An article published in Privacy Unbound, the journal of the international association of privacy professionals Australia and New Zealand (iappANZ), March 2015

Lawyers each day grapple with shades of grey. English law is rightly sceptical of absolutes, moral or otherwise, or allegedly self-evident truths. Good judges seek to find standards for acceptable behaviour that accommodate the complexities of human sensibilities and the practicalities of everyday and business life. And so was born our ‘reasonable man’, more recently transgendered as a ‘reasonable person’.

If you work in privacy, then you are probably better friends with this person than you realise.

Getting to know the ‘reasonable man’

The ‘reasonable man’ had dubious antecedents in French enlightenment philosophy. After he crossed the English Channel, he rode the Clapham Omnibus before graduating to the Bondi Tram and the Shaukiwan Tram. Yes, the ‘reasonable man’ is indeed that person you were sitting next to on the tram or bus this morning – even if he was occupying an unreasonable amount of space.

His first English outing was back in 1837, in the case of Vaughan v. Menlove. Mr Menlove built a hay rick (or what we’d call a hay stack in this part of the world) near the boundary of his property, not far from Mr Vaughan’s cottages. Menlove was warned by Vaughan on several occasions that the rick could spontaneously ignite and therefore was a fire hazard. Menlove said that he had insurance and he would chance it. You guessed it, the hay ignited and burned down Menlove’s barns and stable and then Vaughan’s two cottages on the adjacent property. Mr Menlove’s attorney noted his client’s “misfortune of not possessing the highest order of intelligence” – never a problem nowadays - and argued that negligence should only be found if the jury decided Menlove had not acted with "bona fide [and] to the best of his judgment." The Court disagreed, stating that such a standard would be too subjective, and: “Instead, therefore, of saying that the liability for negligence should be co-extensive with the judgment of each individual, which would be as variable as the length of the foot of each individual, we ought rather to adhere to the rule which requires in all cases a regard to caution such as a man of ordinary prudence would observe.” A man of ordinary prudence – that’s our reasonable man.

Ordinary prudence was, of course, an articulation of a principle of sensible risk management long before international standards, operating manuals, OH&S and the Big 4 consultants’ methodologies. And so English law jumped headlong into assessment of risk and finding the right (objectively ascertained) shade of grey for the particular circumstances of each case – or judging things ‘in the round’, as modern privacy practitioners like to say.

Is it personal information? What would the reasonable man say?

We start ‘in the round’ grappling with whether a person is ‘reasonably identifiable’. Most Aussie privacy professionals can recite by rote that personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable (whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not). Whether a person is ‘reasonably identifiable’ clearly requires an exercise of objective judgement about how unlikely it is that an individual’s identity could be ascertained from the information or opinion.

Privacy law does not give us guidance as to the appropriate, objective standard to apply, so it is impossible to definitely state where on the continuum between completely unidentifiable and readily identifiable that we find the point where an individual is ‘reasonably identifiable’. There is no stated standard, such as balance of probabilities, to help us find that point. Sometimes words such as ‘low’ or ‘remote’ are used, but these words don’t help much. This is largely because the practical problem
is actually not defining a point on a continuum at which a possibility can be conveniently found to sit on one side or the other, but assessing a risk. Assessing risk requires a fact-specific enquiry as to what information sources might be available to the person that is dealing with the information in question that might be used to match against or otherwise analyse information about a nominally unidentified individual in order to work out the identity of that person.

In assessing risk ‘in the round’, it seems sensible to follow the lead of the UK Information Commissioner’s Office and the Australian Privacy Commissioner and to have regard to all relevant circumstances surrounding the handling of the relevant information. These circumstances include who has access to it and what safeguards – technical, operational or contractual – are deployed to ensure that purportedly de-identified information is properly protected from re-identification risk. And this is why the discussions that you sometimes see around whether particular types of information are personal information can be sterile debates. Take IP addresses. It depends upon who has the IP address and what capability or inclination they have to match it back to an individual associated with an internet access service to which that IP address was allocated at a particular time. All that can be said as a universal statement is – it depends who has the information and access to other relevant information.

