Reset.
AUSTRALIA

Response to 2023-2030 Australian Cyber Security Strategy Discussion Paper

Reset.Tech Australia
April 2023

Executive Summary

1. Personal data creates cybersecurity risks that warrant consideration in Australia's Cyber Security Strategy. This includes:
    - Excessive **collection and retention** of personal data, which should be considered the first step in the chain of cybersecurity risk,
    - Excessive **transfer** of personal data, which both amplifies existing risks and creates new risks.

    These risks travel across numerous policy portfolios, requiring a comprehensive policy response to effectively mitigate them.

2. **Biometric data**, including health tracking data, and **geolocation data** create unique and serious cybersecurity risks. The widespread use of technologies drawing upon this data drives demand. These technologies warrant consideration in the Cyber Security Strategy, especially frameworks around facial recognition technology, or other AI that uses biometric, tracking, or geolocation data.

3. Existing regulatory models may not be sufficient to ensure cybersecurity. It is our assessment that self- and co-regulatory models are inadequate to address the scale and severity of contemporary cybersecurity risks.

Contents

1. About Reset.Tech Australia & this submission

Reset.Tech Australia is an independent, non-partisan policy initiative and research organisation committed to tackling digital threats to Australian democracy. We are part of a global initiative that develops and drives evidence-based policies and programs on technology and democracy.

We have prepared our submission in response to the question: *"What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?"*.

2. Excessive data collection, retention and transfer is a cyber security risk

Personal data inherently creates cybersecurity concerns. Excessive collection, retention and transfer of this personal data routinely creates unnecessary risks for Australians and has often led to significant harm. This includes harms to *individual security*. For example, excessive data collection has harmed people's financial security, when 'enriched' data is breached. The cost to individuals from identity theft have reached $500.5m per year and with 20% of victims reporting being refused credit as a result.[1] It has also been associated with individual physical security risks, such as broadcasting children's live location data which happens as a matter of course on products like Snap Maps[2] and BeReal.[3] Breaches are not exceptional, and could sadly be considered a routine occurrence.

Routine breaches create broader *societal security risks*. For example, the excessive collection and transfer of personal data has been shown to harm society, such as the destabilising effects that the Cambridge Analytica firm unleashed on democracies around the world,[4] with 300,000 Australians' data collected and retained by Cambridge Analytica.[5] Cambridge Analytica is not an anomaly. A cottage industry of private sector information insecurity actors have emerged, from Team Jorge to the Internet Research Agency to the NSO (discussed below). These actors are comparable – in terms of future financial harm and political

[1] Christie Franks & Russel Smith (2020). Identity crime and misuse in Australia: Results of the 2019 online survey. Statistical Report no. 27. https://www.aic.gov.au/publications/sr/sr27

[2] SnapChat (2023) *How do I find my friends on SnapMaps?* https://help.snapchat.com/hc/en-gb/articles/7012276359700-How-do-I-find-my-friends-on-Snap-Map-

[3] Tim Sandle (2022) *Revealed: BeReal may share your location data without your consent* https://www.digitaljournal.com/social-media/revealed-bereal-may-share-your-location-data-without-your-consent/article

[4] Jesse Witt & Alex Pasternack (2019) 'Before Trump, Cambridge Analytica quietly built psych-ops for militaries" *Fast Company* https://www.fastcompany.com/90235437/before-trump-cambridge-analytica-parent-built-weapons-for-war

[5] Elizabeth Bryne (2023) 'High Court dumps Facebook's challenge against prosecution over Cambridge Analytica privacy breaches' *ABC* https://www.abc.net.au/news/2023-03-07/high-court-dumps-facebooks-cambridge-analytica-challenge/102062516

disruption – to today's ransomware industry.[6] Both the individual and societal risks are significant and active, and need to be considered through the lens of cyber security. Yet despite the risks, the excessive collection, retention and transfer of personal data has become a 'commercial norm' among digital services.

A. Excessive collection and retention

The logic and structure of large digital platforms in particular has encouraged an insatiable demand for personal information. Some of this information is necessary for businesses to maintain for extended periods of time, particularly those with enduring customer relationships. But a significant number of businesses are storing excessive amounts.

Excessive collection—when a company collects more personal information than is strictly necessary to provide their service or product—is rife. For example, one company investigated by the *New York Times* was found to hold a database of people's exact location, tracked up to 14,000 times per day,[7] or once every 6.2 seconds. There is no reason to think the context in Australia is any different. Excessive collection that actively engineers risks, because data collection enables future harms.

Companies frequently retain personal information for longer than is strictly necessary to deliver a service or is required for legal reasons. This excessive retention is equally commonplace. The scale and severity of the Optus breach was in part because they had collected what could have been necessary data, but retained it unnecessarily.[8] Excessive retention extends the longevity of any risks that people face because of misuse of their data.

Excessive collection and retention benefits commercial companies, while creating individual and societal risks. This asymmetry exists despite the fair and reasonable requirements in the Australian Privacy Principles, which should ensure data minimisation, and the Australian Consumer Law, which should guarantee fair terms to consumers.

The first line of defence against cybersecurity issues arising from personal data lies at the moment of data collection. Businesses need to be robustly incentivised to confine their data collection and data retention practices.

B. Excessive transfer

It is important to widen our aperture from the traditional relationships of digitally-enabled businesses and their consumers. These businesses – such as cafés, health providers, and financial institutions, are examples of **known** interfaces between data subjects and data collectors. Underneath this rather orthodox layer of data practices lies the high-risk yet low-visibility data transfer industry – where classic privacy principles of notification and consent become much woolier. Transfer relationships between initial data collectors and

---

[6] Elise Thomas (2022) "Conspiracy Clickbait: Farming Facebook" *Institute for Strategic Dialogue* https://www.isdglobal.org/isd-publications/conspiracy-clickbait-farming-facebook/

[7] Jennifer Valentino-DeVries *et al* (2018) 'Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret' *New York Times* https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[8] Gareth Hutchens (2022) 'Too much data collection means we're more at risk of having personal details stolen, expert says' *ABC* https://www.abc.net.au/news/2022-09-29/we-are-more-at-risk-than-ever-with-personal-data/101481934

third-parties means that personal information can be duplicated and transferred to a virtually limitless number of firms – across a wide range of jurisdictions and geographies.

Companies that hoover up voluminous amounts of personal information often multiply the security risks of data collection and retention by excessively trading personal data, or engaging in data transfers which are not strictly necessary for the delivery of a service. Euphemistically referred to as 'enriching' data, personal data is often ID-linked and combined to create worryingly detailed profiles about each and every Australian.

Enhanced data sets are particularly valuable commodities that are monetised in a variety of ways, with each transfer creating their own security risks. Some companies actively trade this data creating rich marketplaces for data brokers. **Data brokers** often operate without regulatory intervention,[9] but the data they trade can multiply security risks (see below). On top of enabling the development of more enriched, riskier data sets, they also innately multiply the potentials for a breach, as this data is exposed to more and more actors as it is traded.

Data brokers, young people and security

Data brokers hold reams of information about families including children, and children themselves.[10] For example, a quick online search found one Australian data brokerage selling access to families based on:

- Details about 150,000 children's dates of birth, gender and postcode, and their mother's contact details.[11] This data was initially harvested from a 'baby gift pack scheme', where mothers collect a baby gift pack from a leading national retailer when their baby is between 2 and 4 months old.

- Details about nearly 15,000 children's year of birth and postcode, and parents' contact details,[12] harvested when parents responded to a mail offer for a personalised baby product. The product was described as a 'special celebration memento announcing the baby's birth details such as; name, birth date, birth time, weight and length.... The memento is the ideal and special keepsake'.

It is unclear what safeguards are in place to ensure that children's data is protected when it is transferred or used, nor how any trade that relies on collecting and retaining their date of birth ensures their security.

Others internally transfer this data, collecting and combining data from tracking products like **cookies, tracking pixels or SDKs** into enhanced data profiles. These sorts of tracking products are built into all sorts of products and services that Australians use, from mental

[9] Katherine Kemp (2022) *This law makes it illegal for companies to collect third-party data to profile you*https://www.unsw.edu.au/news/2022/09/this-law-makes-it-illegal-for-companies-to-collect-third-party-d

[10] For example, there are international cases of data brokers selling information by school grade. Eg Christian Hetrick (2021) 'NJ data broker tries to sell information on a million kids' *Philadelphia Inquirer* www.inquirer.com/business/technology/alc-princeton-data-broker-personal-info-million-kids-vermont-law-20190319.html

[11] The List Group, nd 'Baby Gift Pack' https://thelistgroup.com.au/wp-dynamic/list-detail.php?card-id=11

[12] The List Group, nd 'Baby product buyers' https://thelistgroup.com.au/wp-dynamic/list-detail.php?card-id=12

health apps to EdTech products to location tracking apps.[13] These risky, enhanced data sets are monetised through behavioural advertising, which as a process can and has been hijacked to create security concerns.

Weaponising behavioural advertising to sow insecurity

There is a cottage industry of private sector information insecurity actors, who utilise Big Tech's services to push destabilising content out to audiences for profit. Their capabilities are singularly dependent on being able to misuse the enhanced data sets held by digital platforms (originally collected for behavioural advertising purposes).

The extreme consequences of these services have variously been labelled 'coordinated inauthentic behaviour', 'disinformation for profit, and 'influence for hire'. For example, Cambridge Analytica deployed "weapons grade" data harvested from social media platforms, and deployed psycho-ops tactics using targeted advertising and disinformation on social media, to interfere with elections in Trinidad and Tobago, Kenya, potentially the UK's Brexit vote, and President Trump's campaign.[14] Or more recently, Team Jorge—a 'black ops' disinformation unit—claims to have manipulated over 30 elections around the world using hacking and automated disinformation on social media, from Nigeria, to Kenya and hijacking French news broadcasters to protect Russian interests in Monaco.[15]

Both Cambridge Analytica and Team Jorge highlight the convergence of 'coordinated inauthentic behaviour' tactics and criminal activities, from data privacy breaches to bribery and hacking, with their criminal success ultimately resting on the failure of digital platforms to effectively protect against their activities. The Institute for Strategic Dialogue finds that these commercial firms are typically *more successful* than their state counterparts.[16]

---

[13] For example, the 4th most downloaded family app in Australia (Find My Kids), collects kids geolocation data, and enriches it with data collected from third parties cookies, and shares it with third parties via cookies. Their privacy policy states ' we may share Your personal information in order to facilitate targeting, delivery, and measurement of online advertising on third-party services, or otherwise facilitate the transmission of information that may be useful, relevant, or of interest to you. Such partners include: Facebook Inc., Adjust GmbH. We do not share children's personal information for these purposes', but they do not share the personal data of those under 13 for advertising purposes. Data potentially may be shared for other purposes, or data about 13-18 year olds shared for advertising purposes, See Find My Kids nd *Privacy Policy* https://findmykids.org/docs/privacy-policy/en

[14] Larry Madowo (2018) 'How Cambridge Analytica poisoned Kenya's democracy' *Washington Post* https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/, Eric Auchard (2018) 'Cambridge Analytica Stage Managed Kenyan President's Campaign' *Reuters* https://www.reuters.com/article/us-facebook-cambridge-analytica-kenya-idUSKBN1GV300; Mark Scott (2019) 'Cambridge Analytica did work for Brexit Groups' *Politico* https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/; Peter Lewis & Paul Hilder (2018) 'Leaked Cambridge Analytica's Blueprint for the Trump Victory' *The Guardian* https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

