SUMMARY

1. The personal information Facebook obtains from users is aggregated and used to train its Artificial Intelligence (AI) learning system to predict future user behaviour. There is a threat that the aggregation of data, particularly 'psychographic' data, to train its AI system allows Facebook to attain insights into users' personalities and lives beyond what they understand or intend their information to be used for.
2. These methodologies lack *transparency* as users cannot provide informed consent to the gathering and use of their private and at times, sensitive information.
3. Facebook's use of its aggregated stores of psychographic data to modify user behaviour is potentially *manipulative* and is analogous to those employed by *Cambridge-Analytica*'s psychographic 'micro-targeting'.
4. The current Privacy Principles as contained in the *Privacy Act 1988* (Cth) are inadequate to protect Australians from such abuse of their private information.
5. The use of psychographic targeting is currently exempt under the *Privacy Act 1988 (Cth)*.
6. Recommendations.

1 *Big Data & AI Learning*

As users tend not to conceive of the sheer scale of data compiled, nor the purpose and accuracy with which it is employed, Facebook essentially strips people of the right to decide how and what they will disclose in a way that undermines consumer autonomy and privacy.[1] For *each* of its 2.9 billion monthly users Facebook collects up to 52,000 data points that are then gathered into its 'hive'[2] which stores 300 petabytes of data.[3] If converted into copies of books, the information stored would stack from the earth to the moon 49 times.[4] From within this hive, Facebook's AI learning system, 'FBLearner Flow', ingests trillions of data points every day, from which its algorithmic models can make more than 6 million predictions per second.[5]

Despite the public guise that such information is employed to improve user experience, private admissions indicate more nefarious uses. In a 2017 leaked confidential document, Facebook touted its ability to exploit its vast stores of personal information, to train its machine learning system to "predict future behaviour".[6] With the ultimate aim of achieving the maximum probability that users undertake a desired action**,** Facebook use its aggregated data, particularly 'psychographic' data, to not only predict user behaviour but modify it.[7] This gives rise to the following issues:

- **[2] Invasion and Transparency:** Facebook's aggregation of data on 2.9 billion monthly users, particularly 'psychographic' data, allows its AI system to:

---

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019), 98; Attorney-General's Department, *Privacy Act Review* (Discussion Paper, October 2021) 77

[2] S Dixon, 'Facebook: number of monthly active users worldwide 2008-2022' *Statista* (Web Page, 13 February 2023) https://www statista com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~:text=How%20many%20users%20does%20Facebook,used%20online%20social%20network%20worldwide; Mat Lebowitz, 'Facebook, should we just be friends?' *VentureBeat* (Web Page, 4 September 2021) https://venturebeat com/2021/09/04/facebook-should-we-just-be-friends/#:~:text=Facebook%20is%20rumored%20to%20track,data%20points%20on%20every%20user;
Jeffrey Dunn, 'Introducing FBLearner Flow: Facebook's AI Backbone' *Engineering at Meta* (Web Page, 9 May 2016) https://code facebook com/posts/1072626246134461/introducingfblearner-flow-facebook-s-ai-backbone

[3] Ankush Sinha Roy, 'How does facebook handle the 4+ petabyte of data generated per day? Cambridge Analytica - facebook data scandal', *Medium* (Web Article, 16 September 2020) https://medium com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4#:~:text=Facebook%20generates%204%20petabytes%20of,about%20300%20petabytes%20of%20data

[4] Richard Spurlock, 'Petabyte - How Much Information Could it Actually Hold?' *CobalIron* (Web Page, 31 October 2019) https://info cobaltiron com/blog/petabyte-how-much-information-could-it-actually-hold

[5] Jeffrey Dunn, 'Introducing FBLearner Flow: Facebook's AI Backbone' *Engineering at Meta* (Web Page, 9 May 2016) https://code facebook com/posts/1072626246134461/introducingfblearner-flow-facebook-s-ai-backbone

[6] Sam Biddle, 'Facebook uses artificial intelligence to predict your future actions for advertisers, says confidential document' *The Intercept* (Web Article, 14 April 2018) https://theintercept com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/

[7] Shoshana Zuboff, *After the Digital Tornado: Networks, Algorithms, Humanity* (Cambridge University Press, 2020) 189

- a) potentially reveals sensitive information about users without their knowledge or consent, and
- b) potentially constitutes an **invasion** of privacy due to its ability to extract highly granular psychological insights.

- **[3] Subversive influence and Manipulation**: Facebook not only seek to predict but, actively attempt to modify, future user behaviour to ensure users take a desired action. To achieve this, Facebook use its AI learning system and highly granular psychographic data to identify emotional vulnerabilities, this is:
  - a) potentially manipulative,[8] and
  - b) methodologically analogous to the techniques used by Cambridge Analytica during the 2016 U.S. presidential elections.

2 Invasion & Transparency

'Psychographic' data entails information on consumers; personality traits, activities, interests, opinions, needs, values, and attitudes. [9] There is concern that Facebook's aggregation of data, particularly psychographic data, allows its AI learning system to extract highly granular insights into users beyond what they would expect. Further, that it potentially constitutes an *invasion* of privacy by enabling unauthorised access to users' personal and at times 'sensitive' information.[10]

As illustrated by Kosinski (2013), by solely relying on Facebook 'likes', an accurate prediction could be made on a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, and personality traits.[11] As defined under the *Privacy Act 1988 (Cth)* this information falls within the definition of 'sensitive information'[12].

By inference, the predictive capabilities of Facebook are substantially greater when considering the fact that 'likes' are only a fraction of the data available to it. Facebook has access to everything in the online milieu, including: photos, messages, videos, locations, communication patterns, attitudes, preferences, interests, faces and purchases.[13] There is concern that they then aggregate this data with the psychographic data of their 2.9bn monthly users and utilise it to train an AI system that makes up to 6 million predictions per second about future user behaviour.

As shown by Kosinski (2013), using a single source of data, 'likes', sensitive information that individuals have not revealed and would typically assume to be private could be accurately predicted in a statistical sense from other aspects of their lives.[14] Thus, there is concern that Facebook's use of aggregated data to train its machine learning system allows it to accurately estimate a wide range of sensitive information and, generate highly granular psychological insights into users without their knowledge.[15] This raises the following issues:

[8] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019) 272–78
[9] William D Wells, ' Psychographics: A Critical Review' (1975) *Journal of marketing research* (12), 196-213; Vian Bakir, 'Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting' (2020) 5(67) *Frontiers in Communication*
[10] Paul Maluga, 'Let Me and My Metadata Alone: Australia's Compliance with Article 17 of the International Covenant on Civil and Political Rights' (Thesis, Master of Research, Macquarie University) 24 April 2017, 15
[11] Michal Kosinski, David Stillwell, and Thore Graepel, 'Private traits and attributes are predictable from digital records of human behavior' (2013) *Proceedings of the National Academy of Sciences* vol 110(15) 5802
[12] Office of the Australian Information Commissioner, 'Chapter B: Key concepts' *Australian Privacy Principles guidelines* (Web Page, 22 July 2019) 27
[13] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019), 139
[14] Michal Kosinski, David Stillwell, and Thore Graepel, 'Private traits and attributes are predictable from digital records of human behavior' (2013) *Proceedings of the National Academy of Sciences* vol 110(15) 5802
[15] Michal Kosinski, David Stillwell, and Thore Graepel, 'Private traits and attributes are predictable from digital records of human behavior' (2013) *Proceedings of the National Academy of Sciences* vol 110(15) 5802

- Users tend not to conceive of the sheer quantity or accuracy with which their data is gathered and used, raising the question of whether consent can be considered free and informed.[16]
- The granularity with which psychological insights can be attained far exceeds the limits people expect on what is known about them and what others will find out.[17]
- Facebook's methodologies are opaque to end users and governments alike and, potentially undermine the individual's ability to ensure that personal information is used for the purposes they desire.[18]

3 Subversive Influence & Manipulation

Facebook exploit its vast stores of psychographic data to train its AI system not only to predict and influence consumer behaviour but modify it.[19] The methodologies Facebook employ to achieve this are potentially manipulative as they seek to pinpoint and exploit emotional vulnerabilities to ensure the maximum probability that users undertake a desired action. Its use of psychographic data to subversively influence choice in this way is analogous to *Cambridge Analytica's* psychographic 'micro-targeting'; which, Bakir (2020) concluded was a form of 'psy-ops' or 'information warfare'.[20]

A Cambridge-Analytica Micro-Targeting

During the 2016 United States presidential election, data analytics firm Cambridge Analytica harvested data from 87 million Facebook users.[21] In what was described as a mass-scale emotional manipulation experiment,[22] psychographic 'micro-targeting' was used to build psychological profiles of voters with the ultimate aim of influencing their behaviour.[23] Microtargeting is a form of targeted advertising that extracts users' digital footprints to identify the interests of a specific audience or individual in order to influence their actions.[24]

B Facebooks analogous practices

As stated by Chris Wylie, whistle-blower and data scientist involved in the founding of Cambridge Analytica, despite the dissolution of Cambridge Analytica, the psychographic targeting capabilities still exist.[25] Elsewhere, he warned that "we are placing blind trust in companies like Facebook to do the honourable and decent thing".[26] In many ways, Facebook's methodologies are analogous to those employed by Cambridge Analytica as the interventions are both designed to enhance certainty by manipulating behaviour in specific directions.[27]

---

[16] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Final Report, June 2014), 199
[17] Daniel Solove, 'A Taxonomy of Privacy' (2006) 154(3) University of Pennsylvania Law Review 477, 508; ALRC, *For Your Information* (Report 108, Vol 3, May 2008) 1710
[18] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Final Report, June 2014), 82; Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1108
[19] Joanna Kavenna, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy', *The Guardian* (Web Page, 4 October 2019) <Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy' | Society books | The Guardian>
[20] Vian Bakir, 'Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting' (2020) 5(67) *Frontiers in Communication* 1
[21] Australian Senate, *Select Committee on Foreign Interference through Social Media* (First Interim Report, December 2021) 26
[22] Office of the Australian Information Commissioner, *Privacy Act Review* (Issues Paper, 11 December 2020) 25
[23] Billy Perrigo, 'The Capabilities Are Still There ' Why Cambridge Analytica Whistleblower Christopher Wylie Is Still Worried', *Time* (Web Article, 8 October 2019) <https://time com/5695252/christopher-wylie-cambridge-analytica-book/>
[24] Sandra Matz, Ruth Appel, Michal Kosinski, 'Privacy in the age of psychological targeting' (2020) (31) *Current Opinion in Psychology* 116
[25] Billy Perrigo, 'The Capabilities Are Still There ' Why Cambridge Analytica Whistleblower Christopher Wylie Is Still Worried', *Time* (Web Article, 8 October 2019) <https://time com/5695252/christopher-wylie-cambridge-analytica-book/>
[26] Terry Gross, 'Whistleblower Explains How Cambridge Analytica Helped Fuel U S 'Insurgency', *NPR News* (Web Article, 8 October 2019) <https://www npr org/2019/10/08/768216311/whistleblower-explains-how-cambridge-analytica-helped-fuel-u-s-insurgency>
[27] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019), 213

In a 2017 leaked confidential document Australian Facebook executives boasted about the accuracy with which its AI system could attain psychological insights into young people.[28] The document stated that Facebook's AI system could discern when young people felt, 'anxious,' 'nervous,' 'stressed,' 'defeated,' and 'overwhelmed'. It further detailed how these psychographic insights could be employed to pinpoint when a young person was "…most vulnerable to a specific configuration of advertising cues and nudges".[29] Thus, it is clear that Facebook has attempted to modify user behaviour by exploiting its access to highly granular psychological data.

Facebook use psychographic data to pinpoint user emotions and vulnerabilities and direct or constrain information accordingly, to ensure a user takes a desired action. This can, at minimum, be understood as manipulative and potentially, constitutes a form of "information warfare". Per Bakir (2020) "if psychographic profiling and [micro]-targeting married with big data becomes coercive (for instance, by modulating people's exposure to information in ways that constrain their choices and behaviour), it would be accurate to describe it as psy-ops" a subset of information warfare.[30]

4 Privacy Principles

The primary issue is that Facebook is essentially shielded by the current privacy principles.

APP 3 stipulates entities must not collect personal information unless it is reasonably necessary for one or more of its functions or activities and must do so only by lawful and fair means.[31] Per APP 6, personal information must only be used or disclosed for the primary purpose for which it was collected.[32] Applicable to both APP 3 and 6 is that to collect sensitive information, an entity must obtain consent.[33]

Operatively, there are two fundamental flaws which render these principles ineffective for their purpose. First, the very function of Facebook is the collection and commodification of data. Further, by users providing access to personal data this business model allows Facebook to claim that it is not *selling* data; it merely asks businesses what audience segment they want to target.[34] Second, as a result of the deliberate concealment of the full range of data handling practices and techniques, the consent of users is trivially easy to gain.[35] In conjunction, these flaws have the effect of enabling Facebook to utilise the information for a broad range of primary purposes, without consent or within consumers' expectations.[36] The extent of Facebook's data handling practices is effectively hidden from users, this erodes their right to decide how and what their data will be used for, ultimately, diminishing consumer autonomy and privacy.

