Australian Human Rights Commission

How expanding ecosystems risks consumer rights to privacy in the Metaverse

Australian Human Rights Commission

Submission to Australian Competition and Consumer Commission: Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers

05 April 2023

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Contents

1 Introduction

1. The Australian Human Rights Commission (Commission) welcomes the opportunity to make this submission to the Australian Competition and Consumer Commission's (ACCC) Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers issue paper (Issues Paper) as part of the Digital platform services inquiry 2020–25 (Digital Platforms Inquiry).
2. The role of the Commission is to work towards an Australia in which human rights are respected, protected and promoted. While the Commission has expertise and knowledge in the area of human rights generally, relevant to this Issues Paper, it has also developed specific expertise with respect to the human rights risks posed by digital technologies. Most recently, this can be seen in the Human Rights and Technology Project, which was a three-year, national investigation that culminated with the release of the Human Rights and Technology Project Final Report in 2021 (Final Report).
3. This submission builds on the previous work that the Commission has done to advocate for human rights-centred design and deployment of new and emerging technologies, and demonstrates a commitment to global leadership in respect of human rights in digital spaces.
4. The Commission has continued its work in 2023 on human rights and technology. This submission is in addition to other 2023 submissions to date, including to the:
    - Select Committee on Foreign Interference through Social Media
    - Targeted Review of Divisions 270–271 of the *Criminal Code Act 1995* (Cth) (in respect of technology facilitated crime)
    - Attorney-General's Department Review Report on the *Privacy Act 1988* (Cth)
5. The Commission welcomes further opportunities to provide a submission to the ACCC's Digital Platforms Inquiry – but notes that this submission addresses only question 11 posed in the Issues Paper. This is not indicative of the relative importance of the particular question compared to other questions raised in the Issues Paper. Rather, it reflects the Commission's relevant expertise in certain areas, and current capacity.

2 Definitions

6. The Issues Paper specifically refers to the internet of things (IoT). Throughout this submission we have adopted the same definition for this term.[1] IoT

means: 'The use of internet-connected technology in physical devices that have not traditionally featured such technology, such as cars, household appliances and speakers. This allows these devices to collect, share and make use of data.'

7. This submission considers consumer risks to privacy in the Metaverse as a key example of the potential harms arising from the evolution and expansion of digital ecosystems.

8. The Metaverse is not defined in the Issues Paper. For the purposes of this submission the Commission draws upon the definition provided by the XR Safety Initiative.

> 'The Metaverse is a network of interconnected virtual worlds with the following key characteristics: Presence, Persistence, Immersion and Interoperability. Metaverse is the next iteration of the internet enabled by several converging technologies such as Extended Reality (XR), Artificial Intelligence (AI), Decentralised Ledger Technologies (DLTs), neuro-technologies, optics, bio-sensing technologies, improved computer graphics, hardware, and network capabilities.
>
> Metaverse has four main aspects; presence, persistence, immersion and interoperability. Presence is the feeling of being present or physically located within a digital environment. Through stimulating realistic sensory experiences and enabling participants to interact with objects and other participants, it creates a sense of immersion and engagement within the virtual world, as if participants were in the same physical space. The sense of presence is carried out through technologies such as virtual reality glasses. Persistence refers to the ability of virtual objects, environments, and experiences to assist over time, even when participants are not actively interacting with them. It allows participants to make progress, own virtual property, and build ongoing relationships. Immersion refers to the degree to which a participant is fully engaged and absorbed in a virtual environment, to the point where the individual may forget about their physical surroundings. A sense of immersion is created through technologies such as virtual reality (VR) headsets, haptic feedback devices, and 3D audio. Interoperability refers to the ability of different virtual worlds and systems to communicate and interact with each other seamlessly, allowing individuals to move freely between different digital environments and experiences. It is essential for creating a cohesive and interconnected virtual world that allows individuals to seamlessly move between different experiences and platforms.[2]

9. The Metaverse also requires various technologies and ecosystems for interaction between the physical world and the Metaverse – for example

artificial intelligence (AI), computer vision, 5G/6G, IoT and robotics.[3] However the Commission notes that any definition of the Metaverse is fundamentally nebulous, as the technology is constantly evolving and morphing in both function and application.

3 Question 11

What types of potential consumer harms have arisen from these providers of digital platform services expanding their ecosystems?

