A TARGET ON YOUR BACK?

REGULATING TARGETED ADVERTISING ON FACEBOOK

PENNY O'BRIEN

A dissertation submitted in partial fulfilment of the degree of Bachelor of Laws (with Honours) at the University of Otago – Te Whare Wānanga o Otāgo

October 2020

ACKNOWLEDGEMENTS

To my supervisor, Professor Colin Gavaghan, for your guidance, enthusiasm, and encouragement throughout the year.

To my friends, for making my time at university so special.

To my sister, Victoria, for all the laughs and study break Facetime calls.

To my brother, Michael, for listening to my ideas and correcting my apostrophes – I could not have done this without you.

To my parents, Chris and Maria, for everything.

CONTENTS

Introduction

> *"Earlier this year, my friend Max gave me a knife from Japan as a gift. That evening, as I was lying in bed looking at [Facebook-owned] Instagram, I scrolled passed (sic) an ad of what looked like exactly the same knife. I did a double take, got out of bed, retrieved the knife from the kitchen and compared it to the one on my screen—it was a perfect match, a Masomoto KS. I hadn't Googled the knife, taken a picture of it, or even sent a text about it. The only interaction I had about the knife was face to face with Max when he gave it to me. This felt like more than a coincidence — it felt like I was being listened to."*[1]

In today's world of smart phones and social media, people are increasingly concerned by how online platforms collect, store, and use their personal information. These concerns often relate to social media platforms like Facebook because their eerily accurate targeted advertising mechanisms make users feel like they are being "spied on". Despite longstanding rumours that Facebook listens to users' conversations through their smart phones, there is little evidence to suggest that this is true.[2] To listen to users' conversations would require highly sophisticated software and consume such copious amounts of information that it would not go unnoticed by the average user. The jarring reality is that Facebook does not need hidden microphones to target its users – it has more effective ways to do so already.[3] Artist and engineer Tega Brain explained that "we are stuck in this 20th century idea of spying, of wiretapping and hidden microphones. But really there is this whole new sensory apparatus, a complicated entanglement of online trackers and algorithms that are watching over us."[4]

With 1.73 billion daily users,[5] Facebook can access unprecedented amounts of personal information. This gives the platform great power, including the ability to generate billions of dollars in yearly revenue through targeted advertising.[6] The 2018 Cambridge Analytica controversy demonstrated that inadequate regulation and monitoring of these processes can have catastrophic effects for online privacy.[7] Further, Facebook's 2019 housing discrimination charge demonstrated the way that Facebook's targeted advertising tools themselves can be used to target on objectionable grounds.[8] Thus, it is crucial that there are suitable controls on Facebook's information handling processes, and that these controls are complied with. It is also important to prevent misuse of this information within the targeted advertising process

---

[1] Oscar Schwartz "Digital ads are starting to feel psychic" (13 July 2018) The Outline <https://theoutline.com/post/5380/targeted-ad-creepy-surveillance-facebook-instagram-google-listening-not-alone?zd=1&zi=7awbjkxo>.
[2] Liarna La Porta "Is your phone always listening to you? (5 September 2019) Wandera <www.wandera.com/phone-listening/>.
[3] Antonio Garcia Martinez "Facebook's Not Listening Through Your Phone. It Doesn't Have To" (10 November 2017) Wired <www.wired.com/story/facebooks-listening-smartphone-microphone/>.
[4] Schwartz, above n 1.
[5] *Facebook Reports First Quarter 2020 Results* (29 April 2020) at 2.
[6] *Facebook Reports Fourth Quarter and Full Year 2019 Results* (29 January 2020) at 1.
[7] Alex Hern "Cambridge Analytica: how did it turn clicks into votes?" (6 May 2018) The Guardian <www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.
[8] *Department of Housing and Urban Development v Facebook* [2019] ALJ No. 01-18-0323-8 (Charge of Discrimination) at 1.

itself – namely to ensure there are adequate legal mechanisms in place to restrict advertisers' ability to target based on perceived vulnerabilities and discriminatory factors.

This dissertation will assess these key concerns about targeted advertising on Facebook, and evaluate whether New Zealand's law is fit for purpose in the current technological environment. Specifically, it will deal first with concerns about how Facebook collects and stores personal information for targeted advertising, and second with concerns about how advertisers disclose and use this information to target ads on Facebook.

Part I will introduce the topic by providing a background to targeted advertising, and explain how and why social media targeting has become the dominant form of advertising.

Part II will discuss the privacy concerns arising from Facebook's collection and storage of personal information for targeted advertising. First, it will explain how Facebook collects and stores personal information about its users. Second, it will outline the relevant law in New Zealand and certain overseas jurisdictions, assess how the law applies to Facebook, and consider the extent to which it adequately addresses these concerns. Finally, it will suggest how and why the law in New Zealand ought to be amended to better protect and enforce privacy rights.

Part III will discuss the concerns arising from how advertisers disclose and use personal information to target ads on Facebook. It will open by explaining the process of targeted advertising on Facebook and the contractual relationship between Facebook and advertisers. It will then explain the privacy concerns that arise from advertisers' disclosure of customer information when creating custom audiences on Facebook, and the concerns around wrongful targeting that arise from advertisers' use of audience selection tools when targeting ads on Facebook. In respect of these concerns, this Part will outline the relevant law in New Zealand, assess how it applies to targeted advertising on Facebook, and consider whether it is adequate. It will then discuss whether there is a need for change and what change might look like.

Finally, Part IV will discuss the implications of banning targeted advertising altogether. It will outline the potential benefits of such an approach in relation to issues of privacy and wrongful targeting, and ultimately explain why the most viable solution to these issues nonetheless remains regulating Facebook's processes rather than banning them.

Part I: Introduction to targeted advertising on Facebook

A Background to targeted advertising

The practice of advertising has existed as long as there have been products and services to sell, and messages to spread. Its early origins can be seen in etchings from ancient Egypt and Rome, and later in the 16th century print press.[9] Targeted advertising, on the other hand, is a much more recent development. Targeted advertising is a personalised method of advertising that is aimed at audiences with particular traits relevant to the product or service being advertised.[10] The aim of targeted advertising is to reduce inefficiency by ensuring that ads predominantly reach the consumers who are most likely to purchase the product or service in question – for example, targeting ads for pet food at pet-owners, targeting ads for kindergarten services at new parents, and targeting ads for a restaurant at people that live within a 5km radius. Advertisers select these audiences based on demographics like age, sex, and occupation; psychographics like lifestyle, values, and attitudes; past behaviour, and location.

The introduction of targeted advertising marked a shift from a product-centric model of advertising to a more consumer-centric model, whereby the needs of individual consumers became central to marketing strategy. Although hints of targeted advertising emerged in the mid 20th century; for example, targeting women with ads placed in fashion magazines or during soap opera commercials, it was not widely used until advertisers began to reach consumers online.[11] The internet played a key role in the emergence of targeted advertising because it provided advertisers with the ability to collect millions of data points on individual users, segment them into groups, and then reach specific groups with personalised ads. This made it easier to connect potential consumers with relevant products or services, build meaningful relationships, and generate more sales.

B Targeted advertising on social media

Effective targeting requires a great deal of information about the target audience. One of the best sources of this information is an individual's social media profile. This is because social media platforms are premised around users building an online profile and connecting with other users. Accordingly, users are encouraged to share information about themselves, their friends, and their interests, to create a bigger and more personalised network. These platforms use algorithms to tailor relevant content to each user based on the information they provide – the more information the platform has about a user, the "better" the users experience.[12] This

[9] Frank Presbrey "The history and development of advertising" (2000) 1(1) ASQ.
[10] Christian Schlee *Targeted Advertising Technologies in the ICT Space* (Springer Vieweg, Darmstadt, 2013) at 9.
[11] At 1.
[12] "Data Policy" Facebook (21 August 2020) <www.facebook.com/about/privacy/update>.

personalised content not only includes relevant posts by friends, liked pages, news articles, and suggested friends, but it also includes targeted ads.[13]

Social media targeting is a form of targeted advertising that uses social media platforms' comprehensive user information and in-built targeting mechanisms to place relevant ads in front of relevant audiences.[14] This is hugely beneficial to advertisers because it allows them to reach billions of potential consumers on one platform, more specifically micro-target at both a group and individual level, and gain valuable insights about the performance of their ads.[15] Accordingly, social media targeting is now at the forefront of many businesses' advertising strategy.[16]

C Targeted advertising on Facebook

Regarded as the "king of social media",[17] this dissertation will focus on targeted advertising on Facebook. Facebook is an American online social media platform launched and created in 2004 with the mission to "bring the world closer together".[18] Key features of the platform that work towards this objective are the Newsfeed, through which users are exposed to content; Messenger, through which users can directly message each other; and the Groups and Events tools, which facilitate connectivity and discussion. Despite this focus on connectivity, the social aspect of the platform has no direct bearing on its revenue. Instead, Facebook's business model relies on advertising. With 1.73 billion daily users and over seven million advertisers active across its platform,[19] Facebook generated approximately US$69.66 billion in advertising revenue in 2019, which accounted for 98.5 per cent of its global revenue.[20] Thus, given Facebook's market power and financial reliance on advertising, it is important to understand how these processes work, how they are regulated, and whether anything needs to change.

---

[13] "Terms of Service" Facebook (31 July 2019) <www.facebook.com/terms.php> at cl 1.
[14] "The essential guide to social media targeting" Digital Marketing Institute <https://digitalmarketinginstitute.com/blog/the-essential-guide-to-social-media-targeting>.
[15] Michael Stelzner *2020 Social Media Marketing Industry Report* (Social Media Examiner, May 2020) at 7.
[16] At 17.
[17] Ross Gerber "Snapchat Is Fun, But Facebook Is The King Of Social Media" (13 May 2017) Forbes <www.forbes.com/sites/greatspeculations/2017/03/13/snapchat-is-fun-but-facebook-is-the-king-of-social-media/#4338bad37ccd>.
[18] "Company Info" Facebook <https://about.fb.com/company-info/>.
[19] "Marketing" Facebook <www.facebook.com/business/marketing/facebook>.
[20] Facebook, above n 6, at 1.

Part II: Collection and storage of personal information by Facebook

A Introduction

The process of targeted advertising on Facebook can be examined in two stages – the collection and storage of personal information by Facebook, and the disclosure and use of that information by advertisers. This Part will address the first stage by evaluating the applicability and adequacy of New Zealand's privacy laws in relation to Facebook's collection and storage of user information for targeted advertising.

Section B will outline how Facebook collects and stores personal information for targeted advertising and then explain the privacy concerns raised by these processes. For the purposes of applying the relevant law, this Section will explain these processes as Facebook describes them, not as they are speculated to operate. This is because there is little evidence to support the rumours that Facebook is dishonest in its information collection methods.[21] However, the underlying concerns around Facebook's potential dishonesty will nonetheless be raised in Section D to support discussion about the need for stricter laws.

Section C will outline the relevant law in New Zealand and certain overseas jurisdictions, assess how the law applies to Facebook, and consider the extent to which it adequately addresses these concerns. The pertinent New Zealand law is found in the Privacy Act 1993 and the new amendments in the Privacy Bill 2020. The effectiveness of this law will be considered in comparison to the overseas positions taken in the Australian Privacy Act 1988, and the European Union (EU) Regulation 2016/679 on the General Data Protection Regulation (GDPR).

Finally, Section D will suggest why and how New Zealand's law ought to be amended to better protect and enforce privacy rights. I argue that the Privacy Bill is better equipped to protect personal information collected and stored for targeted advertising on Facebook than the current Act because it explicitly states the law's extraterritorial application and strengthens its enforcement mechanisms. That said, I argue that penalties and the enforcement powers afforded to the Privacy Commissioner must be increased, like in Australia and the EU, to deter large multi-national companies like Facebook from breaching the law.

B The collection and storage of personal information on Facebook

1 How Facebook collects personal information

Facebook cites four main types of information that it collects to support its advertising service,[22] and to which users consent through their use of the platform.[23] The first of these is

[21] La Porta, above n 2.
[22] "About Facebook Ads" Facebook <www.facebook.com/ads/about/?entry_product=ad_preferences>.
[23] Facebook, above n 13.

information users directly provide to Facebook. This includes all user activity across Facebook Products, such as profile information like age, gender, and occupation; usage information like features used and content interacted with; and network information like content uploaded by other users.[24] The second of these is information advertisers already have about users.[25] People share information like their name, email address, and phone number with businesses when they make purchases or sign up for newsletters and discounts. Businesses often upload this information to Facebook so that Facebook can match it to specific user profiles and show them ads accordingly. The third of these is information about user activity off Facebook.[26] This includes activity on other websites like visiting a website or adding a product to checkout. Businesses often share this information with Facebook using Facebook tools to enable users to be shown ads based on products they have previously looked at.[27] Finally, the fourth of these is information about users' location.[28] This includes information about where users connect to the internet, where they use their phone, and the location they share on their profiles. Facebook collects this information to show users ads from advertisers trying to reach people in or near a specific place.

2 How Facebook stores personal information

There are a number of provisions in Facebook's Data Policy and Terms of Service (Terms) that specify how Facebook stores this information. In its Data Policy, Facebook states that users can manage or delete information held about them at any time through Facebook settings. If users do not elect to do this, their information is stored on Facebook "until it is no longer necessary to provide [Facebook's] services or until [their] account is deleted – whichever comes first".[29]

Facebook's Terms states that "when [users] delete content, it's no longer visible to other users; however, it may continue to exist elsewhere on [Facebook's] systems" in a number of circumstances.[30] These circumstances include where immediate deletion is not possible due to a technical failure, where information has been used by another user who has not deleted it, and where information is required to be kept so Facebook can investigate a breach of Terms or comply with a legal obligation.[31] In the case of technical failures, Facebook guarantees that the information will be properly deleted within 90 days of the original request, and in respect of investigating a breach of Terms or complying with a legal obligation, Facebook states that the information will only be held for as long as is necessary for that purpose.[32]

---

[24] Facebook, above n 12.
[25] Facebook, above n 12.
[26] Facebook, above n 12.
[27] "The Facebook pixel" Facebook <www.facebook.com/business/learn/facebook-ads-pixel>.
[28] Facebook, above n 12.
[29] Facebook, above n 12.
[30] Facebook, above n 13, at cl 3.3.
[31] At cl 3.3.
[32] At cl 3.3.

3 The issue

The collection and storage of personal information for targeted advertising on Facebook raises privacy concerns relating to what information is collected, how it is collected, how it is stored, and the length of time it is held. These concerns are exacerbated by the sheer quantity of personal information Facebook processes every day,[33] and the frequency and significance of past privacy breaches that have resulted in the improper use of this information from millions of Facebook accounts.[34]

One of the most prominent and well-known privacy breaches is that involving Cambridge Analytica. Cambridge Analytica was a political consulting firm that used personal information about members of certain populations to inform political campaigns.[35] The controversy arose in 2018 when it was discovered that Cambridge Analytica had used personal information from 50 million unknowing Facebook users to target personalised ad campaigns aimed at influencing the 2016 United States Presidential Election.[36] The firm accessed this information via the "thisisyourdigitallife" app, a personality and political test taken by 32,000 American voters who were required to log in through Facebook to receive payment for their participation. Connecting to Facebook allowed the app to collect personal information from test-takers' Facebook accounts, as well as personal information from their Facebook "friends". Each participant's test results were then matched with their Facebook information and other sources to create a comprehensive set of records with hundreds of data points per person. This allowed Cambridge Analytica to target these individuals with highly personalised ads.

This controversy demonstrates the value and power of personal information and the privacy risks associated with its collection and storage on social media platforms generally. Although Cambridge Analytica was based in the United Kingdom and focused on American politics, this information grab included information about 64,000 New Zealanders.[37] This shows that New Zealanders are not exempt from these seemingly overseas privacy breaches and signals the need for New Zealand's laws to address these concerns. Accordingly, this Section will assess whether New Zealand's privacy laws adequately protect and enforce New Zealanders' privacy rights in respect of their personal information collected and stored for targeted advertising on Facebook.

C Privacy law

1 New Zealand

[33] Facebook, above n 5.
[34] Facebook "An Update on Our Plans to Restrict Data Access on Facebook" (press release, 4 April 2018).
[35] Hern, above n 7.
[36] Hern, above n 7.
[37] Madison Reidy "Cambridge Analytica 'misuse' may affect nearly 64,000 Kiwis, Facebook says" (9 April 2018) Stuff <www.stuff.co.nz/business/102928825/facebook-estimates-63724-kiwis-may-be-affected-by-cambridge-analytica-data-misuse->.

New Zealand's privacy law is governed by the Privacy Act 1993, but the new provisions outlined in the Privacy Bill 2020 were enacted on 30 June 2020 and will have effect from 1 December 2020.[38] This section will therefore outline the relevant provisions under the current Act alongside key amendments introduced by the Bill. It will then assess how this law applies to the collection and storage of personal information for targeted advertising on Facebook and consider how adequately it addresses the associated privacy issues.

Liability under the Act arises from an interference with an individual's privacy. This is established by a breach of one of the 12 Information Privacy Principles (IPPs) that causes loss, harm, or significant humiliation to an individual.[39] The provisions relating to the collection and storage of personal information are set out in IPPs 1 to 5 and 9. They require agencies to collect personal information in connection with a necessary lawful purpose, directly from the individual it relates to, in a way that is not unreasonably intrusive, and is compliant with transparency requirements. Further, these IPPs require agencies to reasonably protect personal information against loss, disclosure, and other misuse; and not to keep personal information for longer than is required for its necessary lawful purpose. "Personal information" is defined widely as "information about an identifiable individual".[40] This includes information "which informs, instructs, tells, or makes aware"[41] anything about a "natural living person"[42] that only needs to be identifiable to one person other than the data subject.[43] Further, "agency" is broadly defined as "any person or body of persons, whether incorporated or unincorporated, and whether in the public sector or the private sector".[44]

Individuals who believe their privacy rights have been infringed may raise complaints with the Privacy Commissioner,[45] who may decide to investigate the complaint and act as a conciliator.[46] The Commissioner does not have powers to enforce these laws and cannot make any rulings. Thus, if the parties are unable to settle, the Commissioner may refer the matter to the Director of Human Rights Proceedings, who can then undertake proceedings in the Human Rights Review Tribunal (HRRT) on the complainant's behalf.[47] If the HRRT is satisfied on the balance of probabilities that a defendant's action constitutes an interference with an individual's privacy, it may award remedies including declarations of breach, conduct restraint orders, remedial orders, and damages.[48]

Currently, any person or organisation who commits an offence under the Act is liable to pay a fine of up to NZ$2,000.[49] However, the Bill introduces increased fines for offences of up to

[38] Privacy Bill 2020 (34-3), cl 2.
[39] Privacy Act 1993, s 66.
[40] Section 2.
[41] *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385 at 402.
[42] Privacy Act 1993, s 2.
[43] *Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277 at 285.
[44] Privacy Act 1993, s 2.
[45] Section 67.
[46] Section 69.
[47] Section 77.
[48] Section 85.
[49] Section 127.

NZ$10,000.[50] These offences include obstructing the Commissioner in exercising his or her powers, non-compliance with lawful requirements made by the Commissioner, and the making of false or misleading statements.[51] The Bill also introduces stronger powers for the Commissioner, such as the ability to issue compliance notices which force agencies to comply with their obligations under the Act.[52] Such orders will be enforceable in the HRRT if not complied with.[53] In addition, the Bill introduces a new mandatory data breach notification provision that will require agencies to notify the Commissioner[54] and affected individuals[55] of privacy breaches as soon as practicable.

Although Facebook falls within the definition of an "agent" and much of the user information it collects and stores for targeted advertising is "personal information", the Act likely does not currently apply to Facebook.[56] This is because the Act does not expressly state that it has an extraterritorial effect. The Supreme Court in *Poynter v Commerce Commission* took the position that "where statutes are silent on the question of extraterritorial application, the content and purpose of the legislation may overcome the [common law] presumption" that statutes "are presumed not to have extraterritorial effect".[57] In that case, the Commerce Act 1986 did not displace this presumption because s 4 described the only circumstances in which the Act applied to conduct outside of New Zealand.[58] Similarly, s 10 of the Act currently outlines when information held by an agency includes information held outside New Zealand. Using this reasoning, social media platforms like Facebook are likely not required to comply with the Act and therefore cannot be found liable for interferences with New Zealanders' privacy.[59] This issue was on display in 2018 where Facebook refused a complainant access to personal information held on other users' accounts on the basis that it did not have to comply with the Commissioner's request to review the information.[60] Although the Commissioner was of the opinion that Facebook is subject to the Act because it provides services to New Zealand citizens and monetises their information,[61] this point has not been relied upon by a court and thus the Act likely does not currently apply to Facebook.

---

[50] Privacy Bill, cl 212.
[51] Privacy Act 1993, s 127.
[52] Privacy Bill, cl 124.
[53] Clause 130.
[54] Clause 118.
[55] Clause 119.
[56] Privacy Act 1993, s 2.
[57] *Poynter v Commerce Commission* [2010] NZSC 38 at [15].
[58] At [15].
[59] Although the High Court in *Chief Executive of the Department of Internal Affairs v Mansfield* [2013] NZHC 2064 held that "the sending of an unsolicited commercial electronic email into New Zealand [was] an act or conduct that occur[ed] in New Zealand" and that "the Court [therefore had] jurisdiction to deal with the matter" [at 35] this test is unlikely to be applied to Facebook's collection and storage of personal information for targeted advertising. This is because the case concerns the transmission of online materials into New Zealand by an overseas person, whereas the collection and storage of personal information by Facebook concerns the transmission of online materials outside of New Zealand.
[60] Office of the Privacy Commissioner "Privacy Commissioner: Facebook must comply with NZ Privacy Act" (media release, 28 March 2018).
[61] John Edwards, Privacy Commissioner "My Role, The Privacy Bill and Emerging Challenges" (guest lecture to LAWS423 class, Dunedin, 28 March 2019).

Jurisdiction in relation to internet-based companies is a hotly contested issue for which there is no straightforward solution.[62] However, the Bill attempts to resolve this issue by introducing a cross-border disclosure principle. Clause 3A clarifies the extraterritorial application of the law, stating that the Act will apply to overseas agencies doing business in New Zealand, regardless of whether they have a place of business in New Zealand or intend to profit from their business in New Zealand. This is intended to capture online companies like Facebook that conduct business in New Zealand but do not have a physical presence. This means that Facebook can be potentially liable for improper collection and storage of personal information about New Zealand users. The passing of the Bill will also require Facebook to comply with the Commissioner's requests and to notify the Commissioner and affected individuals of privacy breaches.

Overall, once the Act explicitly applies to Facebook, I believe it will likely impose adequate obligations on Facebook when collecting and storing information from New Zealand users for targeted advertising. This is because the IPPs apply to a broad range of circumstances, set reasonably high standards for compliance, and require clear actions to be taken to protect personal information. Accordingly, there is no need to hold agencies like Facebook to a different standard, notwithstanding the heightened privacy risks. The problem, however, is that the Act lacks the enforcement mechanisms necessary to ensure that Facebook will comply with its standards. Although the amendments introduced by the Bill will better equip the Act to protect personal information collected and stored for targeted advertising on Facebook, I do not believe these changes are enough. This is because the new penalty of NZ$10,000 remains low and will unlikely be sufficient to deter large multi-national companies like Facebook from engaging in misleading practices. Further, the new powers afforded to the Commissioner are unlikely adequate to enforce the application of its provisions.

2 Australia

To understand the effectiveness of New Zealand's law, and to make suggestions for its possible amendment, it is helpful to compare the New Zealand Privacy Act to the equivalent law in other jurisdictions. The Australian Privacy Act 1988 is relevant to New Zealand for two key reasons. First, because Australia and New Zealand share similar histories, cultures, and geographically isolated positions in the world. Second, because the Australian Act is currently being amended to strengthen its regulation of social media platforms.[63]

The Australian Act is similar to the New Zealand Act in that liability arises from interferences with privacy. This occurs where an APP entity (an agency or organisation)[64] breaches one of the Australian Privacy Principles (APPs) in relation to personal information.[65] The provisions

[62] Internet & Jurisdiction Policy Network "More coordination or a less cross-border internet, shows world's first Internet & Jurisdiction Global Status Report" (press release, 27 November 2019).
[63] Christian Porter and Mitch Fifield "Tougher penalties to keep Australians safe online" (media release, 24 March 2019).
[64] Privacy Act 1988 (Cth), s 6.
[65] Section 13.

relating to the collection and storage of personal information are set out in APPs 3 to 5 and 11. They require APP entities to collect personal information only if reasonably necessary for the entity's functions, by lawful and fair means, directly from the individual the information relates to, subject to notification requirements. Further, they require APP entities to reasonably protect personal information from misuse or loss and destroy or de-identify personal information where it is no longer required for its collected purpose. Like the New Zealand Act, "personal information" is widely defined as "any information about an identified or reasonably identifiable individual, whether or not it is true or recorded in a material form".[66]

Although these charging provisions are in substance the same as in the New Zealand Act, the two Acts differ in terms of their penalties and enforcement mechanisms. Under both Acts, individuals who believe they have suffered a privacy breach may lodge a complaint with their respective Privacy Commissioner,[67] who may decide to investigate it[68] and act as a conciliator.[69] However, the Australian Commissioner has greater powers, including the ability to apply to the Federal Court for a civil penalty[70] and the ability to issue formal and enforceable determinations that require APP entities to take certain actions to remedy breaches.[71] Further, the maximum civil penalty for serious or repeated interferences with privacy under the Australian Act is AU$2.1 million.[72] This is significantly higher than the current and proposed penalties in New Zealand but even it is not particularly high compared to Australian consumer law and standards across Europe.[73]

Like the New Zealand Privacy Bill, the Australian Act applies to information collected and stored for targeted advertising on Facebook. This is because Facebook, being an organisation that achieves an annual turnover of more than AU$3 million, falls within the definition of an "APP entity",[74] and much of the information it collects and stores about its users is "personal information".[75] Further, the Australian Act applies extraterritorially to acts done outside Australia by organisations like Facebook that do business in Australia.[76] This is reflected in the recent Federal Court action launched against Facebook in relation to the Cambridge Analytica controversy, which involved disclosure of personal information collected and stored about 311,127 Australian Facebook users.[77] Although this case will set an important jurisdictional precedent as to the scope of the law's extraterritorial application, the key aspect

[66] Privacy Act 1988, s 6.
[67] Section 36.
[68] Section 40.
[69] Section 40A.
[70] Section 80U(2).
[71] Section 52.
[72] Section 13G.
[73] Angela Flannery and Sarah Cass "Liability for breaches of Australia's Privacy Act to increase but class actions unlikely to be supported" (20 May 2020) Holding Redlich <www.holdingredlich.com/liability-for-breaches-of-australia-s-privacy-act-to-increase-but-class-actions-unlikely-to-be-supported>.
[74] Privacy Act 1988, s 6.
[75] Section 6.
[76] Section 5B.
[77] Office of the Australian Information Commissioner "Commissioner launches Federal Court action against Facebook" (media release, 9 March 2020).

of this decision will be the quantum of any penalty awarded.[78] This will require the Court to determine if the breaches alleged by the Commissioner constitute one collective breach or multiple breaches for each act of disclosure. Accordingly, the penalty awarded could range from AU$1.7 million (the maximum penalty available at the time of breach) to over AU$500 million.[79] The likeliest outcome is that the Court would not impose a penalty so highly in excess of the stated maximum penalty because it appears to go beyond the scope of its authority and Parliament's intentions. Nonetheless, legal commentators have remarked that this "proactive action taken by the Commissioner demonstrates a clear increase in the scrutiny and accountability expected of" social media platforms and "is an unprecedented step in enforcement of Australian privacy laws".[80]

Despite this, the existing protections and penalties under the Australian Act have been deemed insufficient to prevent misuse of personal information collected and stored by online social media platforms.[81] This is particularly in light of the 2019 Christchurch terror attack where footage of the massacre was livestreamed on Facebook for 17 minutes before it was taken down. These events drew attention to the law's regulation of social media, with Scott Morrison, Australian Prime Minister, saying it was "unacceptable to treat the internet as an ungoverned space."[82] Accordingly, in 2019 the Australian Government announced a number of amendments specifically designed to target platforms like Facebook.[83] This includes increasing the maximum penalty for serious or repeated interferences with privacy to the greater of "AU$10 million, three times the value of any benefit obtained through the misuse of information, or 10 per cent of a company's annual domestic turnover".[84] In addition, the Office of the Australian Information Commissioner (OAIC) will be granted greater powers, like the ability to "issue infringement notices and impose penalties for failure to cooperate with efforts to resolve minor breaches".[85] The 2019-20 Budget has also earmarked an additional AU$25.1 million for the OAIC to investigate and enforce privacy breaches by social media platforms.[86]

Taking into account the imminent amendments to the New Zealand Act and the Australian Act, it is clear that the Australian Act will be better equipped to protect and enforce privacy rights in relation to information collected and stored for targeted advertising on Facebook. This is primarily due to the greater enforcement powers granted to the OIAC and the significantly

---

[78] Gavin Smith, David Roundtree and Claudia Hall "OAIC's landmark case against Facebook to have major implications on Privacy Act" (12 May 2020) Allens <www.allens.com.au/insights-news/insights/2020/05/oaic-landmark-case-facebook/>.
[79] Smith, Roundtree and Hall, above n 78.
[80] Luke Dale, Daniel Kiley and Kelly Williamson "This is your private life: Facebook faces privacy law enforcement proceedings" (16 March 2020) HWL Ebsworth <https://hwlebsworth.com.au/this-is-your-private-life-facebook-faces-privacy-law-enforcement-proceedings/>.
[81] Porter and Fifield, above n 63.
[82] "Christchurch shootings prompt new laws for social media platforms in Australia" (26 March 2019) Radio New Zealand <www.radionz.co.nz/news/world/385639/christchurch-shootings-prompt-new-laws-for-social-media-platforms-in-australia>.
[83] Porter and Fifield, above n 63.
[84] Porter and Fifield, above n 63.
[85] Porter and Fifield, above n 63.
[86] Commonwealth of Australia *Budget 2019-20* (Budget Paper No. 2, 2 April 2019) at 53.

increased penalties that will force Facebook to take notice of the law and work harder to comply with it.

3 European Union

Widely regarded as the world's "strongest set of data protection rules",[87] the GDPR is another overseas framework worth comparing New Zealand's privacy laws against. The GDPR was enacted on 25 May 2018 to further regulate the processing of personal data within the EU and to protect privacy rights online.[88] Since its introduction, it has risen the standard of privacy across the EU and served as a catalyst for the strengthening of privacy laws across the world.[89]

The GDPR regulates the processing of personal data within the EU.[90] This means it imposes obligations onto controllers or processors anywhere in the world so long as they collect data from or about people within the EU. Liability under the Regulation arises from an infringement of its provisions.[91] Key provisions that regulate the collection and storage of personal data are set out in Art 5. These are similar to the IPPs, and require that personal data only be collected for a specific and legitimate purpose, to the extent necessary for that purpose, for no longer than is necessary for that purpose, in a manner that ensures appropriate security of the data.[92] The GDPR also outlines information disclosure requirements when collecting from or about individuals,[93] creates a right for erasure of personal data,[94] and requires controllers to ensure reasonable security of personal data[95] and to notify affected individuals of data breaches.[96] Although these provisions are slightly more comprehensive than in New Zealand, they impose similar standards on agencies that collect and store personal information. Like the privacy regimes in New Zealand and Australia, the GDPR defines "personal data" widely as "any information relating to an identified or identifiable natural person" and defines "processor" and "controller" as including individuals, agencies, and organisations.[97] Accordingly, the GDPR applies to Facebook.[98]

Like in New Zealand and Australia, the GDPR allows individuals who believe that their privacy rights have been infringed to lodge a complaint with the relevant supervisory

---

[87] Matt Burgess "What is GDPR? The summary guide to GDPR compliance in the UK (24 March 2020) Wired <www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018#:~:text=The%20EU's%20says%20GDPR%20was,those%20that%20interact%20with%20them.>.
[88] Ben Wolford "What is GDPR, the EU's new data protection law?" GDPR.EU <https://gdpr.eu/what-is-gdpr/>.
[89] Wolford, above n 88.
[90] Wolford, above n 88.
[91] Regulation 2016/679 on the General Data Protection Regulation [2018] OJ L 127, art 83.
[92] Article 5.
[93] Articles 13-14.
[94] Article 17.
[95] Article 32.
[96] Article 34.
[97] Article 2.
[98] "What is the General Data Protection Regulation (GDPR)?" Facebook <www.facebook.com/business/gdpr>.

authority.[99] The GDPR also empowers individuals to file actions directly in court.[100] The supervisory authority for each Member State is similar to the New Zealand and Australian Privacy Commissioners in that their role is to handle complaints and to supervise, educate, and advise on the application of the GDPR.[101] That said, supervisory authorities have a far wider range of corrective powers, including the ability to issue warnings and reprimands, to order compliance with requests, to impose bans on data processing, and to order the rectification, restriction, and erasure of personal data.[102] Supervisory authorities can also impose administrative fines for infringements of certain provisions and non-compliance with their orders.[103] The maximum penalties available under the GDPR range from the greater of €10 million or two per cent of global revenue for smaller offences, to the greater of €20 million or four per cent of global revenue for the most significant offences.[104] This amount is over double the new maximum penalty available in Australia and over 2,000 times that of New Zealand. If these penalties had been in operation during the Cambridge Analytica controversy, Facebook could have been fined a maximum of €1.32 billion for breaching user privacy.[105] This is significantly higher than the £500,000 penalty Facebook received pursuant to the Data Protection Act 1998,[106] and the €1 million penalty imposed by Italy's Privacy Guarantor.[107]

Although the GDPR unequivocally applies to Facebook, and Facebook has updated its Terms to comply with its provisions,[108] there have been a number of instances where Facebook has attempted to circumvent its intent. For example, in September 2018 Facebook notified the relevant supervisory authority of a data breach within the required 72-hour window,[109] but it omitted important details necessary for its investigation.[110] Later that year it was also discovered that Facebook waited three months before disclosing another data breach, claiming that "we let our regulator know within the 72-hour timeframe…as soon as we established it was considered a reportable breach under the GDPR".[111] Despite these acts of avoidance, the Irish Data Protection Commission (IDPC) has recently announced developments on a number

[99] Regulation 2016/679 on the General Data Protection Regulation, art 77.
[100] Article 79.
[101] Article 57.
[102] Article 58.
[103] Article 83.
[104] Article 83.
[105] Jim Waterson "UK fines Facebook £500,000 for failing to protect user data" (25 October 2018) The Guardian <www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica>.
[106] Letter from Elizabeth Denham (Information Commissioner of the Information Commissioner's Office) to Facebook Ireland Ltd and Facebook Inc regarding the issuing of a monetary penalty notice under the Data Protection Act 1998 (24 October 2018).
[107] Garante Per La Protezione Dei Dati Personali "Cambridge Analytica: the Privacy Guarantor fines Facebook for 1 million euros" (press release, 28 June 2019).
[108] Facebook "Facebook's commitment to data protection and privacy in compliance with the GDPR" (press release, 30 January 2018).
[109] Facebook "Security Update" (press release, 28 September 2018).
[110] Data Protection Commission Ireland (@DPCIreland) "@DPCIreland is awaiting from Facebook further urgent details of the security breach impacting some 50m users" <https://twitter.com/DPCIreland/status/1046417378236608512>.
[111] Kalev Leetaru "Facebook's Latest Breach Illustrates The Limits Of GDPR" (14 December 2018) Forbes <www.forbes.com/sites/kalevleetaru/2018/12/14/facebooks-latest-breach-illustrates-the-limits-of-gdpr/#26a2659974a5>.

of cross-border GDPR decisions relating to Facebook-owned platforms.[112] The furthest along is an inquiry into Facebook's transparency around the user information it receives from (Facebook-owned) WhatsApp.[113] The IDPC has also finished investigations into Facebook Ireland's obligations to establish a lawful basis for personal data processing and made inquiries into other cases concerning (Facebook-owned) Instagram and WhatsApp.[114] Another key milestone in the GDPR's application to Facebook is the *Schrems II* decision, in which the European Court of Justice recently ruled that companies moving European users' data to other jurisdictions must ensure an equivalent level of protection to the GDPR.[115] These decisions demonstrate the meaningful impact that the GDPR is beginning to have in empowering European regulators to deter and prevent privacy breaches on Facebook.

Accordingly, it is clear that the GDPR is far more effective than New Zealand's law in regulating, monitoring, and enforcing the protection of personal information collected and stored for targeted advertising on Facebook. This is largely due to its more extensive provisions, its larger penalties, and the greater enforceability powers possessed by its supervisory authorities. These provisions are much stricter than the law in New Zealand and Australia (including their respective amendments) and will allow people far more protection of their personal information.

