Cybersecurity Strategies: Protecting Privacy with Genomic and Extended Reality Technologies

Peta Estens

Acknowledgements: *I would like to express my sincere appreciation to *Dr John Doe, whose unwavering support and guidance have been crucial to my professional development as an early-career STEM researcher, and in producing this submission. *Dr John Doe has been an incredible mentor, generously offering his time, expertise, and constructive feedback to understand the opportunities, challenges, and risks of genomic technology and data research. His support in preparing this submission is invaluable.*

This submission responds to the following two questions:

Q19: How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?
Q17: How should we approach future proofing for cyber security technologies out to 2030?

The professional bio for Peta Estens is included at the end of the document.

1.0 Introduction

Emerging technologies such as virtual reality (VR), augmented reality (AR), extended reality (XR), artificial intelligence, quantum computing, and genomics technology offer new opportunities for innovation, growth, and social impact across all sectors. The projected market compound growth rate (CAGR) of XR technologies is 43.5%, from US$64.5 billion in 2022 to $604.3 billion by 2028 [1]. And the global genomics market size was valued at US$ 24.16 billion in 2021 and is projected to witness a CAGR of 16.4% from 2022-2030 [2]. With the projected market growth of XR technologies and the genomics growth market, the potential for data collection and sharing is immense.

However, these datasets also present new cybersecurity vulnerabilities, threat actors, attack vectors, and risks for individuals, organisations, and nations. Biometric data, which refers to the physical or behavioural characteristics that can be used to identify an

individual, is used in XR to create a more immersive experience. And genomic data is the biological information encoded in DNA. Together, genomic, and biometric data can be used to map the biological, behavioural, physical, and psychological traits of an individual [3], [4]. If combined, this complete profiling of a person poses significant privacy and security risks including the capacity for bad actors to engage in nefarious activities such as discrimination, exploitation, blackmailing, behaviour modification, and identity theft [5]. Such interferences affect human behaviour and decision-making, which could undermine the principles of the Universal Declaration of Human Rights and threaten Australia's democracy [6]. We anticipate that protecting biometric and genomic data, which is currently collected, stored, and shared will be a highly critical and complex challenge. This is partly due to reconciling differences in international and domestic legislation and regulatory measures designed to protect privacy. The security of biometric and genomic data is also challenged by the increasing sophistication and rapid deployment of innovative technologies. Collaboration between stakeholders, including governments, industry, and the public is necessary to mitigate risks. In designing a national cybersecurity strategy, it is important to prioritise the potential risks of Web 3.0 technologies and the management of biometric and genomic data.

2.0 Privacy and security risks

Genomic and biometric datasets are vulnerable to cyber-attacks, as they represent valuable targets for threat actors seeking to gain unauthorised access to personal and sensitive information. Rapid development in genomics technology enables data to be increasingly collected, stored, analysed, and shared for various purposes, such as health care, research, forensics, and personal genomics. Genomic data can reveal sensitive information about a person and their blood relatives' identity, ancestry, health status, predisposition to diseases, and response to drugs [7].

XR technologies rely on accurately tracking and adapting to participants' psychological and sensory experiences to create an immersive environment. Failure to accommodate a highly personalised experience causes motion sickness, which can render participants

unable to operate the technology [8]. As illustrated in Image 1, extended reality enables the profiling of participants' biometric data. Strong inferences of an individual can be profiled including sensitive information: cognitive processes, cultural background, drug consumption, mental workload, skills and abilities, fatigue, age, geographical location, gender, physical, and mental health. XR technologies pose a substantial risk of private and sensitive data being collected, sold, harvested, or hacked by multiple third parties for further use, misuse, and/or abuse.

Image 1. XR Technology and Biometrically Inferred Data

There are instances where XR technology have been used to collect biometric data from both children and adults for diagnostic and behaviour modification purposes [9], [10]. These applications of XR technology raise concerns about privacy and ethics, as the collection and use of such sensitive information must be carefully regulated and monitored.

An example highlighting the risks of using XR Technology for unintended purposes is an adult study titled 'Using immersive virtual reality and ecological psychology to probe into child molesters' phenomenology'. The participants were given a consent form stating their results would remain strictly confidential and would not be used in any correction or legal process [10]. However, less than five years later, the lead researcher and author of the study was quoted in the media discussing how the technology is used to profile individuals

for use as evidence in court [11]. This is an alarming example of how technology can be used for purposes other than their intended design and can transform from a therapeutic tool to an incriminating one. Parolees may be presented with evidence of guilt based on instinct rather than the necessary Actus reus, a guilty act required for criminal liability. Like the concerning case studies of XR technologies use of biometric data, there are numerous reports from around the world about the mishandling of genomic information specific to concerns of privacy [7].

Moreover, genomic data when combined with biometric data (e.g., fingerprints, iris scans, facial recognition), behavioural data (e.g., online activity, social media posts), and environmental data (e.g., location, air quality), allow to create a comprehensive and unique profile of a person. This profile can be used for beneficial purposes, such as personalised medicine and precision in public health services. However, these can be used by bad actors for malicious purposes, including bioterrorism, and cognitive warfare, if left unprotected. For example, genomic data can be used to potentially design pathogens that are more lethal or contagious for certain ethnicities, blood types, or immune statuses [12]. Adversaries can weaponise biometric data through behaviour modification for the purpose of influencing public and government policy and destabilising public institutions [13].

3.0 Aims and objectives for biometric and genomic data security

An Australian cybersecurity strategy for these emerging datasets should aim to achieve the following objectives:

3.1 To protect the privacy and security of biometric and genomic data through

- stronger industry-specific legislative and regulatory measures defining the authorised collection, storage, use, sharing, access, and or disclosure of datasets
- clearer determination of ethical and responsible use of combining biometric and genomic datasets for legitimate purposes

- strategic dissemination of educational material promoting data literacy and the risks of XR and genomic technology
- Human-centred frameworks to facilitate individual-centric data systems, offering them full control and ownership of their data

3.2 To prevent illegitimate use, misuse and/or abuse of biometric and genomic data through

- enforcing clearly defined and appropriate penalties for breaching legislative and regulatory standards related to the handling biometric and genomic data
- mandating direct-to-consumer organisations, offering XR experiences or genomic sequencing services, disclosure of the types of data they collect and process. This disclosure should be clear and comprehensive for compliance purposes.

3.3 To foster the innovation and collaboration in genomic and biometric data research and applications through developing public trust and social acceptance. Recommendations include

- clearly defining industry-specific boundaries and limitations of genomic and biometric data research and application
- establishing an independent authority to assess and approve industry-specific genomic and biometric research and application
- strategically promoting ‘good news’ case studies of how biometric and genomic datasets advance Australia’s interests.

3.4 To achieve desirable outcomes, the cybersecurity strategy should consider the following aspects:

- *The technical aspects* of securing biometric and genomic data at rest and in transit using encryption, authentication, access control, auditing, and anonymisation.
- *The legal aspects* of complying with relevant legislation and regulations regarding biometric and genomic data protection and governance at national and international

levels. This includes updating, adapting, and extending current laws and regulations to be fit for purpose.

- ➢ *The ethical aspects* of respecting the rights and interests of biometric and genomic data providers and users and ensuring transparency, accountability, consent, and fairness
- ➢ *The organisational and operational aspects* of establishing industry-specific policies and procedures for biometric and genomic data management. This includes auditing and oversight within and across organisations.
- ➢ *The human aspects* of educating and training biometric and genomic data stakeholders on cybersecurity best practices and awareness. This includes a wider data literacy initiative for all citizens.

While each of these aspects is interconnected and interrelated, the following section separates the technical and legal dimensions to unpack the complexity of cybersecurity challenges. While consideration of the regulatory, ethical, organisational, operational, and human aspects is equally important for designing optimum solutions, it necessitates a design-thinking approach and collaboration among many stakeholders, which is beyond the scope of this submission.

Furthermore, in acknowledging there are many legislative acts protecting specific types of data, for the purpose of brevity this submission focuses only on the proposed amendments to the Australian Privacy Act Review (2022), the Australian Privacy Principles (2012), and the Competition and Consumer (Consumer Data Right) Rules 2020.

4.0 Legislative Compliance: Technical Strategies for Improving Biometric and Genomic Data Management

The Confidentiality, Integrity, and Availability (CIA) is the triad model informing the following strategies to manage biometric and genomic data. The Distributed, Immutable, and Ephemeral (DIE) model informs strategies to secure the infrastructure containing the

datasets [14]. The following strategies are preliminary suggestions, and further research and collaboration with industry partners is required to present extensive, valid, and trustworthy recommendations.

