
23 Hickson Road
Millers Point NSW 2000
Tel: 02 8288 4790
Email: