SUBMISSION BY CIVIC DATA

PRIVACY ACT REVIEW - DISCUSSION PAPER, OCTOBER 2021

January 2022

SUITE 03 LEVEL 12
14 MARTIN PLACE
SYDNEY NSW 2000

TEL +61 2 9346 8434

info@civicdata.com.au
www.civicdata.com.au

ABN: 58 643 216 166

Attorney-General’s Department

4 National Circuit

Canberra ACT 2600

By email: PrivacyActReview@ag.gov.au

24 January 2022

Review of the Privacy Act 1988

Civic Data welcomes the opportunity to make the following submission in relation to the review of the *Privacy Act 1988* (Cth).

At Civic Data, we are vertical integration data specialists, providing advanced insights into the compliant use of big data for marketing and communications. We are an Australian consulting firm, founded last year to assist businesses with technology and advise on how to collect, organise, analyse and activate data for privacy first marketing and communications initiatives.

While other experts have made submissions where their horizontal expertise is relevant, our focus is on deploying tools and strategies that use data for digital targeting, digital measurement and digital engagement in relation to marketing and communications.

Our submission specifically addresses three issues raised by the Issues and Discussion papers:

1. What is meant by 'technical and inferred' information;
2. Introduction of statutory fines for malicious re-use of de-identified data; and
3. Options around pro-privacy default settings.

These topics are relevant to Questions 2-4, 6, 25-32, 34, 37-40, 42-47, 53-55, 58-61 within the discussion paper.

In addressing these three main issues, we note the extremely fast-paced developments in this space. For this reason, we highlight the difference between what “Digital” means currently and what it will mean in the near future.

It is our aim to raise awareness about aspects that may not have been highlighted in other submissions of the digital economy and data that can be collected and used.

What is “Digital”?

The concept of “digital marketing” and what is included in this category is larger than ever and is constantly growing. It extends well beyond emails, website cookies & mobile phones as discussed below.

A number of examples of what could be currently included under digital marketing:

- Digital motorway and shopping centre billboards that use data collected from mobile phones and Wi-Fi for targeting and measurement;

- “Smart shelving” in supermarkets that can detect gender, age and race to display dynamic pricing and relevant messaging;1
- “People-tracking systems” that track customer journeys through a store and match the very microsecond that same customer uses a Rewards Card or Credit Card at the automatic payment counter;2
- Movies / TV shows sold through the living room TV using algorithms powered by the very same behavioural data collected by a paid streaming TV subscription and/or layered with data from search engines, YouTube views and other data;
- Video games on gaming consoles that can target individuals with messages and characters, blended so perfectly they would not register as one-to-one advertising;3 and
- Screens within and on top of privately owned rideshare and delivery cars. While a sole trader drives these cars, every mile driven (drivers + passengers) is enriching the data and infrastructure that is owned by foreign entities such as Uber (USA), Didi (China) and Ola (India) etc. (Note: The data currently collected by these apps is inclusive of not just uniquely identifiable passenger travel patterns from habitual home location/ work location/ social activities/ mealtime events, but also facial recognition through each app where an estimated 70,000 Australian drivers must submit photos of themselves regularly).[4]

In such a rapidly expanding and developing sector, what will digital marketing data encompass in the near future? While it may seem out of scope, it is not unreasonable to think that by the time this review is completed, digital targeting, measurement and engagement will mean content displayed on innocuous “mixed reality” spectacles with a unique IP address. All major tech companies are investing in such technology and some will collect biometric data.[5] Privacy advocates have already discussed in depth elements of RayBan/Facebook’s glasses such as “filming covertly with no red recording light flashing”.[6]

With TikTok’s Chinese parent company acquiring VR headset maker Pico,[7] and the growth of the Metaverse with Facebook, Microsoft and Apple all own hardware that could collect biometric and behavior data to merge with the profiles already stored on file.[8] Even our ‘digital twins’ such as avatars, crypto wallets and digital goods could be used to identify us (if not regulated) and stored alongside other profile data.

It could mean dashboard messages within electric cars that are powered using real-time telemetry/ telematics data. This data could be collected by satellites by the same company that built the car and/or based on what/who/where the car's 7+ camera / sensors are collecting/ sharing/ storing as it drives through Australian neighborhoods.[9]

[1] Coming to store shelves: Cameras that guess your age and gender: **https://www.nbcnews.com/tech/tech-news/coming-store-shelves-cameras-guess-your-age-gender-n998391**.
[2] LiDAR vs Video for instore tracking: **https://www.asmag.com/showpost/32497.aspx**.
[3] Marketers experiment with video ads on console games: **https://www.businessinsider.com/marketers-experimenting-with-tv-ads-on-console-games-2020-7?r=AU&IR=T**.
[4] Ridesharing data and statistics: **https://www.ibisworld.com/au/industry/ridesharing-services/5540/**, **https://www.dinggo.com.au/blog/ride-sharing-statistics** and **https://www.moneyaustralia.net/uber-statistics/**. An example of where this data has been breached: **https://www.itnews.com.au/news/uber-found-to-have-breached-privacy-of-12-million-aussies-in-2016-567809**, **https://www.zdnet.com/article/uber-found-to-have-interfered-with-privacy-of-over-1-million-australians/**.
[5] Overview of Smart Glasses contenders: **https://www.cnet.com/tech/mobile/tcl-joins-the-race-to-create-ar-smart-glasses-challenging-meta-and-possibly-apple/**.
[6] Privacy Pros on RayBan Smart Glasses: **https://cybersecurityventures.com/privacy-pros-on-ray-bans-smart-glasses/**.
[7] A major player in the Chinese VR market: **www.theverge.com/platform/amp/2021/8/30/22648282/bytedance-tiktok-vr-pico-hardware**.
[8] Privacy aspects of the Metaverse: **https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/**.
[9] Harvard Journal of Law & Technology, Who Owns The Data Generated By Your Smart Car?: **https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech299.pdf**.

This real-time video/sensor data could be attached to a Unique Car ID for individual use. This could then also feed into the collective/ overlaid data from tens of thousands of cars that scan, video and map changes on daily routes from all angles, making Google Maps' Street View look antiquated.

1. Technical and inferred information

With the above examples of technical data types and collection methods in mind, we submit, in line with the majority of submissions, that the proposed expansion of terms that define "technical and inferred" information is a welcome and important revision.

In the digital economy, the ability to discern a single unique individual target and act on that has, for some time, been relatively simple. It might have just involved identifying the make of their laptop, the operating system and their browser plugins.

Through cloud computing advances and the dramatic reduction in the cost of collecting, storing and processing large amounts of data, there is now much greater ability to run large-scale deterministic and predictive strategies to seek out individuals and show individually personalised messages to them at scale & on multiple touchpoints across their device graph when using both simple and complex datasets

On the more nefarious end, the simplicity of acquiring commercially available data to "single out" an individual, was highlighted when "commercially available" location data from a vendor was used to determine that a priest had visited gay bars and private residences while using Grindr, a popular dating app[10].

Further, circumnavigating existing de-identification technology (e.g., hashing, tokenisation, identity resolution solution) is also now well within reach of any entity.

Impacts of getting this wrong

Circumnavigating de-identification technology has the potential to be much more than just a "mere" violation of human rights, breach of personal privacy and loss of anonymity. The potential risks of abuse of data pose serious threats on a national security level, globally and commercially.[11]

Having data on all aspects and information on people (often without their knowledge) and being able to use that data for whatever the entity's vested interest poses untold risk.[12]

Getting this wrong poses serious risks to our personal, national, commercial and global interests

This more than just an issue of "privacy", it has the potential to pose an existential threat if the data were to be used for nefarious purposes.

[10] Location-based apps pose security risk for Holy See: **https://www.pillarcatholic.com/p/location-based-apps-pose-security**.

[11] US security concerns on TikTok data harvesting https://www.bloomberg.com/news/articles/2020-07-14/tiktok-s-massive-data-harvesting-prompts-u-s-security-concerns, **https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738**, **https://www.reuters.com/technology/what-is-driving-chinas-clampdown-didi-data-security-2021-07-07/** and **https://www.wsj.com/articles/in-the-new-china-didis-data-becomes-a-problem-11626606002**.

[12] **https://www.businessinsider.com/china-asks-didi-delist-from-us-data-security-fears-report-2021-11?r=AU&IR=T**.

The distinction therefore between the ability to define "identify and target an individual" vs "determining the identity of an individual" is important, as both have an impact on privacy.[13]

Civic Data strongly supports wording within the *Privacy Act* that covers circumstances in which an individual is distinguished/spotlighted from others or has a profile associated with a pseudonym or identifier, despite not being named.

We would further suggest that when an entity discusses Differential Privacy as a method to anonymise data, that the privacy act also considers how hard it is to create a practical differential privacy solution. There are threats attached to each differential privacy method implemented.[14]

2. Statutory fines for malicious re-use

We support statutory fines for malicious re-use of de-identified data. We believe it would deter entities from creating the market for an asset class to feed entities that circumnavigate de-identification.

With that said, however, we suggest considering an amendment to or carve-out from Proposal 2.6. We strongly suggest that, without amendment, the re-introduction of the *Privacy Amendment (Re-identification) Offence Bill 2016* could risk throttling domestic research, development, and testing of new 'compliant' services and solutions that support a domestic digital economy already undergoing many changes.

Australian entities feel or will soon feel the CAPEX and OPEX pressures that cookie blocking, app tracking and targeting/measurement changes have already put onto them and their partners through global privacy pressures.

There is significant and proven costs for discovering and acting on erasure and preference requests across an individual's multitude of devices, operating systems, browsers. This also becomes a further problem where that data also sits across an entity's distributed storage (including files, third party systems etc.).

Civic Data proposes that the Australian Government consider a “regulatory sandpit”

For this reason, the ability to test, without prejudice, methods that *'re-identify in order to locate further locations of data in a compliant way'* would be very useful for Proposals 14.1 and Provision 15 of the Discussion Paper.

Civic Data proposes that the Australian Government consider a “regulatory sandpit” or “ethics-approved research carve-out” to create a formally sanctioned environment where these types of issues could be tested, monitored, and recorded in an approved and safe manner.

Regulatory sandpits have been very successful in driving compliant innovation and investment in the fintech sector, which is in many ways analogous to the martech and adtech markets.

[13] As highlighted in the Discussion Paper, Submission to the Issues Paper: Salinger Privacy, 5. See also Submission to the Issues Paper: Fastmail, 2.
[14] Threat Models for Differential Privacy: **https://www.nist.gov/blogs/cybersecurity-insights/threat-models-differential-privacy.**

3. Pro-privacy default settings

While we believe that enabling pro-privacy settings by default (option 1 in the Discussion Paper) would be more pleasing for privacy advocates, we would recommend opt-out options, for example, the usage of pre-checked boxes. This would ensure that data needed for the functionality of digital services/ accessibility and ONLY for that purpose is an option, This data would then only be collected to avoid impact on 'the mechanics' of how some websites/games/systems work.

With the clear and broad global shift towards data rights and data control, earning trust through being clear and fair on how data is used AND following through on those promises is what now fuels trusted value exchanges. Entities should be given the chance to prove that they can be considerate custodians of data through clear and fair value exchange.

When these settings are not correct, we see huge market interruption and regulatory risk.[15]

Those entities who do not fairly acknowledge the customer as the ultimate owner of data and preferences, will simply fall behind in the Digital Economy through lack of trust.

We understand the extraordinary stakes of getting these matters and issues balanced and correctly weighted. As global tensions increase and data utilization develops, failure to get these settings correct could lead to severe consequences.

About Civic Data

Civic Data are an Australian consulting firm who specialize in adtech, martech and the interaction of data.
We were founded in 2021 to assist businesses with technology and advise on how to collect, organize, analyse and activate data for Privacy First Marketing and Communications initiatives. We call this 'Compliant Growth'.
By securing and growing Consumer trust on how their data is used for marketing and communications purposes, we strive to help our enterprise clients to prepare their technology strategy as the global digital economy adapts to a more privacy focused ecosystem.

[15] , https://www.bloomberg.com/news/articles/2021-07-05/what-is-didi-and-why-is-china-cracking-down-on-it-quicktake.