Consultation with Dr Joel Scanlan, Senior Lecturer within the Australian Institute of Health Service Management (AIHSM)

[Accuracy of notes confirmed by Joel Scanlan via email 28/07/2023]

4 July 2023, UTAS Law Building Meeting Room

Rebecca Bradfield and Yvette Maker attending

We discussed JS's privacy preference. JS subsequently confirmed via email that he is happy with a public submission.

- Regulation helps with information management – organisations think that collecting more data is valuable.
- IT people prefer to be in a heavily regulated industry. Collection of private information is analogous to 'toxic waste' and seeing breaches raises the question of why some of this information has been collected in the first place.
- We need to adopt the right to be forgotten as they have in Europe, with deletion after X number of years.
- Bigger fines have not been actioned yet in the EU – will they be tested?
- One problem is that companies are not accountable for not patching.
- Good regulation means protecting citizens.
- There have been good intention regarding transparency in the EU but it has gone a bit weird (e.g. cookie disclosures) – does increase the right to object but it is a bit broken.
- The other piece is education – regulation is at least forcing awareness on companies to be aware and justifying why they're collecting data.
- Don't think anyone's got this right, not sure what right looks like.
- It is possible for us to jump in front – anyone can.
- There is a cost for companies to delete old data.
- Even the right to be forgotten puts the onus on the customer.
- Data linkage is an interesting question – don't have an answer on that.
    - E.g. 'dark profiles' where you don't login but the site knows you've visited four times, etc.
    - These are really hard questions.
- Simplicity matters.
- With notification of data breach stuff (28-30 days to notify) – there's a simplicity to that.
- The APP is a list of fairly understandable principles.
- It needs to be readable, you shouldn't need a lawyer to understand how long you can keep data for.
- Generally it would be good to have a right to privacy enshrined in law, but how it's defined, how much privacy, is complex.
    - Organisations' perception of the value of data varies. Sometimes it could be about value to sell. Not everyone is doing that, but may think 'we'll use this data somehow in future' (whether with AI or otherwise). It's more like perceived possible future value. That's where the culture needs to change – they should have to justify a need for it now. There are advantages to a 'hammer' – if you don't need it, this is the liability you're taking on. If fines are larger and not related to profit, e.g. a percentage of annual global revenue as in the EU, that should be more effective. The intention with notification of data breach is that disclosing gets you out of the fine.

- The GDPR came in after the Australian NDB scheme – could see notification of data breach was a good change but could already see not as good as the EU.
- Consistency across jurisdictions is something to consider. Misalignment across country lines is more noticeable – what if it's a UK, French etc citizen in Australia? Those complexities are also worth considering. Can still cop a fine if data on an EU citizen is stored here.
- In the health context we see varied perspectives in how much experts are concerned, compared to the financial space where we all have similar views.
    - Support/protection of some 'vulnerable' people is important here.
    - Co-design is needed, not just talking to clinicians.
    - There is a question of whether biometric data counts as health.
- There are misuse possibilities with face recognition and gait, which can be captured very easily.