Summary

- Chapter 2 – I am concerned about location and wish to see it classified as sensitive information
- Chapter 2 – I believe biometric information that cannot be changed should be classified as sensitive information
- Chapter 11 – I think the introduction of restricted and prohibited practices is both necessary and desirable
- Chapter 11 – APP entities should bear the responsibility of restricted practices accountability y measures
- Chapter 11 – the Commissioner should be issuing guidelines on prohibited and restricted practices
- Chapter 15 – yes there should be a right to erasure
- GDPR Adequacy
- Chapter 22 – GDPR Adequacy is a goal Australia should pursue

Chapter 2 - Personal information, de-identification and sensitive information

On page 33 there is a discussion on sensitive data and the paper asks:

- What would be the benefits and risks of amending the definition of sensitive information, or expanding it to include other types of personal information?

With regard to location data and its sensitivity. I strongly support updates to the legislation that clearly signal location is sensitive information. From my own experience in the field of technology (previously CTO of a startup concerned with location) I see have professional experience of this issue and the disconnect many businesses have with the power of this type of data. The issue of misuse of location and just how powerful location is as data can be seen here:

- https://www.theregister.com/2020/05/19/bellingcat_beer_app_osint/ - national security interests compromised by beer app
- https://au.pcmag.com/security/91283/car-thieves-are-using-airtags-to-track-vehicles - car thieves using retail location devices to track victims
- https://www.abc.net.au/news/2020-11-24/domestic-violence-report-shows-increase-in-online-abuse/12911926 - report showing a marked increase in the use of GPS devices in domestic violence cases
- https://www.theregister.com/2021/08/31/guntrader_breach_csv_danger/ - a gun trading website lost its data. Providing its attackers with detailed locations of UK firearms

Note here that the misuses of the location data above require tiny amounts of data (i.e. a single location is enough to trigger the harm) and work across long periods of time. Therefore, I would ask that location be included in the definition of sensitive data.

In the same vein:

- What further information or guidance would assist APP entities when classifying biometric information, biometric templates or genetic information as 'sensitive information'?

I have less experience of working with biometric information professionally but I would suggest that in terms of biometric information there is a clear distinction between that which is changeable and that which is not. For instance, details of my haircut are biometric information. They relate to my body but are easily changed. Take that against my fingerprints, which I cannot change without surgery. There lies a line which is distinct and purposeful. If it's difficult/impossible to remedy a data breach concerning my biometric data then it is clearly sensitive information.

Chapter 11 – Restricted and Prohibited Practices

- Would the introduction of specified restricted and prohibited practices be desirable?

I think the introduction of restricted and prohibited practices is desirable. There are three reasons for this in my opinion:

1. It's clear we're undertaking increasingly complex and impactful decisions with computers as a society. For instance https://www.penguinrandomhouse.com/books/241363/weapons-of-math-destruction-by-cathy-oneil/ is a good overview of the situation in the US. And points us to things that are both close at hand and worrying (for instance teacher evaluation) in the Australian context. Until we're clear that using computers to evaluate human performance improves our lives we should at the very least regulate the data collection that allows such computing to be possible.
2. The lack of technical understanding in society of the consequences and pitfalls of computing means that Australians are hard-pressed to make good decisions about their computing security. In the report https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 "often poor cyber security controls… allowed cybercriminals to launch their attacks with minimal targeting effort or technical expertise". The Australian government therefore provides an important protection for its citizens in limiting both the data collected about individuals and the use of that data.
3. We are simply not in an age of computing where security is robust and ubiquitous. Notably we are unable to verify the correctness of software nor are we able to definitively assert that software is invulnerable to certain classes of attack. Simply put computing (and software in particular) is not equivalent to engineering.

Regarding the question:

- Should restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures, or should individuals be provided with more opportunities to self-manage their privacy in relation to such practices?

For pretty much the same reasons as outlined above I believe that pushing the responsibility of making good privacy and security decisions onto individuals is currently untenable. Organisations have the resources, time and ability to undertake accountability measures. Individual users do not have that same ability.

Finally on this section:

- Should prohibited practices be legislated in the Act, or developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?

My input would be to chose the Commissioner-issued guidelines approach. For two reasons:

1. That saves the parliament of Australia having to weigh the impacts of at times deeply technical discourse with regard to privacy. Which would inhibit the desire to adapt the act to the changing nature of the threats we face. In turn that would leave the legislation to be flat-footed and therefore less likely to achieve and retain GDPR adequacy.
2. The danger in much privacy thinking is the novel linkage of data. That a particular datum which is benign becomes a threat once it is linked to other data. Again that kind of issue is not the standard stuff of law, which is inherently less mutable. The commissioner is able to judge the changing nature of the privacy landscape and therefore the correct course of action in a fluid environment.

Chapter 15 - Right to erasure of personal information

- In light of submitter feedback, should a 'right to erasure' be introduced into the Act?

Yes absolutely. If I cancel a contract or otherwise cease a relationship with an organisation, I don't expect that organisation to keep using my data to its advantage. We've ceased our relationship. Therefore, I want the right to be removed from that organisation's systems.

Chapter 22 – Overseas Data Flows

On page 166 there is a discussion around the benefits and costs of achieving GDPR adequacy. As I wish to run businesses that can compete globally I believe achieving GDPR adequacy is a significant and laudable goal for Australia. I would strongly support progress in this direction.