[15] Stephanie Kirchgaessner, Manisha Ganguly, David Pegg, Carole Cadwalladr and Jason Burke (2023) 'Revealed: The hacking and disinformation team meddling in elections around the world' The Guardian https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan

[16] Elise Thomas (2022) "Conspiracy Clickbait: Farming Facebook" *Institute for Strategic Dialogue* https://www.isdglobal.org/isd-publications/conspiracy-clickbait-farming-facebook/

Others exist in the 'grey zone', such as the **Real-Time-Bidding** process. The RTB process creates extensive cyber security risks. For example every American has their geolocation exposed to third party advertisers on average 747 times a day in the process;[17] lacking any stronger privacy protections, Australians probably see the same level of unregulated location broadcasting. This multiplies the risks, as detailed personal data is frequently exposed to an opaque and unknown set of actors.

C. Policy responses to excessive collection, retention and transfer

Excessive collection and transfer already violates Australia's data privacy principles, but weak enforcement has allowed these practices to continue unabated.[18] Australia is not alone in this regard. Strong regulation backed with strong enforcement is central to curbing these security risks. For example, in Europe the *General Data Protection Regulation* has been limited in its ability to stem the data flows created and exacerbated by real-time bidding markets. Noting esteemed expert and member of the Reset.Tech Advisory Board, Shoshana Zuboff:

> *"Google is the largest RTB company, channeling targeting data to 4698 firms in the United States, or 10% of US broadcasts, and 1058 firms in Europe, accounting for 14% of European broadcasts. The ICCL findings suggest that current legal regimes mitigate but do not abolish these operations. The average person in the United States, where the federal government has yet to pass basic privacy protections, has their online activity and location data exposed 747 times each day. In Europe where data protection laws lead the world, it's 376 daily exposures."*[19]

Zuboff draws on ICCL studies to observe that the approximate halving of daily exposures from the GDPR Is still not enough. One explanation for the only partial impact here lies in non-compliant cultures in the digital advertising industry, and the stymied capacity of enforcement agencies to take action. For example, in the UK, the Information Commissioner's Office confirmed that a key standards-setting body for digital advertising, the IAB, relied on non-compliant transparency and consent frameworks.[20] This significant finding was undermined by the ICO's failure to take action, despite strong arguments that the IAB was responsible for the largest-ever data breach in the UK.[21] Against this backdrop, it

[17]Irish Council for Civil Liberties (2022) T*he Biggest Data Breach: ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe*
https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
[18]Katharine Kemp (2022) 'Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful' http://dx.doi.org/10.2139/ssrn.4224653
[19] Shoshana Zuboff (2022) 'Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization' *Organization Theory* 3(3) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4292299
[20] Information Commissioner's Office 2019 'Update report into adtech and real time bidding' https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf
[21] Johnny Ryan (2020) 'The ICO's failure to act on RTB, the largest data breach ever recorded in the UK' Brave,

is important to note that Australia currently lacks both the strong data protections provided by the *GDPR*[22] and strong enforcement from a relatively underfunded OAIC.[23]

Excessive collection, retention and transfer create significant privacy, security, and economic risks to Australian users and requires a comprehensive policy response to curb. There are some policy solutions in motion that may be useful, including the *Privacy Act Review*, the ACCC's commitment to tackling online scams and fraud, and MInister O'Neil's commitment to protecting Australians from the invasive and extensive data breaches.

Recommendation 1

We recommend that the excessive collection, retention and transfer of personal data be considered in Australia's Cyber Security Strategy. Consideration of these issues needs to address both gaps in protections across the current regulatory landscape, as well as issues with enforcement and existing regulatory responses.