4.1 Selective filtering / data masking

- Technical: Adopt Machine Learning (ML) traffic filtration and data masking techniques to filter out unauthorised and/or illegitimate biometric and genomic data from datasets. Unlike traditional rule-based or heuristic methods, ML-based filtering techniques can learn from the data and adapt to different scenarios and domains. For example, filtering technique could be trained to mask certain genomic variants associated with rare diseases or ethnic groups when sharing genomic data. Also, convolutional neural networks (CNN) based techniques can be useful for filtering out the background or irrelevant information from biometric data collected by XR sensors, such as eye-tracking, head direction, hand position, and bodily motion. However, it is important to balance the privacy considerations with data utility to avoid losing valuable information.

- Legislation: Several Australian legal initiatives, such as the proposed changes recommended in the Australian Privacy Act Review (APAR), the Australian Privacy Principles (APP), and the Consumer Data Right (CDR), are well-placed to adopt the implementation of traffic filtration and data masking techniques. Proposal 4.3 of the APAR includes amendments to the definition of ‘collects’ to cover information obtained from any source and by any means, including inferred or generated information [15]. This proposal includes introducing a Spectrum of Personal Information with risk management rules for strict de-identification, which the implementation of traffic filtration and data masking techniques support. APP 3 prohibits the collection of personal information unless it is reasonably necessary for, or directly related to, the entity’s functions or activities [16]. Genomic and biometric data should only be stored for the time that is necessary to achieve the purpose for which they are collected and processed [5]. Employing traffic filtration

and data masking techniques is an effective strategy to limit the amount of personal information collected in the first place. The CDR is an economy-wide reform that is currently only active in the banking and energy sector but will be rolled out across all sectors. The CDR data minimisation principle requires accredited persons to only collect and use data to provide goods or services in accordance with a request from a consumer and for no other purpose [17]. Adopting traffic filtration and data masking techniques can support the implementation of this principle by minimizing the amount of personal information that is collected and used.

4.2 Encryption methods

- Technical: To effectively protect biometric and genomic data from unauthorised access, use or disclosure, it is important to adopt encryption schemes that are secure against quantum attacks and enable computation on encrypted data. These encryption schemes include post-quantum encryption algorithms based on hard mathematical problems, such as lattice-based encryption algorithms, and homomorphic encryption algorithms that allow computation on encrypted data without decrypting it. These encryption schemes can also support federated learning and multi-party computations, which are techniques that enable collaborative learning and analysis on distributed data without sharing the raw data. These encryption schemes can enhance the long-term security and privacy of biometric and genomic data by minimising the exposure of sensitive data and enabling secure computation and analysis on encrypted data.

- Legislation: Adopting encryption methods is consistent with APP 11.1, which. Requires entities to take reasonable steps to protect personal information by adopting appropriate security safeguards such as encryption [16]. Proposal 21.1 of the APAR recommends expanding the definition of ‘reasonable steps’ to include technical and organisational measures as part of the ‘reasonable steps’ to protect personal information [15]. While APP legislation remains principle-based, adopting encryption methods can help entities comply with outcome focused legislation reforms that require the protection of personal data. Although the CDR does not

mandate the use of encryption methods, data holders must take reasonable steps to protect CDR data, including the use of appropriate security safeguards such [17].

4.3 Authentication:

- Technical: We suggest the use of decentralised identity frameworks based on self-sovereign identity (SSI) technology for identity verification of users or devices who want to access biometric and genomic data [18]. SSI is a decentralised and user-centric approach to digital identity that gives users full control over their own identity data and credentials. This improves the security and privacy of biometric and genomic data by allowing users to prove their identity without relying on third-party intermediaries or centralised databases that could be compromised or abused. SSI can also enable interoperability, user empowerment, and scalability. For example, SSI could allow users to store their data in a personal digital wallet and share it with trusted parties using verifiable credentials.

- Legislation: SSI technology allows individuals to store their data in a personal digital wallet and control the sharing of information with trusted parties. This represents a departure from the mandatory consumer dashboard model proposed by the CDR (see subdivision 1.4.3) as outlined in [17] and aligns with many of the recommendations of the APAR [15]. Adopting SSI technology can help individuals to retake control of their personal information and combat consent fatigue. Through a single personal digital wallet, an individual can manage their data and exercise various rights, including the right to object to the collection, use, or disclosure of personal information (proposal 18.2), the right to withdraw consent (proposal 11.3), the right to erasure (proposal 18.3), the right to correction of data (proposal 18.4), and the right to de-indexation of online search results containing personal information. In addition, using SSI technology, individuals are empowered to take control of the correction of their personal information, which has historically been in hands of organisations subject to APP 13 [16]. Furthermore, SSI technology

may provide solutions to the APAR proposal 13.2 which suggests considering how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information can be adopted as part of implementation of privacy impact assessments for activities with high privacy risks [15].