D Suggested change

1 Why New Zealand needs change

Although the privacy laws in Australia and the EU are both better equipped to regulate online social media platforms like Facebook, that alone does not necessarily justify further amendments to the New Zealand Privacy Act. That said, I propose five additional reasons why New Zealand's privacy regime must change, and specifically, why this change should come from the Act.

First, the fact that Facebook has updated its Terms to comply with the GDPR[116] does not mean that it is bound to apply the same extensive privacy rules to New Zealand users. This is evident from Facebook's decision to move 1.5 billion users' contractual agreements from Facebook Ireland to Facebook Inc immediately before the GDPR came into effect.[117] This means that New Zealand users, as well as users in Africa, Asia, Australia, and Latin America are now

[112] Data Protection Commission "Irish DPC submits Article 60 draft decision on inquiry into Twitter International Company's compliance with Articles 33(1) and 33(5) of the GDPR" (press release, 22 May 2020).
[113] Data Protection Commission, above n 112.
[114] Data Protection Commission, above n 112.
[115] Court of Justice of the European Union "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield" (press release No 91/20, 16 July 2020).
[116] Facebook, above n 108.
[117] David Ingram "Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law" (19 April 2018) Thompson Reuters <www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P>.

technically governed by less strict US privacy laws,[118] thereby limiting Facebook's liability under the GDPR. Facebook justified this action by saying that the GDPR requires more specific language than US law, and downplayed the effect of this change by saying it would still apply the Regulation globally "in spirit".[119] Despite these assurances, this action demonstrates that New Zealand cannot rely on Facebook's compliance with the GDPR to protect New Zealand users – we must instead ensure that the Act does it for us.

Second, even though users technically consent to Facebook's Terms, Data Policy, and Cookie Policy when signing up to the platform, this operates more as a fallacy of consent than as meaningful understanding and acceptance of how their information will be handled. As with many online platforms, users who sign up to Facebook must agree to the relevant terms prior to use. There are two problems with this process. The first is that users are not required to read or click on any of this information. The second is that users who elect to do so are required to read over 10,000 words – an amount that goes far beyond what any reasonable user should be expected to read and understand. This means that Facebook users are generally unaware of their rights and that their acceptance cannot be relied upon as proof that they are actually happy with Facebook's information handling processes. Even if Facebook were to improve this process, it remains inevitable that ordinary users will be unable to appreciate the full extent of what they "consent" to, thus demonstrating the need for stricter laws to protect them.

Third, although anxieties that Facebook records conversations appear misplaced,[120] the fact that speculation around its information collection methods remains prevalent reflects ongoing and legitimate concerns around its honesty and transparency. These concerns persist because of recent studies showing apps sending screenshots of page activity to third parties,[121] and because of the inadequacy of Facebook's user controls, described as a "performative transparency"[122] that "downplays the information it collects about you"[123] and "conceals the scope of their surveillance".[124] For example, the "ad preference menu" (Facebook's primary user control) is difficult to find, contains vague justifications for the categories assigned to users, and is unclear about how the information was collected in the first place.[125] Further, Facebook's "download your data" tool, which in theory allows users to download all their account information,[126] is similarly difficult to find and navigate. This report contains raw information but does not show how individual data points are combined and analysed –

[118] Facebook, above n 13, at cl 4.4.
[119] Ingram, above n 117.
[120] La Porta, above n 2.
[121] Elleen Pan, Jingjing Ren, Martina Lindorfer, Christo Wilson and David Choffnes "Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications" (2018) 18(4) PoPETs 1 at 1.
[122] Schwartz, above n 1.
[123] Louise Matsakis "Facebook's Targeted Ads Are More Complex Than It Lets On" (25 April 2018) Wired <www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/>.
[124] Schwartz, above n 1.
[125] "Your ad preferences" Facebook <www.facebook.com/ads/preferences/edit/>.
[126] "Accessing & Downloading Your Information" Facebook <www.facebook.com/help/1701730696756992?helpref=hc_global_nav>.

particularly in an advertising context.[127] Nitasha Tiku wrote that the "the difference between what Facebook knows about you and what it includes in Download Your Data underscores mounting consumer privacy concerns and the limits of self-regulation. Zuckerberg presented the tool as a check on its power, but Facebook controls what it reveals."[128] This shows that Facebook cannot be trusted to self-regulate transparently, and signals the need for stricter mechanisms to monitor and enforce Facebook's compliance with the law. Moreover, this lack of transparency further reinforces the dubiousness of users' purported consent to Facebook's information handling processes, and the associated need for regulatory reform.

Fourth, despite the moderate fines and reputational damage Facebook incurred as a result of the Cambridge Analytica controversy, Facebook has since continued to breach privacy rights. For example, in 2018 Facebook announced that some applications had continued to retain access to users' profile pictures and identities, despite changing its settings seven months earlier to prevent this.[129] Further, in 2019 cybersecurity researchers found that 145 gigabytes of information from over 540 million Facebook accounts had been made publicly available on the internet.[130] These incidents demonstrate a continued lack of security around Facebook users' information and reinforce the need for stricter laws that will sufficiently deter future breaches.

Finally, the fact that people are still using Facebook despite these scandals signals the need for a stronger regulatory response. A 2019 InternetNZ survey showed that 89 per cent of people surveyed were concerned about the security of their personal information on the internet but 90 per cent of people surveyed said that the positives of the internet outweighed the negatives.[131] This is evident in the fact that the number of daily Facebook users actually rose following the Cambridge Analytica controversy,[132] and has steadily continued to increase since.[133] The dichotomy between users' attitudes towards privacy and their behaviour on Facebook is described as the "privacy paradox".[134] This likely arises because many users lack the knowledge or experience to fully appreciate the extent of risks online – or simply do not care, and because Facebook's market dominance allows it to position itself as a necessity for staying connected online. Further, in many instances, the harm caused by Facebook's practices may manifest more clearly at a social level than at an individual level, and so individual user behaviour may not be a reliable gauge of the problem's scale. Whatever the reason, the fact that people continue to use Facebook does not mean that Facebook's information handling processes do not pose a real and legitimate threat to privacy, and that Facebook users should not be better protected by law. Thomas J in *R v Brooker* said that "privacy is imperative if our

---

[127] Nitasha Tiku "What's *Not* Included in Facebook's 'Download Your Data' (23 April 2018) Wired <www.wired.com/story/whats-not-included-in-facebooks-download-your-data/>.
[128] Tiku, above n 127.
[129] Facebook "Changes to Groups API Access" (press release, 6 November 2019).
[130] "Losing Face: Two More Cases of Third-Party Facebook App Data Exposure" (3 April 2019) UpGuard <www.upguard.com/breaches/facebook-user-data-leak>.
[131] Colmar Brunton "*New Zealand's Internet Insights 2019*" (InternetNZ, December 2019) at 18.
[132] *Facebook Reports Second Quarter 2018 Results* (Facebook, 25 July 2018) at 1.
[133] Facebook, above n 5, at 2.
[134] Nina Gerber, Paul Gerber and Melanie Volkamer "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behaviour" (2018) 77 COSE 226 at 27.

personal identity and integrity is to remain intact" and that "recognising and asserting this personal and private domain is essential to sustain a civil and civilised society".[135] These recent privacy breaches, and the law's current failure to protect the personal information of New Zealanders affected, signal the need for change. The continued use of Facebook demonstrates that the market cannot be relied upon to address these issues. Legal reform is required.

2 Amending the Privacy Act 1993

The Privacy Act was introduced in a time without social media. Thus, although it will likely substantively address many of the privacy issues around Facebook's collection and storage of personal information for targeted advertising once it applies to Facebook, it is hardly surprising that it lacks the enforcement mechanisms necessary to ensure that Facebook will comply with these obligations. The Privacy Bill is better equipped to regulate these processes because it explicitly states the law's extraterritorial application and strengthens its enforcement mechanisms. That said, the developments made in Australia and the EU show that more can be done to address these issues, namely increased penalties and greater enforceability powers for the Privacy Commissioner.

Increasing penalties for privacy breaches is necessary to ensure that Facebook complies with the Act. Measured against Facebook's US$70 billion profit in 2019[136] and the multi-million-dollar penalties available in Australia and the EU, the new maximum penalty of NZ$10,000 is clearly incapable of deterring Facebook's breaches. That is not to say that New Zealand's penalties should match those of Australia and the EU. Although Facebook users can be affected by privacy breaches regardless of their physical location, it is important to remember that New Zealand does not have the same market leverage as other larger, wealthier, and more populated jurisdictions. This means that imposing penalties on the same scale as in Australia or the EU may unduly threaten Facebook's willingness to operate in New Zealand. Nonetheless, I argue that our penalties must at least hit the million-dollar mark – a sum that may not even be enough to deter Facebook from mishandling user information but that would at least give the Act more teeth without being so high so as to unfairly burden smaller agencies. This is the position taken by the Commissioner, who previously lobbied for civil penalties of up to NZ$1 million for private and public sector organisations, and up to NZ$100,000 for individuals.[137] This would better align New Zealand's penalties, relative to its market power, with those of other jurisdictions, and finally begin to recognise the risk Facebook poses to New Zealanders' privacy.