Are our systems good enough? Back to the reasonable man

In recent times, a new brand of risk management consultants has sprung up, selling implementation of standards and proprietary frameworks and methodologies for privacy risk management. For all their strengths in cataloguing sources of risk and mechanisms for risk management and mitigation, these standards, frameworks and methodologies tend to go a bit flabby and vacuous at the point at which we seek to apply the risk assessment generated through their application to everyday processes in dynamic business environments. Having systematically catalogued data flows and information handling processes, how are the risks that we identify to be quantified and weighted? How does a business satisfy itself, its clients and prudential and privacy regulators that the business has effectively quarantined and managed uses of de-identified information at an appropriate level of assurance that this information is properly protected from re-identification risk? What would the reasonable man say?

Any qualification from absolute assurance of persistent de-identification in all hands leads to easy point scoring by some privacy advocates. These advocates point to any possibility of re-identification in some hands – for example, even if proper risk mitigation processes within a corporation handling anonymised information are verifiably implemented and followed but then are breached, for example, through employee oversight – as grounding a conclusion that the purportedly de-identified information should be treated as personal information. Of course, risk mitigation measures must take account of frailties and errors of humans, the devious ingenuity of malicious hackers, the recalcitrant contractors, and so on. But how do you apply a word like ‘low’ or remote’ to work out whether and when you are jumping at shadows?

Heads in the round or in the clouds?

Occasionally the law itself strays into loose use of binary concepts. For example, the Privacy Commissioner’s Guidelines as to ‘disclosure’ reasonably (that word again) inform us that “an APP entity discloses personal information when it makes it accessible to others outside the entity and releases the subsequent handling of the personal information from its effective control” (B.58). Examples provided include where an APP entity “publishes personal information whether intentionally or not and it is accessible to another entity or individual” or “displays a computer screen so that the personal information can be read by another entity or individual” (B.60). When discussing offshore disclosures, the Privacy Commissioner’s Guidelines state that in “limited circumstances providing personal information to an overseas contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. In these circumstances, the entity would not need to comply with APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a ‘use’ by the entity’(B.13).
So what are these “limited circumstances”? The Commissioner states three requirements. First, a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes. Second, the contract requires subcontractors to agree to the same obligations. Third, the contract gives the entity effective control of how the personal information is handled by the overseas recipient. “Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.”(8.14).

The Privacy Commissioner, in my view rightly, doesn’t express a definitive view as to whether any form of controlled view-only access by the contractor would constitute a disclosure by the customer to the contractor rather than a use by the customer.

The example given in the different context of disclosure when a person “displays a computer screen so that the personal information can be read by another entity or individual” is not directly in point, because it is not clear in that case whether the disclosure arose through the viewing being facilitated without effective control – in effect, the information becoming accessible to all passers-by - or because the viewing was possible at all. Some privacy lawyers point to Europe and say the answers here would be much simpler if the Privacy Act incorporated the EU concept of ‘processing’, which covers just about anything you can do with personal information. Viewing personal information amounts to processing and hence is regulated, so whether something is a use or a disclosure doesn’t need to be asked or answered.

Back here in this part of the world, a sensible, risk management interpretation of the law would be that effective controls may mitigate risk to the point where there is no ‘disclosure’ because the risk of an act or practice contrary to the Act is too low or remote. But this practical view does bump up against the binary nature of the word ‘disclosure’ as in common usage. It is reasonable to say that if you disclose something to me, I know it and I could potentially use it or tell someone else regardless of whether I said I wouldn’t tell anyone else. This absolute or binary interpretation of the word ‘disclosure’ is easy to support both by reference to dictionaries and our memories of adolescent playgrounds. However, it does not readily facilitate a sensible risk management interpretation. So to give the word ‘disclosure’ an appropriately nuanced, sensible risk management interpretation, the Privacy Commissioner is forced to narrowly squeeze the natural meaning of disclosure. This is not tricky or wrong, but it is a case of using fencing wire to fashion a workable tool out of an inherently binary concept that the Parliament and the Parliamentary Drafters should not have left for the Privacy Commissioner and the hapless privacy professional to work out or around.

Sensible application of risk management principles to evaluate the effectiveness of technical, operational or contractual safeguards will often lead to controversial and sometimes uncertain conclusions. But this doesn’t mean that privacy law is loose or unpredictable. It just means that we continue to adapt concepts of reasonableness now nearly two hundred year old, but now applying new methodologies for systematic thinking about risk and its mitigation. It’s enough to turn you grey.

Peter Leonard heads Gilbert + Tobin Lawyers Data and Content Practice and is a director of iappANZ.