SalingerPrivacy

We know privacy inside and out.

Submission in response to the *Digital Platform Services Inquiry – March 2024 report on data brokers - Issues Paper* (July 2023)

Australian Competition and Consumer Commission

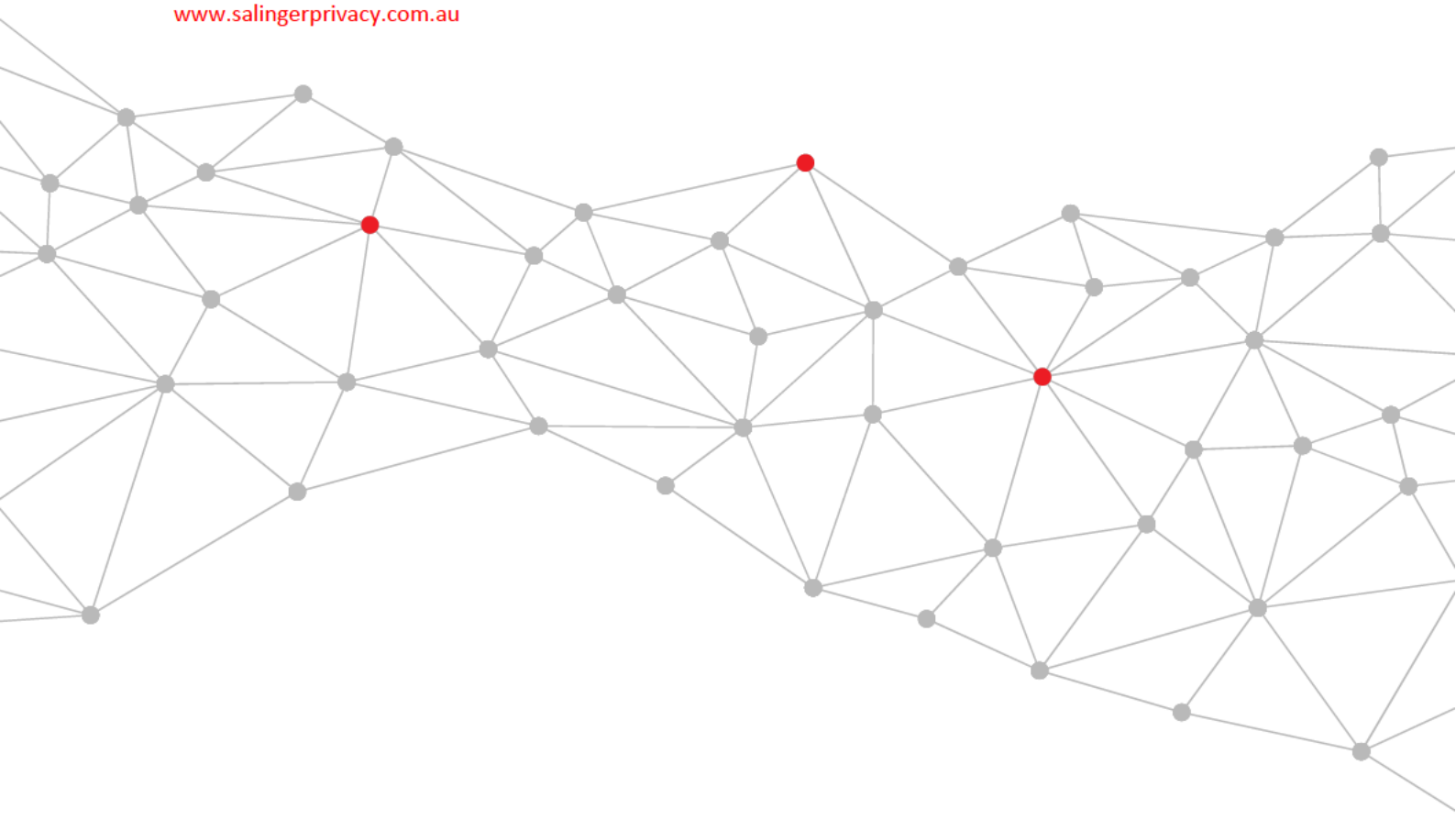
7 August 2023

Salinger Consulting Pty Ltd

ABN 84 110 386 537

PO Box 1250, Manly NSW 1655

www.salingerprivacy.com.au



Covering letter

7 August 2023

Australian Competition and Consumer Commission
By online submission

Dear ACCC Digital Platforms review team,

Thank you for the opportunity to make a submission in relation to the *Digital Platform Services Inquiry – March 2024 report on data brokers - Issues Paper* (July 2023).

Please find our submission attached.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Please do not hesitate to contact me if you would like clarification of any of the comments made in this submission.

Yours sincerely

Anna Johnston
Principal | **Salinger Privacy**

Our submission

We welcome the release of the *Digital Platform Services Inquiry – March 2024 report on data brokers - Issues Paper (July 2023)* (the Issues Paper) by the Australian Competition and Consumer Commission (ACCC). Our submission is as follows.

A harmful industry

With few exceptions,[1] data brokering practices do not benefit consumers.

They certainly can harm consumers, both in terms of the risk posed by data breaches,[2] and the harms which arise from the hyper-personalisation of content consumed in the digital environment.[3]

Tougher regulation, and tougher enforcement of existing regulation, is required, both for consumer protection and essential human rights / privacy protection reasons.

The scope of this review

The ACCC's review should not focus only on 'third party' brokers.