[22] Australia's *Privacy Act* has been described as 'out of date and not fit-for-purpose in our digital age' by the Attorney General for instance. See Mark Dreyfus (2022) *Tweet dated Dec 20th 2022* https://twitter.com/MarkDreyfusKCMP/status/1605023966279921664?lang=en

[23] For example the OAIC is comparatively underfunded. In 2021-22 terms the OAIC received $1.11 AUD pp (Based on an annual budget of $28,487,000 for 2021-22, Australian population of 25,739,256 in 2021). In the UK, the Information Commissioner's Office, received $1.96 AUD pp (based on an annual budget £70,625,526 for 2021-22, UK population of 67,081,000 in 2020). In Ireland the Data Protection Commission received $6.04pp (Based on an annual budget €19,128,000 for 2021-22, Irish population of 5,011,500 in 2021 (Ireland also has EU wide data protection functions)

3. Biometric and tracking data warrants special consideration

Biometric data, including health tracking data, and geolocation data create unique and serious cybersecurity risks. **Location data** creates significant and unique safety risks where they are handled badly,[24] and is particularly concerning to young people[25] and vulnerable communities. **Biometric data** too; unlike other forms of personal information, biometric data cannot be changed where a breach or other issue arises. It is uniquely tethered to its human source, and once people's fingerprints, facial recognition or gait data have been compromised, they cannot be changed. This is not a hypothetical, and significant breaches involving fingerprint and facial recognition data have and are occurring.[26] **'Tracking' data**—such as heart rate and sleep data—are a form of biometric data that shares the same risks around permanent compromise. The widespread use of technologies that use this data drives demand for its collection, retention and transfer. As discussed above this presents significant and unique risks. Given this, the use of technologies that rest on biometric, tracking or location data should be strictly controlled and limited.

We note that a number of jurisdictions are moving forward with legislative requirements around facial recognition technology and other AI that involves biometric data. This includes the EU and Colombia, Argentina, Brazil, Chile and Uruguay developing frameworks regulating the use of AI.[27]

---

[24] For example, we note how location data was allegedly created security risks for users of Uber, see Jo Ling Kent, Chiara Sottile & Michael Cappetta 2016 'Uber Whistleblower Says Employees Used Company Systems to Stalk Exes and Celebs' *NBC News* https://www.nbcnews.com/tech/tech-news/uber-whistleblower-says-employees-used-company-systems-stalk-exes-celebs-n696371

[25] Rys Farthing *et al* 2023 '"It Sets Boundaries Making Your Life Personal and More Comfortable": Understanding Young People's Privacy Needs and Concerns' *Technology & Society Magazine* https://ieeexplore.ieee.org/document/10063169

[26] Such as the leak of over 1 million people's fingerprint data by security firm Suprema. (see vpnResearch Mentor Team 2023 *Data Breach in Biometric Security Platform Affecting Millions of Users* https://www.vpnmentor.com/blog/report-biostar2-leak/). It is worth noting that these security solutions such as biometric readers are available and advertised to Australian clients (see Nedap nd *Biostar integration Seprema* https://www.nedapsecurity.com/technology-partner/suprema/ for example).

[27] See for example Argentina *National Plan of Artificial Intelligence* 2020 https://ia-latam.com/wp-content/uploads/2020/09/Plan-Nacional-de-Inteligencia-Artificial.pdf; Uruguay 2021 *Artificial Intelligence Strategy* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial; Chile 2021 *National Policy on Artificial Intelligence* https://www.minciencia.gob.cl/areas-de-trabajo/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/; Colombia 2021 *Inteligencia Artificial Colombia* https://inteligenciaartificial.gov.co/publicacion/9/; México 2020 *National Mexican Agenda of Artificial Intelligence* https://ia-latam.com/wp-content/uploads/2020/09/Agenda-Mexicana-de-IA-2020.pdf

While some of this may be addressed within the framework of the *Privacy Act*, the security of uniquely sensitive biometric, tracking and geolocation data sets is a cyber security concern and may warrant attention.

Recommendation 2

We recommend that the use of technologies that use biometric, tracking or geolocation data be considered in Australia's Cyber Security Strategy. This may include specific consideration of frameworks around facial recognition technology, or other AI that uses biometric, tracking or geolocation data.