Another way to ensure that Facebook complies with the Act is to give the Commissioner greater powers to enforce it. Although the Commissioner will soon be able to issue agencies with compliance orders,[138] this is inadequate compared to the corrective and administrative powers

[135] *R v Brooker* [2007] NZSC 30 at [252].
[136] Facebook, above n 6, at 1.
[137] Office of the Privacy Commissioner "Privacy Commissioner recommends data portability, brakes on data re-identification and fines up to $1 million" (press release, 3 February 2017).
[138] Privacy Bill, cl 124.

afforded to EU supervisory authorities and squanders the Commissioner's expertise on a relatively powerless role. On this basis I argue that two additional powers are necessary to better enforce privacy rights on Facebook. The first of these is to empower the Commissioner with sole discretion to decide which complaints may proceed to the HRRT, thereby removing the intermediate role of the Director of Human Rights Proceedings. This would reduce unnecessary compliance costs, promote more efficient resolution of complaints, and ensure that complaints are handled by someone with a dedicated privacy function and expertise.[139] This view is shared by both the Commissioner and the Law Commission,[140] who described the current model as "duplicative and inefficient".[141]

The second of these is to empower the Commissioner to apply to the High Court for a civil penalty in cases where there is a serious or repeated interference with privacy. This accords with recommendations made by the Commissioner in 2018.[142] He explained that civil penalties would operate as an "an enforcement mechanism…alongside the current complaints resolution system" to "appropriately and meaningfully" hold non-complaint agencies to account and incentivise compliance with the Act.[143] This would also bring New Zealand's privacy law in line with New Zealand consumer protection law and the administrative powers held by the Australian Commissioner and EU supervisory authorities.[144] I believe these powers are necessary to give the Commissioner a "real and effective ability to enforce"[145] New Zealand's privacy laws and adequately hold Facebook to account.

It is impossible to point to any one regulatory strategy and deem it "enough", and it is unrealistic to imagine that legislation can keep up with Facebook's information handling processes absent consistent revision and revisitation. Nevertheless, the above suggestions would go a long way towards addressing the key privacy issues New Zealanders are facing today, and even going forward into the near future. As John Edwards, New Zealand's Commissioner, remarked – "no, legislation can't keep up, but that doesn't mean it shouldn't try".[146]

---

[139] Privacy Commissioner "Submission on the Privacy Bill to the Justice and Electoral Select Committee" at [4.3].
[140] At [4.3].
[141] Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011) at [6.33].
[142] Privacy Commissioner, above n 139, at [1.7].
[143] Privacy Commissioner "Background paper: Including provision for the Commissioner to seek imposition of a civil penalty for serious privacy breaches" at [3].
[144] Privacy Commissioner, above n 139, at [2.5].
[145] Kensington Swan "Submissions on the Privacy Bill" at [2.4].
[146] Katie Kenny "All you need to know about the proposed privacy laws" (23 May 2018) Stuff <www.stuff.co.nz/national/104126249/all-you-need-to-know-about-the-proposed-privacy-laws>.

Part III: Disclosure and use of personal information by advertisers

A Introduction

The second stage of targeted advertising on Facebook relates to the disclosure and use of personal information by advertisers. This Part will address this stage by evaluating the applicability and adequacy of New Zealand's laws in regulating these processes.

Section B will outline how advertisers disclose and use personal information to target ads on Facebook, explain the contractual relationship between Facebook and advertisers, and then identify two key concerns raised by these processes.

Section C will discuss the privacy concerns raised by advertisers' disclosure of customer information to Facebook when creating custom audiences for targeted advertising. In doing so, it will consider how adequately the Privacy Act 1993 and the Advertising Standards Code regulate this process. As with Part II, I argue that the standard imposed by the Act is likely adequate, but that the maximum penalty ought to be increased to appropriately recognise the risks posed by disclosing information to Facebook and to incentivise large-scale advertisers to comply with its provisions. I also argue that the self-regulatory nature of New Zealand's advertising industry,[147] and the Code's operation alongside the Act,[148] makes the Code an adequate framework for advertisers to adhere to.

Section D will discuss the concerns around wrongful targeting that arise from advertisers' use of audience selection tools when targeting ads on Facebook. In doing so, it will consider how adequately the Advertising Standards Authority (ASA) advertising codes and the Human Rights Act 1993 regulate advertisers' ability to target groups based on perceived vulnerabilities and discriminatory factors. In respect of targeting vulnerable groups, I argue that the Children and Young People's Advertising Code adequately regulates advertisers' ability to target food and drink ads at children and young people on Facebook, but that a new rule should be added to the Advertising Standards Code to protect other vulnerable groups. In respect of discriminatory targeting, I argue that both s 67 of the Human Rights Act and rule 1(c) of the Advertising Standards Code ought to be amended to explicitly apply to targeting ads.

B The disclosure and use of personal information by advertisers on Facebook

1 The targeted advertising process

[147] "Self-regulation and the Industry Levy" Advertising Standards Authority <www.asa.co.nz/industry/self-regulation-industry-levy/>.
[148] "Codes" Advertising Standards Authority <www.asa.co.nz/codes/>.

Facebook describes its advertising function as "how we provide our services for free",[149] and therefore works with advertisers by selling them a space to advertise on its platform.[150] The relevant aspect of this process for the purposes of this Part is how advertisers select their target audience on Facebook. There are three audience selection tools available to advertisers on Facebook.[151] The first of these is the "core audiences" tool. This allows advertisers to define their target audience based on factors like location, demographics, interests, behaviour, and connections. For example, if a violin shop comes to Facebook wanting to reach female violinists in Wellington, the core audiences tool allows it to reach profiles of women who live in Wellington and have an interest in violin or classical music. The second audience selection tool is the "custom audiences" tool. This allows advertisers to reach people who have already engaged with their business. For example, an advertiser can retarget its customers by creating a custom audience using information from its CRM system and email lists. Further, an advertiser can set up a Facebook pixel to automatically create a custom audience of people who have visited its website or social media profile and show them targeted ads for previously viewed items. Finally, the "lookalike audiences" tool allows advertisers to reach new people who have similar interests to those of their current customers.

Once an advertiser has identified its desired audience, it creates its ad and uploads it to Facebook. However, an ad must pass Facebook's review process before it is displayed on the platform.[152] This involves Facebook checking an ad's text, images, targeting, positioning, and context on the desired landing page for compliance with its Advertising Policies and Community Guidelines.[153] Facebook retains sole discretion to accept, reject, or remove any ad from the platform.[154] Once the ad has been accepted, Facebook takes the advertiser's goal, desired audience, and ad, and matches it to users who might be interested in it.

2 The relevant contractual terms

This process is governed by a number of contractual terms. When selecting audiences using the core or lookalike audience tools, Facebook's Advertising Policies state that advertisers "must not discriminate against, harass, provoke or disparage users, or to engage in predatory advertising practices"[155] and must "comply with applicable laws that prohibit discrimination".[156] When creating custom audiences using the custom audiences tool, the Policies also require that advertisers comply with the Customer List Custom Audiences Terms.[157] Accordingly, advertisers agree that they have all "necessary rights and permissions and a lawful basis to disclose and use the [information] in compliance with all applicable laws,

[149] Facebook "Our Advertising Principles" (press release, 27 November 2017).
[150] Facebook "Hard Questions: What Information Do Facebook Advertisers Know About Me?" (press release, 23 April 2018).
[151] "Ad targeting" Facebook <www.facebook.com/business/ads/ad-targeting>.
[152] "Advertising Policies" Facebook <www.facebook.com/policies/ads/> at cl 2.
[153] At cl 2.
[154] At cl 13.6.
[155] At cl 7.1.
[156] At cl 4.3.
[157] At cl 7.2.

regulations and industry guidelines",[158] and that they "instruct Facebook to use the [information] for the matching process".[159] Advertisers that fail to comply with these provisions, laws, and regulations risk their ads being removed or their accounts being terminated.[160]

The contractual relationship between Facebook and advertisers is governed by Facebook's Commercial Terms and Terms of Service.[161] These contracts impose strict obligations on advertisers to comply with "all applicable laws, rules, and regulations" when using Facebook,[162] and limit Facebook's liability to advertisers to the "fullest extent permitted by applicable law".[163] They also allow Facebook to "disclaim all warranties", to "make no guarantees that [its Products] will always be safe, secure or error-free" and to contract out of liability for any businesses' "lost profits, revenues, information or damages" relating to Facebook's advertising service.[164] Facebook also retains a great deal of protection during disputes by requiring an indemnity from the relevant advertiser against all damages, losses, and expenses related to any claim brought against it that relates to an advertiser's actions.[165]

These provisions effectively operate to offload potential liability from Facebook to its advertisers. This means it is an advertiser's responsibility to ensure that its use of Facebook for targeted advertising complies with Facebook's terms and all applicable laws, rules, regulations, and industry guidelines. Accordingly, this Part will assess the applicability and adequacy of New Zealand's laws in regulating advertisers' conduct when targeting ads on Facebook.