It is our submission that you cannot regulate the data brokering industry without tackling the entire ecosystem. That ecosystem currently enables companies to sell their 'first party' data, and/or buy data or 'insights' from brokers to 'enrich' their 'first party' data.[4]

In any case, the line between 'first party' and 'third party' brokers, and between data sellers and data consumers, is increasingly fuzzy.[5]

---

[1] An exception would be services which pull together data *at the request of a consumer*, such as a service building a consumer's credit profile to help the consumer apply for finance.
[2] See 'See your identity pieced together from stolen data', 18 May 2023, at https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688
[3] See our analysis of privacy harms in '*Big Tech, Individuation, and why Privacy must become the Law of Everything*', 22 March 2022, at https://www.salingerprivacy.com.au/2022/03/22/big-tech-blog/
[4] We use the word 'enables' here, rather than 'allows', deliberately. We argue that while privacy legislation would *appear* to prohibit the sharing of personal information between unrelated companies, there is such widespread non-compliance with the legislation that it could be said that the current regulatory environment is such as to enable these practices to flourish - notwithstanding the letter of the law.
[5] See our analysis of the practices of media publishers turned first party data brokers (data sellers) and data consumers in '*The great con job: how the media and marketing industry is getting away with tracking Australians*', 1 August 2023, at https://www.salingerprivacy.com.au/2023/08/01/media-and-marketing-industry-blog/

An industry built on widespread non-compliance

We believe that many data brokering practices are non-compliant with the *Privacy Act 1988* (Cth) (the Privacy Act). We refer to, agree with and support research and submissions by Dr Katharine Kemp in relation to 'the forgotten privacy principle' Australian Privacy Principle (APP) 3.6.[6] If properly complied with, APP 3.6 should greatly inhibit the *demand side* of the data brokering industry, because, in our view, much of the 'customer enrichment' market for companies to buy data from, or use the services of, data brokers is built on non-compliance with APP 3.6. If industry practices involve widespread non-compliance with existing laws, which exist to protect consumers, we submit that the ACCC's review should not exclude this topic from the scope of its review.

We likewise believe that the *supply chain* for data brokers, in which companies' 'first party' data is shared with or sold to 'third party' data brokers, may involve widespread non-compliance with APP 6 in the Privacy Act.

In particular, we dispute such companies' reliance on 'consent' as their purported ground for compliance with APP 6, unless such consent is truly voluntary, informed, specific, current and demonstrably granted actively and willingly by a person with both the capacity to understand and in circumstances in which the consumer had the option to make a choice between granting or refusing their consent, without being denied access to goods or services.[7] Later in this submission we provide a case study from a current consumer complaint to illustrate this point about the hollowness of purported 'consent'-based data sharing.

We also dispute claims that the data being shared is not 'personal information' in the first place.[8]

The brokering players bringing it all together: one example

We submit that every day, Australian consumers entrust their personal information with organisations in order to facilitate a particular type of transaction such as renting a new home, as a consequence of a major life event such as suffering a medical event, or simply by conducting their day-to-day lives, both online and offline.

This trust should not be abused with the re-purposing of personal information for customer profiling and marketing purposes, *at the targeted, individual level*, by unrelated entities.

---

[6] See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4224653

[7] See a discussion of the law of consent under the Privacy Act and our arguments against the claims made by media publishers turned first party data brokers (data sellers) to be using consent-based personal information sharing, in '*The great con job: how the media and marketing industry is getting away with tracking Australians*', 1 August 2023, at https://www.salingerprivacy.com.au/2023/08/01/media-and-marketing-industry-blog/

[8] See our arguments against the claims made by media publishers turned first party data brokers (data sellers) that the data being shared is not 'personal information', in '*The great con job: how the media and marketing industry is getting away with tracking Australians*', 1 August 2023, at https://www.salingerprivacy.com.au/2023/08/01/media-and-marketing-industry-blog/

By way of example, we note that the Issues Paper describes CoreLogic as:

> "a property data and analytics company that produces a range of products including housing affordability reports, construction reports, sales and auction result data and valuation models. Customers include businesses involved in commercial and residential real estate, banking and finance, and construction, as well as the public sector".

While the sale of "property insights"[9] sounds benign, a separate data broker known as SMRTR uses CoreLogic property listing and transaction data *at the individual level* to identify and enable direct marketing to 'home movers':[10]

> "Moving home is a major life event that spikes purchase and service relationship changes. We leverage CoreLogic property data to identify:
>
> - Sellers: listing their property for sale and releasing equity.
> - Movers (renters & owners): starting their new life in the property.
> - Anniversary dates: which identify when annual contracts for things like Home & Contents insurance are due for renewal.
>
> Use cases
> The possibilities are endless, but the most common applications for this data asset include:
>
> - General insurers: Movers are 2.3 times more likely than the general population to switch their Insurance provider and our estimated insurance anniversary date has been proven to have a 3 times campaign uplift for prospects that have moved within the last five years.
> - Utilities: The moving event is highly correlated with switching gas and electricity providers (2.8 times more likely) presenting opportunities to help existing customers transfer their relationship to the new property and acquire new prospects.
> - Retailers: can have conversations with new customers in the area, especially on hardware, homewares, white goods, and local services.
> - Car manufacturers/dealers: Our analysis of movers data combined with our automotive data shows that there is a six-month window for buying new cars after people move into a new home.
> - Media publishers: can add value to the audiences by providing premium advertising to companies that want to communicate with home movers."

[9] https://www.corelogic.com.au/about-us/who-we-are accessed 7 August 2023
[10] https://smrtr.com.au/audience-segments/home-movers/ accessed 7 August 2023

CoreLogic is not the only source of data used by SMRTR, and 'home movers' is not their only category of consumers. In fact SMRTR claims to have "over 500 unique audiences, ready and available for activation in any environment",[11] which "cover 85% of the population".[12]

Other market categories also include people who are 'Ready to refinance', 'Fun-loving fifties', 'Business registered at a home address with between 11 and 50 employees', 'Toyota buyers', 'Tradies' (drawn from "Devices seen at Bunnings"), 'Cardiologist visitors' ("Mobile phone geobehaviour and/or content consumption suggests they have visited a Cardiologist"), 'Obstetricians And Gynaecologists Visitors' (likewise based on mobile phone location and online content consumption), and 'Personal Loan – Behavioural' (which is drawn from "Devices seen at financial institutions focusing on personal finance, financial planning & tax planning").

They claim that "All of our data is directly connected to their corresponding audiences via address, email, social, phone and MAID".[13] (MAID in this context means Mobile Advertising ID, i.e. a mobile phone device identifier).

According to an earlier version of its Privacy Policy we viewed last year, SMRTR collects personal information

> "from a wide number of sources, including, but not limited to:
>
> - directly from you
> - publicly available sources, such as Australia Post, Australian Electoral Commission, Telstra, Australian Communications and Media Authority and Australian Securities and Investment Commission
> - other organisations, including market research organisations, to whom you have provided consent to the collection, use and disclosure of your Personal Information for direct marketing by third parties".[14]

While SMRTR doesn't explain where their mobile phone location data is sourced from, their website provides an example of how they use such data to connect online and offline behaviours, and then deliver personalised advertising or other content accordingly:

> "As we continue to move towards 'people-based marketing', location data remains unrivaled (sic) in its ability to highlight purchase intent and real-world behaviour.
>
> While someone looking at pet equipment online may or may not own a dog, someone that visits a pet store in the real-world and dog parks is more than likely to

[11] https://smrtr.com.au/audiences/ accessed 7 August 2023
[12] https://smrtr.com.au/data-onboarding-activation/ accessed 7 August 2023
[13] https://smrtr.com.au/data-onboarding-activation/ accessed 7 August 2023
[14] https://smrtr.com.au/privacy-policy/ as accessed 24 October 2022; more information available to the ACCC on request. As at 7 August 2023, this text has been replaced with "To provide our data analytics products and services we source compliant data from third party providers."

own a dog. It is here that location data can start to help marketers when it comes to connecting the dots between the online and offline worlds".[15]

In order to connect multiple points of data about individuals, SMRTR uses what they describe as an 'Identity Graph':

> "We combine a range of privacy-compliant IDs to create a connection between offline and online identities, onboarded in your preferred environment".[16]

Their website says:

> "We collect a wide range of data on people, consumption, and behaviour across key industries. We leverage data assets to create business intelligence products that can be used for analysis and marketing.
>
> With smrtr Identity Graph providing the connector between different identifiers and our own data… and already-built connections into technology to drive seamless communication strategies and execution".[17]

In an earlier version of their website, SMRTR was more explicit about what they do, and the fact that their 'Identity Graph' enables them to build profiles on individuals who can then be targeted online or directly by companies:

> "Identity Graph enables multiple data sets to be connected together while maintaining consumer privacy and data security. This enables our clients to:
>
> - Connect our data via whichever IDs they have. Insights can be aggregated for the whole customer base, a segment, or **mapped back to individual customers in CRM systems**
> - Clean, de-identify, and connect first-party data to digital connectors (which is not dependent on cookies) to **enable the targeting of known customers wherever and whenever they are online**
> - Connect our audience segments or custom data to your internal customer and advertising technology (CRM, DMP) or external channels (publishers, DSPs).
> - **Find lookalikes for targeting** in the digital ad-tech ecosystem with their media partners".[18] (emphasis added)

[15] https://smrtr.com.au/news-views/connecting-the-dots-how-you-can-use-location-data/ accessed 7 August 2023
[16] https://smrtr.com.au/data-universe/ as it appeared when accessed on 7 August 2023
[17] https://smrtr.com.au/data-universe/ as it appeared when accessed on 7 August 2023
[18] https://smrtr.com.au/data-assets/identity-graph/ as it appeared when accessed on 24 October 2022; screenshots available to the ACCC on request.

A video linked from the SMRTR website also describes how they use people's personal information to build or add to their 'identity graph' or 'spine'.[19]

> "We... bridge the gap between companies that want to monetise their second-party data assets and companies that want to widen (the) information about their customers.
> …
> By combining our data assets with our SMRTR data universe, we are essentially creating something that is greater than its individual parts."

It then describes the process of bringing together "multi-level second party datasets from our clients and network":

> "reading in the data assets, combining them, and combining them with our SMRTR data universe – our spine data – and the way we do that is with our Identity Graph, which is essentially a matrix of connectors, that enables us to bring disparate datasets together."

We strongly submit that Australians are highly unlikely to be aware, and would indeed likely be horrified to learn, that intimate details about their life - such as that a woman has visited a gynaecologist – are being collected from our mobile phone location data, online browsing habits and other sources, collated into customer profiles, monetised, traded between companies and used by companies or bad actors for direct, personalised marketing or other messaging, influencing or decision-making purposes, without the participation – let alone consent – of either the woman or her gynaecologist.

We submit that the collection of such personal information, about identifiable and addressable individuals, is likely to breach APPs 3.5 (unfair means of collection) and 3.6 (indirect collection) in the Privacy Act. This is true of all categories from 'Tradies' to 'Home movers'. However in addition, data points and inferences found in categories relating to pharmaceuticals and healthcare squarely constitute 'health information', which is a type of 'sensitive information' under the Privacy Act,[20] which also requires consent for its collection (APP 3.3).

SMRTR's current Privacy Policy claims:

> "We do not collect sensitive data, as defined by the Privacy Act, such as, but not limited to, information relating to health, sexual orientation, racial or ethnic origin, political opinion/association, religious beliefs, membership of a trade or professional association and we do not collect banking or credit card information".[21]

[19] Video loaded on YouTube on 24 August 2021 and accessed on 5 October 2022 at https://www.youtube.com/watch?v=iHL8MKMXxzM&t=93s
[20] See http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/pa1988108/s6.html#sensitive_information
[21] https://smrtr.com.au/privacy-policy/ accessed 7 August 2023

We dispute the claim that SMRTR does not collect sensitive information, given the broad definition of 'health information' in the Privacy Act,[22] and the inferences such as 'Cardiologist visitors' upon which SMRTR trades.

Indeed the Facebook page of SMRTR contains a number of complaints from Australian consumers about their collection and use of their personal information for marketing purposes, including the direct marketing campaigns of pharmaceutical and medical screening companies.[23]

Later in this submission we have detailed a case study involving an Australian consumer who has raised a complaint with the OAIC about SMRTR and other parties collecting, using and disclosing her personal information for medical-related direct marketing, without her consent.

Misleading claims about privacy-protecting practices

We submit that claims about data 'aggregation', 'de-identification', 'anonymisation', 'privacy-first', 'privacy-compliant IDs', 'privacy preserving technology' and the like are commonly used by participants in the data brokering industry to allay the privacy concerns of consumers and regulators alike. However we argue that consumers may be misled by such phrases.

We also dispute companies and/or data brokers' reliance on 'de-identification' in particular as their method for complying with (and/or their purported ground for not needing to comply with) the Privacy Act.

For example, while SMRTR claims on its Facebook page that "Our data universe contains 16m Australians mapped to a variety of data assets and **aggregated to protect privacy**"[24] (emphasis added), their own website contradicts their privacy-protecting claim, stating that "All of our data is **directly connected to their corresponding audiences** via address, email, social, phone and MAID" (emphasis added).[25]

Further, we submit that the current trend of using 'data clean rooms' to bring different companies' datasets together is merely a way of laundering data.

[22] http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/pa1988108/s6fa.html
[23] https://www.facebook.com/smrtrau/ accessed 7 August 2023. Screenshots have been taken and can be supplied to the ACCC on request if required.
[24] See the Facebook post and video from 17 February 2022 at https://www.facebook.com/smrtrau/videos/our-data-universe-contains-16m-australians-mapped-to-a-variety-of-data-assets-an/902143313746069/ accessed 7 August 2023
[25] https://smrtr.com.au/data-onboarding-activation/ accessed 7 August 2023

Data clean rooms are laundering data

The industry group Interactive Advertising Bureau (IAB) promotes data clean rooms as an example of the use of "privacy preserving technologies".[26] They define a data clean room as "a secure collaboration environment which allows two or more participants to leverage data assets for specific, mutually agreed upon uses, while guaranteeing enforcement of strict data access limitations".[27]

Their use cases include:

- "Addressability and activation of audiences by advertisers
- Consumer insights and data enrichment using both internal organizational sources as well as external data
- Optimization and Measurement".[28]

(It is worth noting that the IAB's definition of addressability is "Ability or extent of capability to **uniquely identify an individual** or a device between data sets of two or more parties in a given context e.g. targeting individuals with advertisements", while audience activation refers to "A process of connecting advertiser target audience with publisher audience **for targeting them** through digital advertising channels".)[29]

Data broker SMRTR describes their 'data pooling' as:

> "combining together data to improve the overall effectiveness. This is otherwise known as second party data.
>
> Given the need to develop better customer relationships, companies are now looking beyond their own customer data to create a more well-rounded view".[30]

According to the International Association of Privacy Professionals (IAPP):

> "Participating in data clean rooms … allow(s) companies to merge or match first-party data sets to create fresh data analytics segments, while withholding personally identifiable information from involved parties.
>
> Popular and frequently-used clean room providers currently include Amazon, Disney, Google, Habu, LiveRamp and Snowflake".[31]

---

[26] https://iabtechlab.com/datacleanrooms/ accessed 7 August 2023
[27] IAB, *Data Clean Rooms: Guidance and Recommended Practices Version 1.0*, 5 July 2023, at https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf
[28] https://iabtechlab.com/datacleanrooms/ accessed 7 August 2023
[29] See IAB, *Data Clean Rooms: Guidance and Recommended Practices Version 1.0*, 5 July 2023, p.5, at https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf
[30] https://smrtr.com.au/news-views/data-pooling-what-is-it-and-why-does-it-work/ accessed 7 August 2023
[31] IAPP, *Data clean rooms: An adtech privacy solution?*, 24 January 2023, at https://iapp.org/news/a/data-clean-rooms-an-adtech-privacy-solution/

In an op-ed by LiveRamp COO Melanie Hoptman for an Australian industry magazine, Hoptman writes:

> "Data clean rooms are safe and neutral spaces for data collaboration and partnerships to exist without either party having access to the other's personally identifiable customer information (PII)".[32]

(We note that the phrase "PII" means nothing in Australian privacy law, but is a term of art often used in the USA to mean something narrower than 'personal information'.)

She continues:

> "For example, at LiveRamp we have Safe Haven which is an enhanced clean room that is neutral, interoperable and permission-based. It provides the foundation for data collaboration between brands, retailers and media companies to create audiences for targeting and personalisation in a privacy-first way. Beyond this, Safe Haven also allows marketers to activate data, find new audiences, optimize and measure campaigns.
> …
> Data collaboration is advantageous in meeting these needs for several reasons. One, it can **make first-party data accessible to CPGs or suppliers who lack the necessary 1:1 relationship with customers**… Two, it can forge new partnerships between companies who may not have obvious audience overlap. Partnering for data collaboration will offer a chance to **unlock new insights and reach new individuals** throughout the customer journey. Third, it can also **bring together conversion and exposure data** so companies can measure the business outcomes that matter most to their bottom line." (emphasis added)

By re-framing 'privacy' as simply 'data security', LiveRamp claims to deliver privacy:

> "Security and privacy are fundamental to data clean rooms. Since data never leaves the data owner's control, these environments create a balance between privacy and utility. A premier data clean room will also provide advanced privacy controls to each party, including encryption, so the data can't be misused."[33]

However if Company A can learn new insights about their own customers *at the addressable individual level*, from some form of data matching process with data about the customers of Company B, according to the OAIC this will constitute a 'collection by creation', which must comply with APP 3.[34]

---

[32] Melanie Hoptman, 'Why data clean rooms can save your marketing strategy in the looming recession', B&T magazine, 10 January 2023, at https://www.bandt.com.au/why-data-clean-rooms-can-save-your-marketing-strategy-in-the-looming-recession/

[33] Melanie Hoptman, 'Why data clean rooms can save your marketing strategy in the looming recession', B&T magazine, 10 January 2023, at https://www.bandt.com.au/why-data-clean-rooms-can-save-your-marketing-strategy-in-the-looming-recession/

[34] See *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V.* [2021] AICmr 34, at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/34.html

It doesn't matter that the method used to garner that insight may have involved de-identification of the data in the middle of the data matching process. The use of pseudonyms such as hashed identifiers, and/or probabilistic matching techniques, exist to enable links to be drawn between unrelated datasets, such that with the required degree of confidence, the process can establish that customer 12345 from Company A, and customer 67890 from Company B, are the same person.

It doesn't matter that Company A doesn't 'see' Company B's 'raw' customer data. The output – the 'enriched' customer data for Company A - is still 'personal information', which is regulated under the Privacy Act. Therefore neither companies A nor B should be collecting or disclosing their customer data via data clean rooms, except in compliance with APPs 3 and 6.

That this is the case is hinted at in the IAB's guidance on data clean rooms. It takes until page 25 of the document to admit it, but the IAB does state that:

> "Data enrichment where net new insight or intelligence is appended directly to an underlying raw dataset … (may) violate the privacy and data governance principles of the … Data Contributors."[35]

The IAB counsels companies to "consult with their legal counsel about specific steps they should undertake to ensure compliance".[36]

Yet in the words of marketing industry editor Andrew Birmingham, "marketers often fall back on a technical defence: It's first party data and it's encrypted: as if owning a bludgeon that no one understands makes it ok to conk a customer on the head."[37]

In our submission, creating 'a more well-rounded view' of customers, aka customer enrichment, without those consumers' active participation or consent, is a practice potentially in breach of the Privacy Act. Using privacy-preserving techniques like secure collaboration workspaces, encryption or differential privacy may protect the security of data during data flows, but they do not impact on whether the data flows are lawful in the first place.

We draw the ACCC's attention to the fact that the practices described by data brokers or data clean room providers as "privacy-compliant" or "privacy-first" are similar to the data matching and linkage processes widely used in the research sector, where linkage via pseudonymous keys and/or probabilistic matching is conducted by trusted middle parties within secure workspaces.

---

[35] See IAB, *Data Clean Rooms: Guidance and Recommended Practices Version 1.0*, 5 July 2023, p.25, at https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf
[36] See IAB, *Data Clean Rooms: Guidance and Recommended Practices Version 1.0*, 5 July 2023, p.24, as above
[37] 'Treat data like we treat ESG, don't try to hide under privacy tech', Infosum GM tells IAB Privacy and Data Summit; cue tumbleweeds', *Mi3*, 4 May 2023, at https://www.mi-3.com.au/04-05-2023/we-should-treat-data-we-treat-esg-says-infosum-gm-cue-tumbleweeds

The key difference between the sectors is that in our experience organisations participating in the research sector, such as research institutes or government agencies conducting research critical for policy areas from healthcare to education to disability care to child protection, would not dream of suggesting that their data matching and linkage practices are sufficient to ensure compliance with APPs 3 (collection) or 6 (use and disclosure), let alone render data 'de-identified' to the point that privacy laws no longer apply.

Instead, when not grounded in express consent (which as noted above requires prior ethical approval to ensure such consent is informed, specific, voluntary etc), data matching and linkage for research purposes typically relies on specific *exceptions* to APPs 3 and 6 (or State-equivalent privacy principles governing collection, use and disclosure). Those research exceptions have been granted by the legislature on public interest grounds, and are subject to complex and nuanced ethical approval and oversight processes before they can be relied upon. No such exceptions have been granted for marketing use cases.

The use of commercial 'data clean rooms' to allow unrelated companies to learn new insights about individuals, in the absence of true consent from those individuals, makes a mockery of our privacy laws. It also makes a mockery of the research sector, and the months and years that researchers put into ensuring that their projects can comply with privacy requirements.

Opacity prevents consumers from exercising their rights

Data brokering practices are opaque, which makes it very difficult for consumers and regulators alike to test for compliance with consumer protection or privacy laws. We have illustrated this with a current case study, below, involving a consumer known to us.

In that case, a consumer who received unsolicited marketing from a medical screening company has thus far gone through three separate companies, none of whom she had ever heard of or had any relationship with, without yet getting to the bottom of who sold or shared her data without her consent to start with. (The case study demonstrates that consent was not obtained.)

The work done by ABC journalists to illustrate how often consumers' personal information has been caught up in data breaches[38] – breaches at companies most of us have never heard of – illustrates both the opacity of the data brokering industry, and the capacity for consumers to be harmed as a result. (The author of this submission, for example, discovered, using the ABC's tool, that her personal email address had been involved in data breaches involving seven companies, only one of whom she had ever had a relationship with.) This adds to the evidence that online identifiers (even hashed email addresses) and

[38] See 'See your identity pieced together from stolen data', 18 May 2023, at https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688

data enrichment practices need even stronger regulation under the Privacy Act than that proposed by the Attorney-General's Department in its current review of the Act.[39]

Consumers should not be law enforcers

Question 22 in the Issues Paper, which asks how to "better educate and empower consumers", suggests that consumers should being doing the enforcement legwork. We disagree.

Consumers should not have to enforce their own rights, or test for compliance with consumer protection or privacy laws. In any case, as our case study below illustrates, even a well-educated and empowered consumer may be frustrated in their attempts to enforce their rights, let alone obtain a remedy.

The system is broken, and educating consumers will not fix it.

[39] See our analysis of the flaws in the proposed new definition of 'personal information' in 'To fix the Privacy Act, we need one extra sentence', 19 April 2023, at https://www.salingerprivacy.com.au/2023/04/19/one-extra-sentence/

Case study

A friend of the author of this submission has given Salinger Privacy permission to use her experience publicly as a case study.

This case study illustrates a number of concerns, first with the data brokering industry, and second with the regulatory environment facing consumers who seek to enforce their consumer and privacy rights.

For the purposes of this case study we have used the pseudonym 'Justine' in place of the real name of the consumer.

How Justine's data has been shared

In September 2022, Justine received a direct marketing letter to her home address from a biotechnology company promoting a medical scanning service. The letter arrived not long after Justine's 70th birthday, and the medical scanning service related to a disease affecting older women. Both the envelope and the letter noted that people over 70 can have the scan 'bulk billed'.

Justine had never heard of the company advertising the medical scanning service, and wanted to find out how the company knew of her address, age and gender, such as to send such a targeted marketing message about a health condition.

For the next six months, Justine tried in vain to find out how her personal information ended up with the biotechnology company. The trail led from the biotechnology company (Amgen) to one data brokering company (SMRTR), and then to another (Eight Dragons), before the trail stopped dead.

Along the way, Justine discovered that these companies had various forms of information about her. For example, SMRTR held personal information about Justine including:

- Title
- First name
- Surname
- Gender
- Date of birth
- Home street address
- Home phone number

- A personal email address (accurate and current), and
- Another email address (no longer in use).

She also discovered that SMRTR held two pages worth of 'Modelled Data' about her, such as:

- Working status (i.e. Retired)
- Owns her own home
- Number of people living in the home
- Low disposable income
- Has no children
- Has no investments
- Has no credit card
- Not 'high affluence' or 'high net worth'
- Not 'blue collar'
- Is likely to donate to charity
- Is of an average likelihood of renovating

Justine does not believe the explanation given for how SMRTR had all this data about her: that she had supplied these details (and consented to their use for direct marketing) when she entered a competition in 2019.

There are five reasons why Justine does not believe SMRTR's explanation:

- Justine claims to never enter competitions, and does not remember entering a 'Win a Trip to London' competition on 1 January 2019.
- The company making the claim (Eight Dragons) had no proof that she had done so, such as a copy of her competition entry form.
- The details allegedly collected directly from her via the competition entry in 2019 included details about Justine's life such as an old work email address, that had not been active for many years prior to 2019.
- The data collected about her included inferences such as 'not blue collar' and likelihood of donating to charity or renovating, not likely to have been details a competition entry form would ask for directly.
- In the data held about Justine by SMRTR was a field labelled "SelfReported", which was explained to mean "An indicator on whether the personal information has been sourced from a supplier which uses self-reported information, i.e. surveys or competition entries, 0=No, 1=Yes". In Justine's record, the field was "0", meaning "No".

In other words, SMRTR told Justine that her personal information had been collected with her consent when she entered a competition, but the information they held about her (supplied to Justine when she exercised her Access rights under the Privacy Act) in fact stated the opposite.

So where did all this information come from? Justine has not been able to find out.

What happened when Justine complained

Once the trail stopped dead, Justine made a complaint to the OAIC, in May 2023. Overleaf we have reproduced a copy of Justine's correspondence with the OAIC, but with details of Justine's name, contact details and date of retirement redacted. (Unredacted copies of all correspondence, including between Justine and the marketing and data brokering firms, is available to the ACCC on request.)

Justine's complaint related to the collection, use and disclosure of her personal information without her consent, in breach of a number of APPs.

The OAIC replied by email on 31 May 2023:

> "We will first assess your correspondence and consider if we are able to assist you. If we are unable to assist, or require further information, we will contact you. Due to the volume of correspondence we receive, this may take some time. …
>
> Unfortunately, we are not able to allocate all complaints to a case officer immediately. We will contact you as soon as we can. Once a complaint is allocated, a staff member will make contact to discuss the next steps."

It is now three months later, and Justine has received no further correspondence from the OAIC.