10. The proliferation of data collection and usage by the providers of digital platform services expanding their ecosystems raises human rights concerns. Increasing interoperability and expanding ecosystems is amplifying human rights risks for all consumers in Australia. Organisations such as Alphabet, Amazon, Apple, Meta and Microsoft all operate in data-driven markets.[4] How these organisations collect, maintain and utilise consumer data is of the utmost importance in protecting the human rights of consumers.
11. The risk profile is exacerbated by expanding ecosystems into new products, sectors or technologies (such as the Metaverse).[5] Such new and emerging technologies provide organisations increased opportunities to accumulate and utilise the personal information of consumers.[6]

3.1 The human right to privacy

12. This proliferation of data collection and usage poses a significant risk to consumers' rights to privacy. The right to privacy developed over centuries. For example, in the fourth century B.C.E Aristotle drew the distinction between the public sphere of politics and the private sphere of domestic life. Thousands of years later, the 'fourth industrial revolution' is characterised by rapid technological development and expanding digital ecosystems. These changes have arguably reinforced the central importance of the right to privacy.
13. The right to privacy is protected under Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) and Article 12 of the *Universal Declaration of Human Rights* (UNDHR).
14. The Commission's recently launched Position Paper: A Human Rights Act for Australia (Position Paper) specifically recommends the inclusion of a 'right to privacy and reputation' in the proposed Australian Human Rights Act.[7] The proposed inclusion of a positive right to privacy and reputation demonstrates the importance of the right to privacy in the digital age – especially in relation to the collection and usage of personal data.[8]

15. The right to privacy is a cornerstone human right. It also underpins freedoms of association, thought and expression, as well as freedom from discrimination.[9]

3.2 How expanding ecosystems risks human rights

16. Vint Cerf, Vice President and Chief Internet Evangelist at Google, once stated that 'privacy may actually be an anomaly'.[10] The recognised challenges to privacy protection are magnified in light of expanding interoperability and data sharing.

17. The Issues Paper states that the services provided by large providers of digital platforms are 'an integral part of modern society'.[11] However, to utilise these staples of modern living, consumers are required to relinquish vast amounts of personal information and data. The notion that participation in modern living should come at the expense of privacy can lead to human rights violations and harm.

18. By way of example, misuse of geolocation data – which violates not only the right to privacy, but may also provide the basis for unjustified discrimination and risk the safety of individuals. In 2020, consumer insight firm Mobilewalla released a report that used phone location data secretly collected during the Black Lives Matters protests. The firm buys mobile phone data and, at the time the article was published, had 80–90% device coverage in the United States (US).[12] The report published age, gender, ethnicity and location of attendees at Black Lives Matter protests in 2020. While this report is no longer available online, its publication highlights the potential misuse of location data.[13]

19. There are also reports that the same company also used geolocation tracking data to determine how frequently people attended evangelical churches in the leadup to the US election.[14] That information was then used to tell voters classified as 'evangelicals' to vote, if their phone hadn't been 'seen' near a polling place on election day.[15]

20. The ACCC consumer survey showed that 86% of respondents considered such offline location and movement monitoring, without consent, a misuse of personal information.[16]

21. The above example provides an insight into the pervasiveness of data collection and abuses of privacy only in respect of geolocation data. There are many other examples which highlight the human rights risks associated with how data is already being used, and potentially misused.

22. Expanding ecosystems will only exacerbate potential harms in conjunction with the 'mosaic effect' –when organisations gather seemingly small and

innocuous pieces of personal information which, on their own, provide no great insights about a consumer. However, these small pieces of data, accumulated, provide detailed profiles about consumers.[17]

23. The Issues Paper notes that several providers of digital platform services have created 'extensive digital platform ecosystems of interrelated and interconnected services, often in data-intensive sectors, expanding their reach and impact on both the global and Australian economy'.[18] These expanding services facilitate the collection and sharing of even greater amounts of consumer information. This will allow organisations to collate vast amounts of small pieces of information to create more detailed profiles than ever before. However, with the rise of the Metaverse, these pieces of information become much more personal and qualitative.

3.3 Privacy in the Metaverse

24. This submission focuses on privacy in the Metaverse in respect of question 11.

25. While the Commission has raised previous concerns about the erosion of privacy in digital spaces,[19] the expansion of digital platform services into the Metaverse creates an unprecedented risk to consumers' privacy and data. The risk of privacy and security invasions in the Metaverse (inherited from underlying technologies or emerging from the new digital ecology) may be prolific.[20]

26. The Metaverse is a nebulous digital construct which is constantly evolving – but broadly speaking it can be considered as the next generation of the internet with the aim to be a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space for humans to play, work, and socialize.[21] This allows individual users to live as 'digital natives' and experience an alternative virtual life,[22] while at the same time have the ability to facilitate transactions and activities that also have a presence in the physical world.