4.4 Access control:

- Technical: Access control is a crucial mechanism for regulating data access under specific conditions. Depending on the scenario, different types and models of access control can be applied, including discretionary or mandatory access control, role-based or attribute-based access control, or dynamic or context-aware access control. These mechanisms ensure compliance, accountability, and auditability. For instance, attribute-based access control can enable users to grant or revoke access to their biometric and genomic data based on their attributes or preferences. Implementing access control is similar to a passport/visa process, where data users are first verified and provided with appropriate credentials to access the data. However, the ownership of genomic data is often unclear due to multiple stakeholders, including patients who provide their DNA, labs that sequence it, and clinicians who request DNA testing. Therefore, it is essential to establish clear ownership rules to ensure that access control mechanisms work effectively and that all stakeholders' rights are protected.

- Legislation: While biometric and genomic data are highly sensitive types of personal information that require robust access controls for privacy protection, compliance with Australian law may vary depending on industry-specific regulations and standards, and the context-specific risks and threats involved. In validating access control measures, it is worth noting the role-based approach is based on defining policies that determine who can access resources based on their employment role and/or responsibilities. This ensures access is only granted to users with a legitimate need to access that data, which can help organisations comply with APP 6 [16]. Similarly, the mandatory access control approach is based on strict access control policies that cannot be changed by individual users or

administrators. This approach ensures access to biometric and genomic data is tightly controlled and monitored which can help organisations comply with proposal 28.1 of the APAR [15]. Furthermore, the recommended mandatory data breach notifications are consistent with international standards [15]. One area where access control measures are crucial to comply with Australian legislation is the implementation of the CDR. Access control measures are necessary to ensure that only authorised parties can access and use genomic and biometric data in compliance with the CDR rule 7 regarding consumer's consent and privacy preferences [17].

4.5 Auditing:

- Technical: Organisations holding biometric and genomic data face unique privacy risks that require specialised auditing techniques. As mentioned above, data minimisation (4.1), encryption (4.2), and access controls (4.4) are important techniques for safeguarding this type of data and are useful for auditing purposes. Additionally, logging and monitoring can be used to continuously track access to biometric and genomic data, enabling identification of any unauthorised or suspicious access attempts. Regular privacy impact assessments can help identify and mitigate potential privacy risks, while audit trails can track access to sensitive information. Employee training and awareness programs can help ensure that employees understand the importance of privacy and security, improving auditing techniques and demonstrating compliance with relevant privacy laws and regulations.

- Legislation: Auditing plays a crucial role in protecting private information by detecting anomalies or breaches in data security and improving the management of practices and infrastructure systems. In Australia, auditing is often a regulatory requirement and requires compliance with industry-specific standards. As stated on page 6, such a thorough interrogation of auditing processes of biometric and genomic datasets across multiple sectors is beyond the scope of this paper. While

auditing requirements may vary across different industries and regulatory authorities, the CDR is a legally binding instrument created under the Australian Competition and Consumer Act (2010) that mandates extensive auditing of records. Rule 9 requires entities to maintain records and produce them on request to the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC).

The APAR proposes recommendations that can improve auditing practices in addition to the CDR requirements. For example, proposal 15.1 requires entities to determine and record the purposes for data collection, use, and disclosure of personal information at or before the time of collection, which aligns with the data minimization principle as discussed in (4.1) [15]. Furthermore, proposal 15.2 recommends designating a senior employee responsible for privacy within the entity, which can foster a culture of direct accountability for data handling and ensure compliance with regulatory standards [15]. As discussed in (4.3) the APAR requires entities to conduct a Privacy Impact Assessment for activities with high privacy risks and to produce the Privacy Impact Assessment to the OAIC and/or ACCC on request. Additionally, APP 1.2 obliges entities to implement practices, procedures, and systems to enable them to deal with inquiries, disputes, and complaints from individuals. Auditing can assist with complying with APP 13 and correcting inaccurate, out-of-date, incomplete, irrelevant, or misleading data [16].

