Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/about/contacts

6 May 2021

Win3 Pty Ltd t/as Openly Australia
public-consultation@openly.com.au

Assistant Commissioner, Regulation and Strategy
Office of the Australian Information Commissioner
Melanie.Drayton@oaic.gov.au

Consultation re Openly Code under the Privacy Act 1988

This submission responds to the invitation by Openly Australia for comment on the proposed registration of a Code under section 26F(2) of the *Privacy Act 1988* (Cth).

The submission

The submission is made by the Australian Privacy Foundation. The Foundation is the nation's preeminent civil society body concerned with privacy. It is independent. Its membership and board feature experts in information technology, health, public administration, marketing and law. Background information about the Foundation is attached.

The following paragraphs provide an appraisal of the proposed Openly scheme before addressing specific concerns. Overall the Office of the Australian Information Commissioner should **not** proceed with registration of the proposed Code, in particular pending completion of the current review of the Act.

Appraisal

The Privacy Act provides for registration of Codes that are have effect under that statute and are developed by entities other than the Office of the Australian Information Commissioner (OAIC).

The expectation appears to be that a specific Code will gain substantial acceptance among nongovernment entities covered by the Act and address the needs of particular sectors. The Foundation's reference to 'appears' is deliberate, given disagreement during development of the legislation and the absence of widespread industry support for codes.

That absence of support is highlighted by the demise of the Biometrics Industry Code that was registered but expired due to non-commitment by large and small entities concerned with biometrics and disregard by consumers or other stakeholders. Few consumers, research entities and government agencies appear to have been aware of the Code's existence or accepted that it provided a meaningful public benefit.

We are unpersuaded that the proposed Openly Code will gain substantial traction among Australian and overseas commercial and government entities, meaning that it is unlikely to be sustainable.

We are also unpersuaded that the proposed Code will attract the endorsement of consumers and other stakeholders, something that is the prerequisite for a Code that is both legitimate and commercially viable. Legitimacy is pertinent, given that the OAIC in registering a Code lends the Code operator the authority of law and the regulator. It is axiomatic that such a benefit requires dispassionate appraisal rather than 'you get it because you asked for it'.

Our wariness about the proposed Code reflects Australian and overseas experience regarding private certification schemes, aka trust marks. Consumers, trade practices regulators and other entities have for example expressed deep concerns regarding the failure of US private codes such as TrustE and eTrust to provide effective protection for consumers, in particular to address breaches of the particular code on a timely basis that deters future misbehaviour and gains consumer trust. The extensive academic and professional literature indicates that few privacy 'seals' or 'trust marks' are indeed trusted by consumers and protect meaningful protection.

We have no commercial interest in seals or private sector certification mechanisms. Given our comments above we note, however, the difficulty that will be faced by Openly as a start-up in gaining and maintaining significant support. We consider that the OAIC should be very conscious of overseas experience and the defunct Biometrics Code. It would be inappropriate to enshrine a private Code that fails to gain traction and accordingly expires after a few years, particularly a Code whose operator because of lack of support is unable to undertake enforcement of the Code through for example auditing of claims made by subscribers to that Code.

We note that the proposed Code does not appear to have been endorsed by any of major banks, insurers, health service providers, internet service providers and telecommunication companies.

That non-endorsement is unsurprising given our view that the proposed in practice offers little benefit for businesses or consumers, an assessment that we discuss below.

Openly Code Objectives

Openly indicates that the "primary purpose" of the draft Privacy (Openly Australia) Code 2021 "is to provide Openly Certified Entities with greater clarity around how APP 1, APP 3, APP 6 and APP 7 are to be complied with" and incorporate "higher standards of privacy protection than is required by the Privacy Act".

We are unpersuaded by any of the publicly-available documentation from Openly that the proposed Code will indeed provide "greater clarity" about the interpretation of the Australian Privacy Principles (APPs). Our view is that if the OAIC's current explanation of the APPs is inadequate that inadequacy should be addressed by the OAIC on a commercial neutral basis through for example amendment of the OAIC's existing detailed guidelines.

The proposed Code does not meaningfully provide "higher standards" than required by the Act. Overall it can be read as inviting businesses to pay money to do what they are *already* required to do under the Act or what they already should do in anticipation of law reform.

We reiterate that the OAIC should **not** be registering a Code until finalisation of the current review of the 1988 Act and community consultation through the parliamentary committee process of any legislative reform consequent on that review.

We commend Openly's reference in the draft articulation of the Code Objectives to enhancing privacy capability and accountability, building community confidence and sustaining a culture of respect for the privacy of individuals. However many consumers are likely to regard that language as unsurprising boilerplate that is aspirational rather than determinative.

We for example see no reasons to believe that the proposed Code will indeed tangibly enhance accountability. Indeed, accountability might best be provided by the OAIC and by the Australian Competition & Consumer Commission rather than by a commercial entity that potentially fears to

bite the commercial hands that feed it or that through administrative incapacity is reliant on misleading claims by clients that they are trustworthy.

We see the OAIC as having a key responsibility in "building community confidence and sustaining a culture of respect for the privacy of individuals". The OAIC indeed characterises its operation in such terms. Individual public/private sector entities must participate in the development of privacy practice that clearly reflects the needs of Australians; development neither should nor can be delegated to a self-interested commercial service provider.

Our scepticism reflects specific weaknesses in the Openly documentation.