27. In the Metaverse, consumers face a wide range of privacy intrusions and security risks, including:

    - the management of massive data streams
    - pervasive user profiling activities
    - unfair outcomes of AI algorithms
    - safety of physical infrastructures and human bodies.[23]

28. The personal data involved in the Metaverse will likely be 'more granular and unprecedentedly ubiquitous to build a digital copy of the real world'.[24] The fusion of this granular data collected by Metaverse technologies and more

traditional data collected by social networking platforms may compromise consumer privacy at heightened levels. Such a fusion, or interoperability of data, may create unpredictably deeper data profiles about consumers.[25]

29. For example, most social media platforms collect, maintain and utilise consumers' metadata – including a consumer's family members, colleagues, locations visited and future plans that users do not directly share.[26] However, Metaverse services will be data intensive and will undoubtedly generate new forms of personal profiling data to deliver a seamlessly personalised service to consumers.[27] To allow consumers to interact immersively via an avatar, Metaverse technologies will also require consumer profiling at an unprecedented granular level (including facial expressions, eye and hand movements, speech patterns and even brain waves).[28] For a consumer to engage in these digital spaces, they must do so via a representation realised through their own personal information.[29]
30. The Metaverse collects and processes vast amounts of data such as:
    - biometrics
    - facial expressions
    - eye movements
    - iris movements
    - hand movements
    - speech
    - brain wave patterns
    - habits
    - choices
    - activities of users
    - behaviours
    - feelings
    - expressions
    - user conversations
    - internet history
    - body movements
    - cultural data
    - financial data
    - communications

- location
- age
- shopping preferences
- favourite movies
- identities
- medical data
- digital assets
- the identity of virtual items
- cryptocurrency spending records
- physiological data
- physical data.[30]

31. Even the motion sensors and cameras usually built into virtual reality helmets, which help track head direction and movement, will draw consumers' rooms and monitor those spaces while being used.[31]
32. The collection of such vast and intrusive information will undoubtedly bring into question the protection of:
    - personal data in the Metaverse, such as digital assets
    - the identity of virtual items, and cryptocurrency spending records can be disclosed
    - interactions between consumers and the Metaverse, which can be leaked
    - consumers may be profiled according to their habits and preferences
    - some attacks such as eavesdropping in communication may be performed, and in addition, data storage may be hacked and its content disclosed
    - privacy laws in the real world may not be accountable in the digital world
    - behavioural data, which is more valuable than classical personal data since it defines how a person acts
    - privacy of consumers may be broken by authorities and governments for unsavoury purposes.[32]
33. The privacy concerns of Metaverse technologies are well noted as disclosure or use of such information can expose consumers to:
    - discrimination

- loss of reputation
- exclusion from society
- unfair treatment
- marginalisation of certain groups.[33]

34. Data interoperability between just two digital spaces – such as traditional social media and Metaverse spaces – creates more intimate consumer profiles. The addition of, for example, the expansion of IoT further expands the range of data available. Privacy risks in the Metaverse are considerable, due to the intimate data collected about consumers – which is more detailed than consumer conversations (such as via social media) or internet history.[34] The fusion of data gathered by the Metaverse and social networking platforms provides data holders the ability to extract incredibly sensitive information about a consumer, with the risk that it may then be misused.[35]

35. While the Commission is worried about how this data may be used by private organisations and public entities (such as government) and the associated risks to privacy, there is also great risk to consumers in terms of their data potentially being compromised via cyber-attacks.[36] In an ever-expanding digital ecosystem, where systems have data interoperability, such data breaches could have severe consequences for consumers in the real world, with no remedies available to undo leaks or the misuse of private information. This is in addition to the risk to consumers of 'doxing' (the publishing of private identifying information with malicious intent), spying and stalking.[37]

3.4 Privacy paradox

36. Despite these risks, the Commission worries that consumers will continue to undervalue their right to privacy in order to engage in modern living. This is supported by the 'privacy paradox'.

37. The privacy paradox refers to research revealing that despite consumers having a high perception of privacy risks, this has no obvious influence on their purchasing behaviours.[38] For example, 74% of Australian consumers have safety concerns in relation to being targeted by products or services.[39] A further 76% consider it is unfair when personal information is used to make predictions about them, while a further 85% consider it is unfair or very unfair for their personal information to be shared with other companies.[40] Despite being aware, and disapproving of, those risks to privacy, consumers are very often unwilling (or unable) to stop using appliances or services – despite their privacy concerns.[41]

38. This reluctance or inability to stop using products or services which threaten privacy may be, in part, a result of a lack of effective competition. As the ACCC notes, such a lack of competition and availability of reasonable alternatives can lead consumers to accept undesirable terms of use.[42] Moreover the Commission considers that even where consumers are aware of the risks, they are often powerless to protect their data.