Data is the resource that powers much of the growth in digital technologies and it continues to expand and merge at an unprecedent scale. The capability of emerging technologies for harvesting highly sensitive genomic and biometric data from Australian citizens poses significant risks. Off-the shelf technologies are already capable of collecting these datasets [19], [20]. The Australian Government's Digital Platforms Inquiry identified the complex challenges of regulating digital platforms due to their global nature, business models, and the pace of technological evolution and transformation [19]. Therefore, this submission has also been emailed to the Australian Competition and Consumer Commission (ACCC) and the Australian Communications and Media Authority

(ACMA) to address the concerns raised in this submission. The former is investigating the expanding ecosystem of digital platform service providers [20], while the later has been granted new powers, including formal information-gathering demands to oversee digital platforms, and the authority to register an enforceable industry code [21]. The security of Australian biometric and genomic data is of national importance since this personal information, unlike a passport or driver's license, cannot be changed. By sharing this submission across the Department of Home Affairs, ACCC, and ACMA a collaborative effort can be made to address the concerns raised herein and integrate them into existing efforts to safeguard human rights and Australian democracy. Such a coordinated approach to regulate digital platforms, including data storage, can help to mitigate the risks posed by emerging technologies and ensure that citizens' sensitive data is adequately protected.

5.0 Afterthoughts

Genomic research holds immense potential for advancing healthcare, but to realise its benefits, we need to ensure that the genomic data is shared effectively and responsibly. Similarly, biometrics promises highly personalised immersive experiences for education, training, healthcare, and entertainment driven by tracing the participant's psychological and physiological responses. However, there is also a need to safeguard against the misuse and abuse of how the biometric data is collected, shared, sold, or hacked.

Web 3.0 technology has the potential to shift the digital paradigm towards a user-centric model where individuals have greater control over their data. Decentralised technologies, such as distributed ledger technology, can enable data to be stored and managed in a distributed manner, eliminating the need for a central authority. However, the next iteration of the internet also faces some challenges. One significant challenge is the identification of malicious users that can compromise data quality. Additionally, users are vulnerable to social engineering attacks and manipulation, leading to the sharing of data without understanding the consequences. As machine learning continues to manage data, it raises concerns about the need for human oversight to verify the accuracy of

biometric and genomic data, ensuring the protection of consumer privacy. Moreover, the manipulation of data used to train artificial intelligence presents significant human rights issues, especially when analysing and processing biometric and genetic data.

To effectively tackle these challenges, it is imperative to establish stronger ethical data governance at a legislative and regulatory level. This can facilitate the development of industry-specific policies that safeguard users from exploitation. Additionally, promoting privacy-preserving technologies is necessary to prevent data breaches and privacy violations. This must be accompanied by a more rigorous education and awareness-raising effort to help the public better understand the value of their data and the risks associated with sharing it. By addressing these issues, we can unlock the full potential of biometric and genomic research and use it safely to embrace new opportunities for innovation, growth, and social impact across all sectors.

Professional Biography

Peta Estens, PhD Candidate

Peta is an ATSE Elevate Scholar and PhD Candidate at Deakin University. She is an award-winning researcher, digital designer, and EdTech specialist. In 2022 Peta graduated with a Master of Visualisation, Simulation, and Immersive Design from UNSW with the Dean's Prize for Academic Excellence. This research catalysed her strong interest in protecting human rights in the digital age of big data. In 2023 Peta graduated with a Certificate of Cyber Law at Deakin University with more questions than answers. Her PhD focus is on mitigating the risk of biometric data harvesting in XR. Additionally, she aims to promote data literacy and how technology impacts the construction of identity, affects a sense of belonging to the community, and determines one's participation in wider society.

References

[1] IMARC Group, (2023, Mar 21). *Extended Reality (XR) Market: Global Industry Trends, Share, Size, Growth, Opportunity Forecast 2021-2026* [Online]. Available: https://www.imarcgroup.com/extended-reality-market

[2] IQVIA Institute, (2020, May 12). *Understanding the Global Landscape of Genomic Initiatives* [Online]. Available: https://www.iqvia.com/insights/the-iqvia-institute/reports/understanding-the-global-landscape-of-genomic-initiatives [Accessed: Apr. 6,2023].

[3] A. S. Geroski, (2019, Feb 17). *Spring 2019 Journal: Abuse of Our Genetic Data is the Next Privacy Scandal* [Online]. Available: https://bppj.berkeley.edu/2019/02/27/spring-2019-abuse-of-our-genetic-data-is-the-next-privacy-scandal/

[4] J. Pandya, (2019, Mar 9). *Hacking Our Identity: The Emerging Threats from Biometric Technology* [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/?sh=36741ce65682

[5] Institute for Development of Freedom of Information, (2022, Feb 28). *Processing of Biometric and Genetic Data-European Standards* [Online]. Available: https://idfi.ge/en/processing_of_biometricand_genetic_data

[6] United Nations, (1948, Dec 10). *Universal Declaration of Human Rights* [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[7] Wan, Z., Hazel, J.W., Clayton, E.W. et al., "Sociotechnical safeguards for genomic data privacy," *National Review Genetics,* vol. 23, pp. 429–445, Jul. 2022. DOI:10.1038/s41576-022-00455-y

[8] A. Singleton, (2020, May 28). *Physical Factors: Motion Sickness in XR* [Online]. Available: https://medium.com/pintsizedrobotninja/physical-factors-motion-sickness-in-xr-9271de8f6d2.

