# Making privacy core business

**Privcore Pty Ltd**

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000



Structural Reform Division
Treasury
Online submission

9 September 2019

Dear Treasury,

**Submission:**
**Consultation on the ACCC's Digital Platforms Inquiry Final Report**

## Introduction

Thank you for the opportunity to participate in the consultation regarding the ACCC's Digital Platforms Inquiry Final Report (the Final Report). This submission largely supports the recommendations of the ACCC, which have in part also been based on extensive work undertaken by many organisations and individuals over the last decade involved in privacy reform. The ACCC adds a weighty voice to these views and further advances the important privacy reform work needed. In particular, taking an economy-wide view is critical in a world where global supply chains are inter-connected and less complexity and greater consistency would be beneficial to all stakeholders.

Many companies operate globally today and geographic boundaries should increasingly be irrelevant when transacting with global brands online. Consumers don't want to be treated differently with lower standards just because of where they may be transacting/located in the physical world. This decreases trust in global brands.

Privcore's submission focuses on four foundational areas that would be helpful to clarify as part of the reforms. The four areas relate to:

- The definition of 'personal information', including inferences and its interpretation (recommendation 16a and 17)
- Access to 'personal information' and notice of collection, particularly in relation to indirect collection (in part recommendation 16b)
- Consent to the collection, use and disclosure of 'personal information' (16c)
- World-wide versus domestic percentage of turnover penalty option (recommendation 16f)

## About Us

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens.

Annelies Moens, CIPT, FAICD, CMgr FIML, a privacy professional practising since 2001 founded Privcore and is a former President of the International Association of Privacy Professionals which she co-founded. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She had the benefit of resolving hundreds of privacy complaints whilst working at the Australian privacy regulator and consults globally on privacy. Her bio is available at: www.privcore.com/bios.

## 1) The definition of 'personal information', including inferences and its interpretation

In its Final Report, the ACCC recommends updating the definition of 'personal information' in the *Privacy Act 1988* (Cth) (the 'Privacy Act') to clarify that it includes technical data such as IP addresses, device identifiers, location data, and other unique identifiers that may be used to identify an individual online or via their mobile devices (p.393).

The ACCC also states that: "the large amounts of information collected from consumers may not constitute 'personal information', such as personal information that has been de-identified or inferred information that does not relate to a specific, identifiable individual"(p.393) (even though harm may occur to individuals as a result of that inference (whether accurate or not) or re-identification).

Whilst the definition of 'personal information' in the Privacy Act is broad, it does not include a list of specific data points within the definition. The current definition is constructed in such a way, so that what constitutes 'personal information' in one context may not constitute 'personal information' in another context. A simple example of this is a photograph with individuals in it. In the hands of one entity that does not recognise any of those individuals and has no means to identify them, the photograph is not 'personal information'. However, that very same photo in another entity's hands may constitute 'personal information', for example if they know the individuals in the photo, or can easily verify one or more of those individuals through, for example, matching the face in the photo to a database containing facial images or checking online. As such, the definition of 'personal information' is not black and white and is context dependent.

The technical data items that the ACCC recommends be added to the definition are highly likely to already constitute 'personal information' under the current definition in the Privacy Act depending on the context. An IP address, in particular, on numerous occasions, foreign case law has held to be personal information; this is particularly so where the IP address is static and not dynamic. It is even described as personal information in the *Telecommunications (Interception and Access) Act 1979* (Cth)(see sections 187LA and 187AA (IP address being a source of communication).

Additionally, if you can target (or make contact with) an individual audience of 'one' (for example by providing a tailored advertisement to a unique device), even if you don't know who they are by name, arguably that would constitute 'personal information'. Apple, in its interpretation of personal information, puts it simply: "Personal information is data that can be used to identify or contact a single person" (p.408).