The unsolicited marketing continues

Meanwhile also in May 2023, Justine received a letter from another organisation unknown to her - CBM Australia, a Christian charity - soliciting a donation. In the fine print at the end of the letter, CBM Australia stated that they had sourced Justine's information "via third party sources" and that "we may disclose your data to other organisations in Australia or overseas". They had already allocated Justine a 'supporter number'.

Justine sent them a letter on 11 May asking how they obtained her personal information. CBM Australia has not replied.

On 22 May 2023 Justine received a letter from Anglicare, also soliciting donations. Justine does not recall any earlier contact with the Anglicare. That their letter begins with "I'm not sure if you've heard of Anglicare…" would suggest she is correct in her recollection. In the fine print of the letter, Anglicare states that: "Occasionally we allow like-minded organisations to contact you with information that may be of interest to you, including some organisations located outside Australia. These organisations allow us to do the same and in this way we can reach more people with vital information."

Justine notes that SMRTR's "Modelled Data" on her includes a prediction of a 'high' likelihood of her donating to charity. She suspects – but of course does not know – that CBM and Anglicare may have received her personal information from SMRTR.

As at 4 August 2023, Justine has received no further correspondence from the OAIC, or indeed any other party.

Copy of complaint lodged with the OAIC

[REDACTED ADDRESS]
5 May 2023

Office of the Australian Information Commissioner (OAIC)
GPO Box 5288
SYDNEY NSW 2001

Dear OAIC,

This is a privacy complaint about the collection, use and disclosure of my personal information without my consent by the following three businesses, in circumstances which I believe breach the Australian Privacy Principles (APPs).

These businesses are all unknown to me; I have not had any dealings with them prior to this privacy issue arising.

Amgen Australia Pty Ltd
PO Box H125
Australia Square NSW 1215
Contact: Ms Susan Dean, Data Privacy Officer
[REDACTED EMAIL ADDRESS]

smrtr Pty Ltd
C/O Wheeler Accounting & Taxation Pty Ltd
Suite 246, 117 Old Pittwater Road
Brookvale NSW 2100
Contact: Mr Lee Coats, Director of Customer
[REDACTED EMAIL ADDRESS]

Eight Dragons Digital Pty Ltd
124 Missenden Road
Camperdown NSW 2065
Contact: Mr Earl Roberts, Chief Marketing Officer
[REDACTED EMAIL ADDRESS]

I have complained to these businesses, but am dissatisfied with their responses. A summary of our correspondence follows.

Chronology

On 30 September 2022, a few weeks after my 70th birthday, I received a letter from Amgen Australia Pty Ltd (a company I had never heard of before) inviting me to have a DEXA scan for osteoporosis. The letter was direct marketing, disguised as a 'disease education message'. It was aimed at people

over 70, and it was sent to my home address. Although my name was not on the letter, there is a unique bar code. (Copy attached)

The letter contained the statement:

> *Name and addresses have been sourced through SMRTR. Your details have been provided to us by SMRTR Pty Ltd. If you wish to opt out of receiving marketing communications or have any questions relating to your data privacy please visit their website - www.smrtr.com.au/contact-us.*

I note particularly that Amgen themselves treat this letter as marketing, and they state they collected my name (even though my name did not appear on the letter).

I was concerned about how this company I had never dealt with knew that someone aged over 70 lived at my address.

On 3 October 2022 I emailed smrtr Pty Ltd:

> *Please provide me with copies of my personal and health information which your company has collected and tell me how and from whom this information was obtained.*

On 13 October 2022 I emailed Amgen Pty Ltd and smrtr Pty Ltd with formal complaints and requests for Access and Correction. (Copies attached)

On 31 October smrtr Pty Ltd provided me with copies of the information it held about me – my name, residential address, gender, date of birth, home phone, my current email address and a former email address (which account was closed in 2012).

It also provided two pages of "Modelled Data" about me, including various inferences about me, such as that I am single, retired, not 'high affluence', not 'blue collar', etc. (Copy attached) I have been given no explanation about where this information about me was collected from, or how these inferences were drawn.

On 4 November 2022 smrtr Pty Ltd informed me they had sourced my information from Eight Dragons Digital and that:

> *All of our datasets are privacy compliant under the Australian Privacy Principles (APPs) and have consent from individuals at the time of collection for the purposes for which we use them. As standard practice, our contracts with data partners require them to warrant that their data collection practices comply with the Privacy Act 1988 and the Spam Act 2003.*
>
> *Eight Dragons Digital have advised that the data was collected from you on 01/01/2019 when you entered a "Win a Trip to London" competition. The competition's terms and conditions referenced this privacy policy:*
> *https://www.8ddigital.com.au/PrivacyPolicy*
> *We have also attached the data collection statement which references this Privacy Policy.*
> (Copy attached)

On 8 November 2022 Amgen replied to my complaint of 24 October 2022. (Copy attached) They had also been informed by smrtr Pty Ltd that my information was obtained by Eight Dragons Digital when I entered a competition.

I note that I do not believe this claim (that my personal information was collected when I entered a competition) to be true. Firstly, because I make a habit of not entering competitions. Secondly, because one of the email addresses allegedly collected from me on 1 January 2019 was an old work email address not in use since [REDACTED RETIREMENT YEAR, WELL BEFORE 2019].