[9] L. Stallmann, D. Dukes, M. Tran, V. D. de Gevigney, D. Rudrauf, and A. C. Samson, (2022, Mar 10). *Virtual Reality and Mixed Reality for Emergency Response Training: A Systematic Review* [Online]. Available: https://www.frontiersin.org/articles/10.3389/frvir.2022.826241/full.

[10] P. Renaud, S. Chartier, J. L. Rouleau, J. Proulx, "Using Immersive Virtual Reality and Ecological Psychology to Probe into Child Molesters' Phenomenology," *Journal of Sexual Aggression,* vol. 19, no. 1, pp. 102-120, Jan. 2011. DOI:10.1080/13552600.2011.617014

[11] O. Solon, (2019, Jun 8). *Polygraph for pedophiles: how virtual reality is used to assess sex offenders* [Online]. Available: https://www.theguardian.com/technology/2017/jun/07/virtual-

reality-child-sexual-abuse-pedophile-canada-research

[12] M. S. Green, J. LeDuc, D. Cohen, D. R. Franz, “Confronting the threat of bioterrorism: realities, challenges, and defensive strategies,” *The Lancet Infectious Diseases,* Oct. 2018. DOI:10.1016/S1473-3099(18)30298-6

[13] R. Waltzman, (2022, Nov 18). *The Role of Today’s VRE and Considerations for Cognitive Warfare* [Online]. Available: https://www.act.nato.int/articles/cognitive-warfare-considerations#:~:text=Cognitive%20warfare%20can%20be%20functionally,%E2%80%9D%20%5BBernal%20et.at.

[14] Copado (2022, Dec 19). *CIA Security Triad Complementary, Not Competitive* [Online]. Available: https://www.copado.com/devops-hub/blog/making-die-model-security-vs-the-cia-security-triad-complementary-not-competitive

[15] Australian Government Attorney-General’s Department, (2023, Feb 16). *Privacy Act Review Report* [Online]. Available: https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[16] Office of the Australian Information Commissioner, (2014, Jan). *The Australian Privacy Principles: From Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012* [Online]. Available: https://www.oaic.gov.au/__data/assets/pdf_file/0006/2004/the-australian-privacy-principles.pdf

[17] Commonwealth of Australia, (2020, Dec 23). *Competition and Consumer (Consumer Data Right) Rules 2020* [Online]. Available: https://www.legislation.gov.au/Details/F2021C00076

[18] Dock, (2023, Mar 24). *Self-Sovereign Identity: The Ultimate Guide 2023* [Online]. Available: https://www.dock.io/post/self-sovereign-identity

[19] E. Rosenbaum, (2018, Jun 16). *5 biggest risks of sharing your DNA with consumer genetic-testing companies* [Online] Available: https://www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html

[20] J. Ahvenainen, (2022, May 1). *The metaverse is coming for your biometric and health data* [Online] Available: https://medium.com/prifina/the-metaverse-is-coming-for-your-biometric-and-health-data-1d185a93519c

[21] Commonwealth of Australia, (2019, Dec 12) *Regulating in the digital age: Government Response to the Implementation Roadmap for the Digital Platforms Inquiry*. Available: https://treasury.gov.au/publication/p2019-41708

[22] Australian Competition and Consumer Commission, (2023, Mar). *Digital Platform Services Inquiry- September 2023 Report on the expanding ecosystems of digital platform service providers Issues Paper*. Available: https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20September%202023%20report%20-%20Issues%20paper_0.pdf

[21] HWL Ebsorth Lawyers (2023, Mar 29). *Media Regulator ACMA to be Given New Powers to Help Protect Australians from Online Misinformation* Online]. Available: https://hwlebsworth.com.au/media-regulator-acma-to-be-given-new-powers-to-help-protect-australians-from-online-misinformation/#:~:text=29%20March%202023&text=On%2020%20January%202023%2C%20the,and%20disinformation%20on%20digital%20platforms.