Spelling out explicitly that the growing variety of technical data are 'personal information' would avoid entities evading their privacy obligations due to the lack of specificity in the current definition and avoid the situation that arose in proceedings leading to the decision in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4. However, any redrafting of the definition should be mindful that when a data point in isolation (such as device identifier or IP address or location data) is explicitly defined as 'personal information', flow on implications to the access, correction and security/deletion principles should be considered. For example, how would an individual obtain access to that 'personal information', and how would an entity provide access to that 'personal information' without any other information?

<u>Inferences</u>

The ACCC also recommends that consideration should be given to whether the Privacy Act should offer protections for inferred information, especially sensitive inferences (p.476). There is limited discussion in the Final Report as to whether inferred information constitutes 'personal information'. As noted earlier, the current definition of 'personal information' is broad and inferred personal information would arguably come within that definition. There is nothing to suggest otherwise as long as that inferred information is about an individual. As such, the full set of privacy obligations would currently also apply to inferred personal information.

Indeed, inferred personal information arguably requires the greatest level of privacy protection. As the ACCC and others have pointed out, personal information can be collected in many different ways. The most obvious is direct collection from the individual whose personal information it is, the next is from a second or third party,

such as a data broker or a spouse giving information about their other half, the next is the collection of personal information that has been observed, such as through sensors or video surveillance. The final and most risky category is inferred personal information. The reason inferred personal information is the most risky is that it is the most removed from the individual to whom it relates. Therefore, its accuracy, ability for the individual to know that it has been collected and can be accessed/corrected is opaque to the individual to whom it relates. So these four collection methods sit on a continuum of increasing privacy risk (from directly collected (least risk), second or third party collected, observed to inferred (most risk)).

**Recommendation One:** If including specific technical data as personal information ensure that this does not sit in isolation and fits with existing requirements in the definition of 'personal information'. Clarify that inferences can be personal information where they fit within the definition of 'personal information'. These items would then be included in the definition (on a non-exhaustive basis).

## 2) Access to 'personal information' and notice of collection, particularly in relation to indirect collection

The ACCC in its Final Report does not discuss issues directly relating to access to personal information. This is important when considering reform to the definition of 'personal information' and also in relation to notice of indirect collection of personal information the ACCC recommends (p.461).

There is an increasing amount of indirect collection of personal information rather than direct collection of personal information from the individual whose personal information it is. The more personal information is collected from a second or third party, observed or inferred, the greater the privacy risks as compared to direct collection of personal information. Therefore, it becomes increasingly important that notice be given of those indirect collections of personal information.

This would then mean that individuals could also access that personal information to ensure accuracy, relevance and exercise greater control. One example is the purported 'shadow profiles' that Facebook collects on individuals who have no account on Facebook as discussed on page 416 of the Final Report. This personal information is not accessible to those who have shadow profiles, nor can deletion currently be requested.

Provision of notice of indirect collection of personal information is likely to challenge regulated entities. However, from an individual, privacy and consumer rights and risk management perspective this should be implemented.

**Recommendation Two:** Recognise that the method of collection of personal information directly impacts levels of risk to the individual and thereby regulate accordingly.

## 3) Consent to the collection, use and disclosure of 'personal information'

The ACCC recommends strengthening consent, as a way for individuals to make more informed decisions about how regulated entities collect, use and disclose their personal information. It also recommends that default settings be set in favour of preserving the privacy of the individual, so that for example opt-in consent is always required, rather than opt-out consent (so no pre-ticked boxes denoting consent) and that consents not be bundled. Unticked consent boxes and unbundled consents have always been the better privacy approaches from an individual perspective, but business and government don't often like to implement them.

The most notable example in Australia is the electronic health record to which every Australian has been effectively pre-ticked as consenting, unless they take specific action to "untick" and actively ensure they don't have such a record.

Default settings are extremely important, as whatever is the default position is what will be most commonly adopted. This is seen in studies in different economies globally. For example, a study conducted to show organ donation rates differing massively in Germany and Austria and other economies based on the default setting for being an organ donor (see E. Johnson and D. Goldstein, 'Do defaults save lives?' *Science*, Vol.302, 21 November 2003 pp.1338-1339).