5 *Political Interference*

In growing numbers, Political parties seek to leverage the psychographic insights offered by Facebook to run political campaigns.[37] As shown in the U.S. 2016 election this has the potential to undermine open debate and transparency, constituting a serious threat to autonomy, privacy and the democratic electoral process.[38] Thus, in its current form, there is a risk that existing Privacy

---

[28] Shoshana Zuboff, *After the Digital Tornado: Networks, Algorithms, Humanity* (Cambridge University Press, 2020) 188
[29] Shoshana Zuboff, *After the Digital Tornado: Networks, Algorithms, Humanity* (Cambridge University Press, 2020) 189
[30] Vian Bakir, 'Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting' (2020) 5(67) *Frontiers in Communication* 1,2 Briant Emma, *Propaganda and Counter-Terrorism: Strategies for Global Change* (Manchester University Press, 2015) 23
[31] *Privacy Act 1988* (Cth) Schedule 1, APP 3
[32] *Privacy Act 1988* (Cth) Schedule 1, APP 6
[33] *Privacy Act 1988* (Cth) Schedule 1, APP 3, 6
[34] Dr Rita Matulionyte, 'Facebook is selling our data: are there laws to protect it?' *The Lighthouse* (Web Article, 16 November 2020) <https://lighthouse mq edu au/article/november-2020/facebook-is-selling-our-data-are-there-laws-to-protect-it>
[35] Attorney-General's Department, *Privacy Act Review* (Discussion Paper, October 2021) 77
[36] Attorney-General's Department, *Privacy Act Review* (Discussion Paper, October 2021) 81
[37] Tom Dobber, Ronan Ó Fathaigh, Frederik J Zuiderveen Borgesius, 'The regulation of online political micro-targeting in Europe' (2019) 8(4) *Internet Policy Review* 1,4
[38] The Guardian, 'Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles' (Youtube, 18 March 2018) [0 - 1 05min] <https://www youtube com/watch?v=FXdYSQ6nu-M> ; Office of the Australian Information Commissioner, *Privacy Act Review* (Issues Paper, 11 December 2020) 65

legislation fails to comply with Australia's international legal obligations. [39] Per article 17 of the *International Covenant on Civil and Political Rights* ('ICCPR') state parties are required to ensure the protection of individual privacy against unlawful or arbitrary interference.[40]

A The Political Exemption

The ability to freely elect leaders is a fundamental principle of democracy and finds expression in the doctrine of representative government. In upholding the doctrine, the High Court has consistently returned to the democracy and self-government rationale that the sovereign power of government, residing in the people, is exercised through representatives freely chosen.[41]

As exhibited by the 2016 Facebook-Cambridge Analytica matter, the use of psychographic targeting to influence user behaviour has permeated into the political sphere. It raises the concern that attempts by political parties to influence individual behaviour threatens to undermine the integrity of the electoral process by interfering in the political and civic communication that is essential to representative democracy.[42] This risk is exacerbated by the fact that the activities of Cambridge Analytica "…would be likely exempt if contracted to an Australian political party".[43] Currently exempt from the operation of the *Privacy Act 1988 (Cth)* are activities of registered political parties and certain activities of political representatives.[44]

6 *Recommendations*

1. Modify or remove the political exemption so that the use of psychographic targeting is explicitly prevented or, at minimum heavily restricted.
2. Regulate Facebook's aggregation of data, specifically with other products under parent company 'Meta'. Facebook's vast quantities of data should not be allowed to be collated with that of Instagram and WhatsApp which, respectively, have approximately 2bn monthly users.[45]
3. Require Facebook to provide greater transparency into what information its AI system is used to reveal and how it is employed and monetized.
4. Implement more stringent legislative protections for children who, by virtue of their developmental stage are more susceptible to providing consent without sufficient awareness and, are more vulnerable to subversive influence.

[39] Paul Maluga, 'Let Me and My Metadata Alone: Australia's Compliance with Article 17 of the International Covenant on Civil and Political Rights' (Thesis, Master of Research, Macquarie University, 24 April 2017) 6; International Covenant on Civil and Political Rights, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) ('ICCPR')
[40] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Final Report, June 2014) 23 <https://www alrc gov au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/>
[41] David Rolph, Matt Vitins, Judith Bannister, Daniel Joyce, *Media law: cases, materials and commentary* (Oxford University Press 2nd ed, 2015), 21; *Australian Capital Television Pty Ltd v Commonwealth (1992) 177 CLR 106.*
[42] Attorney-General's Department, *Privacy Act Review* (Discussion Paper, October 2021) 59; Miah Hammond-Errey, 'Big data and national security: a guide for Australian policymakers' (Lowy Institute Analysis, February 2022) 19
[43] Attorney-General's Department, *Privacy Act Review* (Discussion Paper, October 2021) 59
[44] Attorney-General's Department, *Privacy Act Review* (Issues Paper, October 2020) 33; *Privacy Act 1988* (Cth) ss 6C(1), 7C
[45] Yqub M, 'Instagram Daily Active Users 2022: How Many People use Instagram Daily' *BusinessDIT* (Web Article, 7 November 2022) <Instagram Daily Active Users 2022: The Latest Data Insight (businessdit com)>; Brian Dean, 'WhatsApp 2022 User Statistics: How Many People Use WhatsApp?' (Web Page, 5 January 2022) <https://backlinko com/whatsapp-users>