On 18 November 2022 I emailed smrtr Pty Ltd, informing them that I never enter competitions and asking them provide me with evidence of their compliance with the APPs and of my consent to their collection, use and disclosure of my information. I asked them to provide a copy of the completed competition entry form and how it was presented to me and how I submitted it. (I also noted that it was odd that I would have supplied two email addresses on an entry form – my current one, and an old work address which account was closed at my retirement in [REDACTED RETIREMENT YEAR, WELL BEFORE 2019].) (Copy attached)

On 23 November 2022 smrtr Pty Ltd emailed me that:

> *As the promoter and collector of the data, they* [Eight Dragons Digital Pty Ltd] *are best placed to provide you with the requested information on the competition and have a robust process for handling and resolving consumer complaints. We have escalated your concerns to the CEO of Eight Dragons Digital, Earl Roberts, who has agreed that from a legal and privacy perspective, it would be best for him to liaise with you directly on the aspects that relate to the competition. With your permission, we can forward your email to him;* (Copy attached)

On 25 November 2022 I asked smrtr Pty Ltd to forward my email to Eight Dragons Digital.

On 30 January 2023, having no reply from Eight Dragons Digital Pty Ltd, I emailed them, asking that they address the matters in my email of 18 November 2022 to smrtr Pty Ltd. (Copy attached)

On 31 January 2023 Eight Dragons Digital Pty Ltd replied:

> *I have forwarded your email through to our privacy department who will get the answers to your questions for me. … I should have the information to you by weeks end*

On 22 March 2023 I emailed Eight Dragons Digital Pty Ltd and smrtr Pty Ltd stating I was still awaiting a response. They have not replied.

My complaint

I am very concerned that these data brokers and Amgen, completely unknown to me, have secretly collected, shared and monetised my personal information.

Personal information

In particular, I believe that the information collected, used and disclosed about me by Eight Dragons Digital Pty Ltd and smrtr Pty Ltd is clearly my 'personal information', including both facts (such as my name, home address, date of birth, gender and contact details) and opinion (multiple inferences).

I also believe that the information disclosed by smrtr Pty Ltd to Amgen Pty Ltd, and collected by Amgen Pty Ltd, was also my personal information. Even though the letter addressed to me by Amgen Pty Ltd did not include my name, they certainly had enough information about me to be able to distinguish me from other people and identify me as a person aged over 70, living at a particular address, and target me for a particular type of direct marketing accordingly. Further, I note that Amgen stated that they collected my name (even though my name did not appear on the letter).

The APPs

I consider all three businesses are potentially in breach of APP 3 in the way they have collected my personal information.

In particular, I allege breaches of:

- APP 3.2, because it was not reasonably necessary for any of these businesses to collect my personal information for their functions or activities
- APP 3.5, because I believe the means of collecting my personal information was not "lawful and fair" (noting in particular the reasons outlined above for I do not believe the claim that I provided my personal information via a competition entry; and in any case no explanation has been provided for the source of the inferences drawn about me), and
- APP 3.6, because they collected my personal information indirectly, in circumstances where it was not "unreasonable or impracticable" to expect them to *not* collect personal information indirectly.

I consider all three businesses are potentially in breach of APP 6 and/or 7 in the way they have used my personal information.

In particular, I allege breaches of APP 7 because my personal information was collected from a third party instead of from me, and none of these businesses had my consent to use or disclose my personal information for direct marketing, when - in the circumstances of an indirect collection - my consent should have been obtained under APP 7.3.

Finally, I also consider that Eight Dragons Digital Pty Ltd and smrtr Pty Ltd are potentially in breach of APP 6 and/or 7 in the way they have disclosed my personal information.

I ask the OAIC to investigate my complaint.

Yours sincerely

[REDACTED NAME]
[REDACTED EMAIL ADDRESS]
[REDACTED PHONE NUMBER]

Further resources

For further details on points raised in this submission, please see:

- Our critique of the conduct of 'first party' data brokers such as News Corp, Nine Group and Seven West Media
- Our detailed submission to the Attorney-General's Department on the Privacy Act Review Report, 2023
- Our analysis of the flaws in the proposed new definition of 'personal information'
- Our analysis of privacy harms in 'Big Tech, Individuation, and why Privacy must become the Law of Everything'

About the author

This submission was prepared by Anna Johnston.

Anna Johnston is founder and Principal of Salinger Privacy. Anna has served as:

- Deputy Privacy Commissioner of NSW
- Chair of the Australian Privacy Foundation, and member of its International Committee
- a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
- a member of the Advisory Board for the EU's STAR project to develop training on behalf of European Data Protection Authorities
- a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
- a Member of the Asian Privacy Scholars Network
- a member of the Australian Law Reform Commission's Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
- an editorial board member of both the Privacy Law Bulletin and the Privacy Law & Policy Reporter.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the global designation of Fellow of Information Privacy (FIP).

In 2022, Anna was honoured for her 'exceptional leadership, knowledge and creativity in privacy' with the IAPP Vanguard Award, one of five privacy professionals recognised globally whose pioneering work is helping to shape the future of privacy and data protection. While her day-to-day work involves assisting clients to develop innovative approaches to privacy protection, the Vanguard award was bestowed in reflection of Anna's contributions to the privacy profession, and to the protection of privacy for the benefit of all.

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).

About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy consulting services, specialist resources and training.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Salinger Privacy offers specialist consulting services on privacy and data governance matters, including Privacy Impact Assessments and privacy audits, and the development of privacy-related policies and procedures. Salinger Privacy also offers a range of privacy guidance publications, eLearning and face-to-face compliance training options, and Privacy Tools such as templates and checklists.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

SalingerPrivacy

We know privacy inside and out.

Salinger Consulting Pty Ltd

ABN 84 110 386 537

PO Box 1250, Manly NSW 1655

www.salingerprivacy.com.au