With the ACCC recommending strengthened consent through requiring active opt-in consent and no bundling of consent, it is clearly proposing to shift the balance further to the individual for whom the Privacy Act is designed to protect and appears necessary.

It should be noted that consent is only one mechanism through which to collect, use and disclose personal information for other purposes, and has generally been a weak protection as it is an exception to the default position that personal information should not be used or disclosed for a purpose other than that for which it was collected. Also business and government often use consent to erroneously justify the over-collection, use and disclosure of personal information (see A. Moens, Privcore, 'Submission: Consultation on Artificial Intelligence, Australia's Ethics Framework - A Discussion Paper" May 2019).

### 4) World-wide versus domestic percentage of turnover penalty option

The ACCC notes that "closer alignment of Australian privacy regulations with the GDPR's higher standards of protection could significantly increase the effectiveness of Australian privacy law and increase the accountability of entities processing the personal information of Australian consumers" (p.439). It is not entirely clear why this would be the case, since whilst there are certainly some rights under GDPR that are non-existent under Australian privacy law, there are also requirements under Australian privacy law that are non-existent under GDPR. The main being that under Australian privacy law 'processors' are not provided with lesser/fewer privacy requirements (as compared to controllers) as this distinction does not exist under Australian privacy law. The widespread impact of GDPR has largely been due to its world-wide turnover penalty provisions and extra-territorial application. Australian privacy law also has extra-territorial application, but that impact is not felt as widely overseas as Australia is a relatively small market.

The introduction of greater penalties under Australian privacy law should presumably largely contribute to increasing the awareness of Australian privacy law, though not necessarily its effectiveness as this depends on many variables, including adequately resourcing the regulator and enforcement of the law. Economies that merely adopt equivalent GDPR legislation without enforcing, do not increase effectiveness of privacy for individuals.

The ACCC recommends that penalties under the Privacy Act should be increased to reflect the penalties under the *Competition and Consumer Act 2010* (Cth) – that is, whichever is the higher of:

- AU $10 million
- three times the value of the benefit received, or
- 10 per cent of the entity's annual turnover in the last 12 months, if a court cannot determine benefit obtained from the offence.

In some cases, this may exceed GDPR penalties where three times the value of the benefit received exceeds maximum GDPR fines and turnover which is based on historical information (preceding financial year turnover).

Increased penalties have been supported by the Government, in its announcement on 24 March 2019 of tougher penalties and other measures to protect Australians' online privacy and increased penalties for serious or repeated breaches to whichever is the greater of:

- AU$10 million,
- three times the value of any benefit obtained through the misuse of information, or
- 10 per cent of a company's annual *domestic* (emphasis added) turnover

which were based on the ACCC's Preliminary Report to this Inquiry.

Whether the turnover penalty option is based on previous year's domestic or world-wide turnover is worth clarifying. The EU has chosen penalties based on world-wide turnover, but it would appear the Australian Government has understood that the ACCC is recommending that the turnover penalty should be based on the regulated entity's *domestic* Australian turnover for the previous year. The annual turnover of the domestic arms of many large multinationals operating in Australia is minimal compared to their operations overseas.

The ACCC recently successfully argued in the Full Federal Court that when calculating the entity's annual turnover in the penalty provisions under the *Competition and Consumer Act 2010* (Cth), (which are recommended to be the same under the Privacy Act), all business activities of the defendant entity and its related bodies corporate connected with Australia should be taken into account (see *ACCC* v *Yazaki Corporation* [2018] FCAFC73 16 May 2018). Yazaki Corporation's special leave to appeal to the High Court was refused with costs on 19 October 2018.

**Recommendation Three:** Clarify the meaning of "10 per cent of the entity's annual turnover in the last 12 months" to include world-wide turnover.

## Conclusion

Data is core to all businesses and government agencies. Its exploitation and regulation needs to be carefully managed to ensure a trusted ecosystem and balanced bargaining positions. When imbalance strikes, the rules of the game inevitably shift. Privcore would be pleased to contribute to further discussions in targeted consultation meetings and to assist in the privacy reform agenda.