39. While many models of regulation in the privacy and data space place great emphasis on 'choice' as an effective safeguard for consumer data and privacy,[43] consumers often have very little ability to 'choose' services and products which enable modern living without risking their privacy. The privacy paradox and numerous behavioural studies, have also demonstrated that placing the onus on consumers to protect their own data is insufficient.[44]

40. Such onus-heavy models also do not acknowledge the substantial power difference between large companies and individual consumers. Even where an individual understands how their data will be used, this power imbalance remains as 'one party controls the design of applications and the other must operate within that design'.[45] The ACCC has found that terms may be provided on a 'take-it-or-leave-it' basis across interrelated services, which leads to excessive data collection inconsistent with consumer wishes.[46]

41. Many consumers may not even understand how their data will be used, or the effect it may have on their privacy. Research has shown the emergence of 'dark patterns' which confirms the use of manipulative and deceptive designs cause consumer harm.[47] This can lead to Australians losing control of their data, or being manipulated into making choices which are not in their interests.[48]

42. Even where individuals do not genuinely understand how their data is being used, they will still disapprove of its misuse. Individuals have been shown to often have a very strong negative reaction when confronted with the difference between:

    - the reality of how their data is being used versus
    - their perception of how their data is being used.

43. This is particularly the case where the difference between reality and expectation becomes explicit and too contrasting.[49] The Cambridge Analytica Data Scandal provides an apt example. Many consumers willingly shared data on Facebook, however when the use of that data by Cambridge Analytica came to light there was public outcry, leading to Facebook being called to hearings before both the US congress and UK Parliament.[50]

44. The privacy paradox, illusion of choice and power imbalances may all contribute to consumers being realistically unable to engage in modern living

without relinquishing their privacy (even where they are wary of the risks to their personal information). This issue is heightened as digital service providers expand their ecosystems (especially in respect of the Metaverse). Without greater scrutiny of expanding ecosystems and data interoperability, especially in the Metaverse, consumers face increased risks to their privacy and human rights.

45. Without greater legislative protection for consumers, expanding ecosystems with increased data interoperability will potentially lead to increased risks of discrimination and violations of the right to privacy and freedom of expression. However, the Commission does note that the Attorney-General's Department is currently reviewing the *Privacy Act 1988* (Cth), with the aim of reforming Australia's privacy framework to meet '[t]he challenge of realising the benefits of data-driven technology while protecting individuals' privacy'.[51] Ensuring the protection of human rights (such as the right to privacy) should be a key priority for all policies and reforms in this area.

Endnotes

[1] Australian Competition and Consumer Commission ('ACCC'), '*Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers*' ('Issues Paper') (Commonwealth of Australia, Issues Paper, March 2023) 18.
[2] See XR Safety Initiative, 'The Metaverse' (website) https://xrsi.org/definition/the-metaverse
[3] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 81 citing Lik-Hang Lee, et al., 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' 2021 *arXIV*.
[4] ACCC, 'Issues Paper' (Commonwealth of Australia, Issues Paper, March 2023) 5.
[5] ACCC, 'Issues Paper' (Commonwealth of Australia, Issues Paper, March 2023) 7 citing ACCC, *Digital Platform Services Inquiry Fifth Interim Report* (Commonwealth of Australia, Firth Interim Report, 11 November 2022) 35.
[6] See generally Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 80-81.
[7] Australian Human Rights Commission ('AHRC'), 'Free & Equal Position Paper: A Human Rights Act for Australia' (Position Paper, 07 March 2023) 111 & 347.
[8] See especially AHRC, 'Free & Equal Position Paper: A Human Rights Act for Australia' (Position Paper, 07 March 2023) 111 in respect of the "note" contained within the right to privacy and reputation.
[9] Office of the Australian Information Commissioner ('OAIC'), '*What is Privacy?*' *https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy*.
[10] Jacob Kastrenakes, 'Google's chief internet evangelist says 'privacy may actually be an anomaly'' *The Verge* (online, 21 November 2013) https://www.theverge.com/2013/11/20/5125922/vint-cerf-google-internet-evangelist-says-privacy-may-be-anomaly.
[11] ACCC, 'Issues Paper' (Commonwealth of Australia, Issues Paper, March 2023) 2.
[12] Zak Doffman, 'Black Lives Matter: US Protesters Tracked by Secretive Phone Location Technology', *Forbes* (online, 26 June 2020) https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=6eeb5fa84a1e.
[13] Zak Doffman, 'Black Lives Matter: US Protesters Tracked by Secretive Phone Location Technology', *Forbes* (online, 26 June 2020) https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=6eeb5fa84a1e.
[14] Lorenzo Franceschi-Bicchierai, 'Firm That Tracked Protesters Targeted Evangelicals During 2016 Election', *Vice* (online, 27 June 2020) https://www.vice.com/en/article/9353qv/mobilewalla-tracked-protesters-targeted-evangelicals-during-2016-election.
[15] Lorenzo Franceschi-Bicchierai, 'Firm That Tracked Protesters Targeted Evangelicals During 2016 Election', *Vice* (online, 27 June 2020) https://www.vice.com/en/article/9353qv/mobilewalla-tracked-protesters-targeted-evangelicals-during-2016-election.
[16] ACCC, '*Consumer Views and Behaviours on Digital Platforms*' (Commonwealth of Australia, Final Report, November 2018) 21.
[17] AHRC, '*Human Rights and Technology Final Report 2021*' (Final Report, 01 March 2021) 115 citing David Pozen, 'The Mosaic Theory, National Security, and the Freedom of Information Act' (2005) 115 *Yale Law Journal* 628.
[18] ACCC, 'Issues Paper' (Commonwealth of Australia, Issues Paper, March 2023) 2.