Openly indicates that an OCE (ie a client) "must have a Privacy, Security and Safety Plan". There is no requirement for that Plan to be tested or 'gold standard'. Given Openly's reliance on self-assessment by OCE's (notionally validated through a 40 point checklist) the standard might indeed be simply that there is 'a plan', providing protection that is potentially much weaker than the Privacy Impact Assessments undertaken on a self-assessment basis by some government agencies. There is no reference to independent standards and independent verification.

Openly indicates that OCEs "must implement a privacy training and awareness program that is regularly delivered to employees'. As with the requirement to have a plan – potentially 'a plan, any plan' (including one left in a drawer) – there are uncertainties about whether the training will be meaningful. Is Openly planning to provide the training … and perhaps self-audit?

The documentation indicates that OCEs must report annually to Openly as the Code Administrator about privacy complaints. It is unclear whether Openly will (and indeed can) respond on a timely basis. There appears to be no requirement for Openly to publish a client's disregard of the Code or to publish detailed data about the operation of the proposed scheme, for example to enable evaluation of the Code, of Openly and of OCEs.

The documentation refers to a Privacy Code Integrity Committee. That Committee is, in our view, worryingly misnamed. It has no authority and observers of a range of such committees overseas will conclude that it is at best an inadequate governance mechanism.

The proposed Code involves OCE "self-assessment" with fifteen "mandatory modules" assessing compliance with "best practice, the Code, the Guidelines, the Agreement and Australian Privacy Law'. Given our above statements we consider that the OAIC should not endorse that self-assessment in the absence of publicly-available information about what the modules cover and whether they are sufficiently rigorous to justify endorsement under the Privacy Act. It would be easy to develop fifteen modules that individually comprise little more than a single question answered with a 'yes' or a tick. Such an assessment would lack legitimacy. It incumbent on the OAIC to seek details.

Scope

Openly states that the scope of the public consultation includes specific questions.
Building on our preceding comments, we respond as follows:

- *whether organisations are likely to opt-in to be bound by the code;*
  Not in sufficient numbers to justify the Code.
- *whether organisations that will be bound by the APP code have sufficient resources to implement the code's requirements;*
  Unclear. Major entities are likely to see no benefit.
- *whether existing legislation, regulation or a code covers the same or similar topics that may negate the need for this code;*
  Yes. In particular we highlight the inappropriateness of registering the Code until any statutory changes are in place following the review of the Privacy Act.
- *whether the code adequately imposes additional requirements to those imposed by one or more of the APPs;*

We see no meaningful benefit. More broadly, the Act should be updated to reflect, for example, coherence with the benchmark General Data Protection Regulation and new Californian consumer protection regime.

- *whether the code adequately deals with the internal handling of privacy complaints by all the entities bound by the code;*
  The proposed Code is inadequate and does not foster the trust that is one of Openly's stated objectives.
- *whether the code is likely to impose additional regulatory burden upon the Office of the Australian Information Commissioner (OAIC);*
  Unclear. We note that the Code should not be used as a justification for reducing the already inadequate funding of the OAIC, in other words exacerbating existing regulatory incapacity.
- *whether the code achieves driving broader cultural changes relating to privacy and transparency;*
  the Code is an inadequate mechanism that we believe has the potential to confuse rather than enlighten and comfort. We further believe that an unviable Code will erode trust.
- *whether the code will assist in supporting entities to meet their existing obligations under the Act;*
  Not meaningfully in addition to current arrangements.
- *whether the code is likely to have a positive effect of the privacy of individuals;*
  No. See above. We believe it may have a deleterious effect.
- *whether individuals are likely to understand the benefits of the code; and*
  No. We consider that the benefits are uncertain. We question whether the Code will gain and retain the necessary support from both individuals and businesses.
- *any other matters relating to the Code*
  See above.

Conclusion

In conclusion, we see **no** basis for registration of a new Code prior to finalisation of the review of the Privacy Act. It is conceivable that the review will conclude, consistent with our comments above, that Codes *per se* are ineffective and should not feature in a revision of the Act that provides a fit-for-purpose statutory framework.

We question whether the proposed Code will be beneficial and viable.

Openly states that it aims to remove "the legalese, the tin foil hats and all of the overly complicated foundations of privacy". We caution that the proposed Code appears unlikely to do so. Reference to "tin foil hats" does not justify any mechanism that erodes the rights and responsibilities of individuals and organisations, an erosion that is contrary to Australian jurisprudence and that places Australians further behind their overseas peers.

The proposal should be **rejected** by the OAIC.

Yours sincerely

Roger Clarke
Secretary, for the Board of the Australian Privacy Foundation
(02) 6288 6916 Roger.Clarke@privacy.org.au

Australian Privacy Foundation
Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, Committees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policy Statements https://privacy.org.au/policies/
- Policy Submissions https://privacy.org.au/publications/by-date/
- Media Releases https://privacy.org.au/media-release-archive/
- Current Board Members https://privacy.org.au/about/contacts/
- Patrons and Advisory Panel https://privacy.org.au/about/contacts/advisorypanel/

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) https://privacy.org.au/about/history/formation/
- Credit Reporting (1988-90) https://privacy.org.au/campaigns/consumer-credit-reporting/
- The Access Card (2006-07) https://privacy.org.au/campaigns/id-cards/hsac/
- The Media (2007-) https://privacy.org.au/campaigns/privacy-media/
- My Health Record (2010-20) https://privacy.org.au/campaigns/myhr/