4. Self- or co-regulation will not ensure cyber-safe conditions

For a serious and appropriate response to Australia's cyber threat landscape, it is necessary for Government and independent regulators to lead on drafting and developing the regulatory processes. There is clear, empirical evidence from the Online Safety Codes process that industry-drafted codes created deficient security conditions that do not achieve international best-practice.

We draw attention to the three key areas where industry drafting led to substantially inferior cybersecurity outcomes, with regards to geolocation data and account privacy. Private accounts and geolocation data are important for individual safety; where a young person's account is private, they are not recommended as 'friends' or as accounts to 'follow' to adult strangers, which can be a significant source of risky contacts and grooming.[28] Likewise, live location data also leaves young people exposed to a higher risk of grooming.[29] The industry-drafted Online Safety Codes proposed leaving 16 and 17 year olds unprotected (see figures one and two).

Fig 1. Minimum age thresholds for requirements to default accounts to private		
	On social media	**On online games**
United Kingdom	Protections up to 18	Protections up to 18
Ireland	Protections up to 18	Protections up to 18
California	Protections up to 18	Protections up to 18
Revised Australian Codes	Protections up to 16	Protections up to 16

Fig 2. Minimum age thresholds for additional protections for geolocation data		
	On social media	**On online games**
United Kingdom	Protections up to 18	Protections up to 18
Ireland	Protections up to 18	Protections up to 18
California	Protections up to 18	Protections up to 18
Revised Australian Codes	Protections up to 16	Protections up to 16

[28] For example, Meta found, 75% of all 'inappropriate adult-minor contact' on Facebook was a result of their 'People You May Know' friends recommendation system. As made public in *Alexis Spence et al. v. Meta,* U.S. District Court for the Northern District of California, Case No. 3:22-cv-03294 (filed June 6, 2022) p. 11-12, *Growth, Friending + PYMK, and Downstream Integrity Problems*. https://pugetstaffing.filev.io/r/s/9eb2BZcUfhdTxkxIfV45CJnIivYHhdWcRRuQVwSMz120RVs7ATmxn9r5

[29] 5Rights Foundation (2020) *Risky By Design* https://www.riskyby.design/

Additionally, requirements around children's precise geographic location were much weaker than emerging global norms. In Australia, the revised Codes propose not *broadcasting* children's location data rather than not *collecting* it in the first instance (see figure three). Preventing services from broadcasting precise GPS locations offers weaker security protections than preventing services from routinely collecting GPS location data in the first instance. It overlooks the cybersecurity risks presented from:

- **Data security problems**. Collecting troves of location data creates inevitable security risks from malicious hacking to a lack of internal controls about which staff, if any, should be able to access children's GPS locations.
- **Errors and missteps from services**. For example, a simple failure of process saw Instagram make children's contact details publicly available if they simply opened business accounts.[30] Children's precise location data is not immune to failures of process, even if digital services agree to not broadcast locations.
- **Commercial harm arising from this data**. Not *broadcasting* GPS data does not prevent online service providers accessing and using this data for commercial exploitation, such as targeted advertising.

Fig 3. Protections against default collection of children's precise location (GPS location)

	On social media	On online games
United Kingdom	Must not collect by default	Must not collect by default
Ireland	Must not collect by default	Must not collect by default
California	Must not collect by default	Must not collect by default
Proposed Australian Codes	None; must not broadcast by default	None; must not broadcast by default

Recommendation 3

We recommend that the Cyber Security Strategy include recommendations against self- and co-regulation of digital platforms, and a commitment to progressively replacing existing self- and co-regulatory Codes with compulsory, regulator-drafted requirements.

[30] Natasha Lomas (2022) 'Instagram fined €405M in EU over children's privacy' *Techcrunch* https://techcrunch.com/2022/09/05/instagram-gdpr-fine-childrens-privacy/