[19] See generally AHRC, Submission to *Attorney-General's Department Privacy Act Review Report* which is currently unpublished.
[20] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 319.
[21] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 319.
[22] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 319.
[23] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 320.
[24] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 320; see also Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 82.
[25] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 84.
[26] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 81 citing Anniki Puura, Siiri Silm & Anu Masso, 'Identifying relationships between personal social networks and spatial mobility: A study using smartphone tracing and related surveys' (2022) 68 *Social Networks* 306-317.
[27] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 328.
[28] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 334.
[29] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 80.
[30] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 84.
[31] Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 334.
[32] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 84.
[33] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 80.
[34] See generally Sang-Min Park & Yung-Gab Kim, 'A Metaverse: Taxonomy, components, applications, and open challenges' (2022) 10 *IEEE Access* 4209- 4251.
[35] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 82 citing Roberto Di Pietro & Stefano Cresci, 'Metaverse: Security and Privacy Issues' *Trust, Privacy and Security in Intelligent Systems and Applications Third IEEE International Conference on TPS-ISA* (Conference Paper, 2021) 281-288.

[36] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 81.
[37] Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 82 citing Roberto Di Pietro & Stefano Cresci, 'Metaverse: Security and Privacy Issues' *Trust, Privacy and Security in Intelligent Systems and Applications Third IEEE International Conference on TPS-ISA* (Conference Paper, 2021) 281-288.
[38] Li Li, et al., 'I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem' (2023) 128 *Computers & Security* 1.
[39] Consumer Policy Research Centre, '*2020 Data and Technology Consumer Survey*' (Survey, December 2020) 33.
[40] Consumer Policy Research Centre, '*2020 Data and Technology Consumer Survey*' (Survey, December 2020) 26.
[41] Li Li, et al., 'I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem' (2023) 128 *Computers & Security* 1.
[42] ACCC, 'Issues Paper' (Commonwealth of Australia, Issues Paper, March 2023) 7 citing ACCC, *Digital Platform Services Inquiry Fifth Interim Report* (Commonwealth of Australia, Firth Interim Report, 11 November 2022) 44.
[43] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 4 citing Anthony Nadler & Lee McGuigan, 'An impulse to exploit: the behavioral turn in data-driven marketing' (2018) 35(2) *Critical Studies in Media Communication* 151-165.
[44] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 4.
[45] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 10 citing Jack Balkin, 'The fiduciary model of privacy' 134(11) *Harvard Law Review Forum* (2020) 12.
[46] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 7-8.
[47] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 7-8 citing Consumer Policy Research Centre, '*Duped by Design – Manipulative online design: Dark patterns in Australia*' (June 2022) 6.
[48] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 7-8.
[49] Lik-Hang Lee, et al., 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' (2021) 37 *arXIV*.
[50] Lik-Hang Lee, et al., 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' (2021) 37 *arXIV*.
[51] Attorney-General's Department, '*Privacy Act Review Report 2022*' 1 Privacy Act Review Report 2022 (ag.gov.au).