3 The issues

There are two key issues raised by this process. The first of these is the privacy concerns that arise from advertisers' disclosure of customer information to Facebook when creating custom audiences. As discussed in Part II, people are becoming increasingly concerned by the amount of information Facebook collects and stores about them. The information Facebook receives from advertisers raises additional privacy concerns around what information is disclosed, where it is disclosed, how it is used and protected, and whether the disclosure was authorised in the first place. These concerns are heightened by past privacy breaches, like the Cambridge Analytica controversy, which demonstrate Facebook's lack of security around its users' information and how this information can be used beyond its intended purpose. Addressing these concerns is important because people have a right to exercise control over who has access to their information and how their information is used. Thus, it is important that New Zealand's

[158] "Customer List Custom Audiences Terms" (31 August 2020) Facebook <www.facebook.com/legal/terms/customaudience/update> at cl 1.
[159] At cl 3.
[160] Facebook, above n 152, at cl 13.2.
[161] "Commercial Terms" (31 August) Facebook <www.facebook.com/legal/commercial_terms/update>.
[162] At cl 2.
[163] Facebook, above n 13, at cl 3.
[164] At cl 3.
[165] At cl 5.

laws adequately protect and control the information that advertisers disclose to Facebook for targeted advertising.

The second of these is the concerns around wrongful targeting that arise from advertisers' use of other audience selection tools when targeting ads on Facebook. As discussed in Part I, targeted advertising on Facebook is undoubtedly beneficial to advertisers because it allows them to home in on consumers that are likely to be interested in any given product or service – both increasing sales and reducing inefficiency. That said, targeted advertising on Facebook also offers a number of benefits for the ordinary consumer. Not only does it "enhance the consumer experience"[166] by presenting consumers with ads that are more relevant, useful, and engaging than non-targeted ads, but it also helps time-conscious consumers shop more efficiently in the crowded marketplace by bringing their shopping to them.[167] Showing users "relevant" ads was cited by Rob Goldman, Facebook's former Vice President for Advertising, as one of the driving goals for Facebook's advertising service.[168] However, the issue with this, as identified by Louise Matsakis, is that "nowhere does he define what "relevant" means in this context".[169] She explained that "beyond simple demographics, a "relevant" ad to a marketer might target a specific personality type, or a perceived emotional state. It might also be designed to take advantage of an already vulnerable population".[170] Thus, although targeted advertising on Facebook has a number of benefits – it also has the potential to be used wrongfully by advertisers.

In this dissertation, I define "wrongful targeting" on Facebook as comprising two parts; targeting based on perceived vulnerabilities and targeting based on discriminatory factors. Each of these has the potential to harm different groups of consumers in different ways. For example, targeting vulnerable groups is harmful because it allows advertisers to manipulate consumers' spending patterns (often to their detriment), encourage negative behaviours, and cause emotional distress. This is true of alcohol ads targeted at alcoholics (particularly late at night), fast food ads targeted at children, or weight loss ads targeted at people with disordered eating. Likewise, discriminatory targeting is harmful because it perpetuates inequalities by disproportionately exposing privileged groups to opportunities. This is particularly true of ads for housing, jobs, and credit, which advertisers have previously been able to target on Facebook based on sex, race, colour, income, and familial status.[171] These examples show how easily the mutual benefit of targeted advertising can become skewed towards advertisers and demonstrates the need for adequate regulation of Facebook's targeting processes to prevent this.

---

[166] Gilad Edelman "Why Don't We Just Ban Targeted Advertising?" (22 March 2020) Wired <www.wired.com/story/why-dont-we-just-ban-targeted-advertising/>.
[167] Naomi Campbell "I'm a big fan of targeted marketing because I am tres lazy and prefer my shopping to come to me, than for me to have to search for it" <www.facebook.com/groups/227268451176371/permalink/640067259896486>.
[168] Facebook, above n 149.
[169] Matsakis, above n 123.
[170] Matsakis, above n 123.
[171] Julia Angwin and Terry Parris Jr. "Facebook Lets Advertisers Exclude Users by Race" (28 October 2016) ProPublica <www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>.

Despite recent amendments to Facebook's advertising system and Policies to prevent wrongful targeting,[172] there are a number of reasons why this remains a legitimate issue. First, because Facebook cannot be relied on to prevent all wrongful targeting. This is because Facebook's ad review process depends on the subjective judgement of Facebook's ad moderators,[173] many of whom might not understand the effect a targeted ad will have on particular audiences,[174] and because Facebook's advertising system also depends on targeting algorithms which have been proven to show discriminatory biases.[175] Further, the fact that Facebook retains discretion to change its policies at any time[176] means it cannot necessarily be relied on to protect users into the future. Second, because it remains possible, given the amount of personal information available on Facebook, that advertisers can still target vulnerable groups, or distinguish based on discriminatory factors, by targeting proxy variables. This will become increasingly relevant the more advanced Facebook's audience selection tools become. Accordingly, it is important that New Zealand's laws adequately restrict advertisers' ability to wrongfully target groups on Facebook.

C The privacy issue

New Zealand currently has two legal mechanisms that regulate advertisers' disclosure of customer information to Facebook when creating custom audiences for targeted advertising. These are the Privacy Act 1993 and the Advertising Standards Code. This Section will consider how adequately each of these frameworks restrict advertisers' conduct and protect New Zealanders' personal information. In doing so, it will discuss the need for change and make recommendations about what any such change should look like.

1 The Privacy Act 1993

As discussed in Part II, the Privacy Act is New Zealand's primary statute dealing with privacy rights. The Act regulates advertisers' disclosure of customer information to Facebook for targeted advertising because advertisers fall within the definition of an "agency"[177] and much of the information they disclose to Facebook is "personal information".[178] Although the Act does not explicitly state that it has an extraterritorial effect, it is possible that it applies to overseas advertisers as well as New Zealand advertisers. Unlike Facebook's collection and storage of personal information for targeted advertising, advertisers' targeting of ads at New

[172] Facebook "Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising" (press release, 19 March 2019).
[173] Facebook, above n 152, at cl 2.
[174] Casey Newton "The Trauma Floor: The secret lives of Facebook moderators in America" (25 February 2019) The Verge <www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona>.
[175] Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove and Aaron Rieke "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes" (2019) 3 PACM HCI 2 at 2.
[176] Facebook, above n 152, at cl 13.8.
[177] Privacy Act 1993, s 2.
[178] Section 2.

Zealand audiences is likely captured by the jurisdiction test in *Chief Executive of the Department of Internal Affairs v Mansfield*.[179] This is because it similarly relates directly to the targeted transmission of online materials into New Zealand. However, this application of the test has never been tested by a court. Regardless, the new extraterritoriality provision introduced by the Privacy Bill will soon extend the application of the Act to overseas advertisers that target ads at New Zealand Facebook users.[180]

The key disclosure principle, Information Privacy Principle (IPP) 11, prohibits advertisers from disclosing personal information about their customers to Facebook unless they reasonably believe either that the information is publicly available, that the disclosure was one of the purposes in connection with which the information was obtained, or that the disclosure was authorised by the individual concerned. Although "authorised" is not defined, it has generally been interpreted as requiring a "positive and conscious act by the individual"[181] rather than a "failure to object".[182] This is a higher standard than consent,[183] and means that advertisers seeking to rely on the authorisation exception must obtain active and express permission from customers prior to disclosure. I believe this standard appropriately protects the privacy rights of consumers without unreasonably infringing on advertisers' ability to target their customers. However, an issue with this principle is that it does not distinguish between disclosure to agencies within and outside of New Zealand. This means it does not adequately recognise the greater privacy risks associated with disclosure to overseas companies like Facebook, and the issues which may arise from such companies being subject to different privacy laws and standards of protection.

The Bill attempts to resolve this issue by introducing a new IPP 12 that specifically regulates the disclosure of personal information outside New Zealand. This operates alongside the disclosure requirements in IPP 11, and provides that advertisers may only disclose personal information to foreign receiving agencies like Facebook if they reasonably believe that the receiving agency is subject to privacy laws with comparable protections. If a jurisdiction does not offer such protections, IPP 12 requires that advertisers fully inform the relevant individuals that their information may not be adequately protected, and obtain express authorisation prior to disclosure.[184] This is similar to the cross-border disclosure principle in the Australian Act[185] and Chapter 5 of the GDPR, which demonstrates that New Zealand's disclosure principles are meeting the high standards imposed by other privacy-focused jurisdictions.

I believe this new provision will mitigate many of the privacy concerns associated with advertisers' disclosure of customer information to Facebook for targeted advertising. This is because it further limits the circumstances in which advertisers can disclose customer information to Facebook, imposes additional obligations on advertisers to guarantee reasonable

[179] *Chief Executive of the Department of Internal Affairs v Mansfield*, above n 59, at [35].
[180] Privacy Bill, cl 3A.
[181] Paul Roth *Privacy Law and Practice* (online looseleaf ed, LexisNexis) at PVA6.13(g).
[182] *Case Note 2976* [1996] NZPrivCmr 1 (1 November 1996).
[183] Paul Roth, above n 181, at PVA6.13(g).
[184] Privacy Bill, cl 19.
[185] Privacy Act 1988, sch 1 Australian Privacy Principle 8.

equivalent protection of customer information overseas, and ensures that New Zealand consumers are given further control over whether their personal information will be disclosed to Facebook in circumstances where it might not be adequately protected. This will give consumers confidence that their information will be protected even when disclosed overseas, without imposing such onerous compliance costs on advertisers that they cannot reasonably access Facebook's highly valuable targeting tools. Accordingly, I believe it successfully balances the rights of advertisers to utilise these tools using fairly obtained customer information against the rights of customers to be informed, consulted, and protected during this process.

Thus, I believe these provisions likely adequately regulate advertisers' ability to disclose information to Facebook, and therefore do not need to change. That said, I believe the new NZ$10,000 penalty introduced by the Bill remains insufficient to deter many advertisers from breaching these provisions. I argue, like in Part II, that the maximum penalty ought to be increased to NZ$1 million. This is far more severe than would be warranted in most cases, especially considering the range of small businesses which rely on Facebook's advertising and can likely be deterred by reputational damage alone. However, it is nonetheless important that the maximum penalty available be steep enough to deter egregious breaches committed by powerful advertisers. This is especially true in light of the Act's upcoming extraterritorial effect,[186] which will render large-scale, wealthy businesses subject to its provisions, many of which can afford to incur a NZ$10,000 penalty to obtain the full benefit of Facebook's targeting tools. Although even a NZ$1 million penalty would remain lower than the penalties in Australia and the EU, it would recognise the importance of regulating the disclosure of information in a digital era where information is so easily transferable across jurisdictions, without being so onerous that it would massively disrupt the New Zealand online advertising market.

2 Advertising Standards Code

Advertisers' disclosure of customer information to Facebook when creating custom audiences is also regulated by the Advertising Standards Code. The Code is one of the six advertising codes written by the ASA Codes Committee (which consists of advertiser, media, and public representatives) and operates as a non-binding framework alongside existing laws and regulations to set the standards for responsible advertising in New Zealand.[187] Individuals who believe that an advertiser has breached any of the codes may complain to the Complaints Board (a body comprising five public members and four industry members),[188] which will then review the complaint against the codes and may issue a formal written decision to the parties and the media.[189]

---

[186] Privacy Bill, cl 3A.
[187] Advertising Standards Authority, above n 148.
[188] "Complaints Board (ASCB) Members" Advertising Standards Authority <www.asa.co.nz/about-us/complaints-board-ascb-members/>.
[189] "The complaint decision process" Advertising Standards Authority <www.asa.co.nz/complaints/the-complaints-board-decision-process/>.

The Code applies to "all ads placed in any media" that are targeted at New Zealand audiences and controlled by the advertiser.[190] "Ads" are widely defined as "any message expressed in any language and communicated in any medium with the intent to influence the choice, opinion or behaviour of those to whom it is addressed".[191] This definition has been given a wide interpretation by the Complaints Board, who, for example, deemed Netflix's Facebook post "Fuck it's hot" to be an ad because "it was likely to influence consumer opinion in relation to Netflix".[192] Accordingly, the Code applies to advertisers that target a wide range of ads at New Zealanders on Facebook.

The Code is made up of principles that define the overall standards expected of advertisers, rules that explain how the principles are to be applied, and guidelines that provide information and examples to explain each rule.[193] The relevant rule pertaining to advertisers' disclosure of information to Facebook when targeting ads is the "consent" rule.[194] This operates under the principle of "social responsibility", and states that "advertisers must have appropriate consent from the consumer before engaging in personalised direct advertising communications".[195] According to the guidelines, this means that advertisers may only use private personal information (like email addresses and purchase history) for targeted advertising on Facebook if they have first obtained consent from the consumer to collect, store, and use their information for this purpose. This is similar to the authorisation requirements in the Privacy Act and further incentivises advertisers to comply with its provisions.

However, the problem with this rule is that it does not specify the degree of consent required from consumers. This creates uncertainty on two levels – both for advertisers who do not know which standard to apply, and for consumers who do not know which standard to expect. In theory, this could result in advertisers reading the rule differently. Some might read it as requiring a high standard and limit their use of the custom audiences tool – therefore unnecessarily reducing the quality of their targeted advertising. Meanwhile, others might read it as not requiring a high standard and overuse the custom audiences tool – leading to some consumers "consenting" to disclosure without a real understanding of the consequences.

Despite this vagueness, I do not believe amending this rule is necessary for three reasons. The first is because the Code operates alongside the disclosure provisions in the Privacy Act, which already imposes a higher standard for "authorisation". I believe this renders the Code's rule on this issue largely redundant. The second is because the Code explicitly requires its interpretation to be based on the "spirit and intention of the Code" rather than the specific wording of its provisions.[196] This means that clarifying the rule or adding another guideline would not necessarily resolve the vagueness of the standard set by the Code or meaningfully

[190] Advertising Standards Code 2018.
[191] Advertising Standards Code.
[192] *A Morris v Netflix* 19/046, 26 March 2019 at 3.
[193] Advertising Standards Code.
[194] Rule 1(b).
[195] Rule 1(b).
[196] Advertising Standards Code.

affect its application. The third is because there have been no alleged breaches of this rule since its introduction in 2018.[197] This suggests that consumers either do not believe that their rights have been infringed upon or are instead relying on the Act for its stronger enforceability mechanisms.

Further, although the Code lacks legal force,[198] I do not believe strengthening its enforcement mechanisms is necessary. This is because the Code, and decisions made by the Complaints Board, have an "excellent rate of compliance"[199]. This suggests that we should be less concerned about advertisers trying to circumvent the Code and more concerned with ensuring that the complaints process is accessible to consumers. Accordingly, I believe the Code adequately regulates advertisers' disclosure of customer information to Facebook and does not need to change.

D The wrongful targeting issue

1 Targeting vulnerable groups

The first type of wrongful targeting on Facebook this Section will focus on is targeting vulnerable groups. Vulnerable groups are groups which are "susceptible to some harm"[200] due to physical conditions, cognitive processes, or social circumstances.[201] On Facebook, this includes groups like the young, the elderly, the mentally ill, the grieving, and the addicted – each of whom will be disproportionately susceptible to certain ads for certain products and services at certain times. However, there is no law pertaining to the general targeting of vulnerable groups. Thus, how adequately New Zealand regulates advertisers' ability to target these groups on Facebook will differ according to the group and product or service in question.

This Section will primarily focus on food and drink ads targeted at New Zealand children and young people on Facebook. This is because children and young people are the only vulnerable group specifically regulated by the ASA. Protecting children and young people from targeted food and drink ads is important for a number of reasons. First, because food and nutrition are important for people's overall health and well-being. Second, because one in nine New Zealand children (aged two to 14) are obese,[202] which suggests that New Zealand children are over-consuming unhealthy food and drink. Third, because the low cognitive function of children and young people make them highly susceptible to advertising. Finally, because

---

[197] "Search/browse decisions" Advertising Standards Authority <www.asa.co.nz/decisions/search-browse-decisions/>.
[198] "Frequently Asked Questions" Advertising Standards Authority <www.asa.co.nz/resources/faqs/>.
[199] Advertising Standards Authority, above n 198.
[200] George G. Brenkert "Marketing and the Vulnerable" (1998) Business Ethics Quarterly 7 at 7.
[201] At 3.
[202] "Obesity statistics" (12 November 2019) Ministry of Health <www.health.govt.nz/nz-health-statistics/health-statistics-and-data-sets/obesity-statistics#:~:text=Child%20obesity%20statistics,8.2%25%20of%20European%2FOther%20children>.

children and young people are active on Facebook[203] and therefore may be exposed to food and drink ads on it. Although Facebook has an age requirement of 13,[204] it does not require proof of age. This means that underage children can easily access the platform and create new accounts when or if they are locked out by Facebook's review team.[205] Even if Facebook were able to enforce this rule, young people (aged 13 to 17) are still less likely than a "typical" adult Facebook user to make informed decisions around adverting. Thus, it is important to ensure that New Zealand's laws adequately restrict advertisers' ability to target food and drink ads at children and young people on Facebook.

The pertinent law is found in the ASA's Children and Young People's Advertising Code. The Children and Young People's Code applies to all ads controlled directly or indirectly by an advertiser that targets children or young people in New Zealand.[206] This means that it applies to advertisers who target food and drink ads on Facebook. An important feature of the Children and Young People's Code is its wide definition of "targeting", which states that a child or young person is "targeted" if the ad, or product or service advertised, generally appeals to children or young people, or if the expected average audience includes a significant proportion of children or young people.[207] This is effective because it recognises that the content and context of an ad can be used to target children and young people without advertisers directly selecting a young audience, and limits advertisers' ability to target young audiences by proxy variables.

The relevant rule for targeting children (aged 14 and below) is rule 1(i). It states that "ads for occasional food or beverage products (which are high in fat, salt, or sugar) must not target children or be placed in any media where children are likely to be a significant proportion of the expected average audience".[208] In terms of advertising on Facebook, the Complaints Board has taken the view that as long as advertisers utilise Facebook tools to minimise exposure to children, the fact that children under 13 may violate Facebook's terms and be potentially exposed to certain ads is considered outside advertisers' control.[209] Accordingly, I believe this rule adequately restricts advertisers' ability to target food and drink ads on Facebook without unduly limiting their ability to target these products on Facebook at all. The scale of issue also demonstrates that a stricter rule is not required. Investigation of many rule 1(i) complaints made to the Complaints Board, most of which are not upheld, shows that advertisers generally only target ads at users 18 and above,[210] and children generally only ever comprise a very small

[203] Consumer Reports "CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms" (press release, 5 October 2011).
[204] Facebook, above n 13, at cl 3.
[205] Josh Constine "Facebook and Instagram change to crack down on underage children" (20 July 2018) Tech Crunch <https://techcrunch.com/2018/07/19/facebok-under-13/>.
[206] Children and Young People's Advertising Code.
[207] Children and Young People's Advertising Code.
[208] Rule 1(i)
[209] *NZ Dental Association v Frucor, Pepsi Max* 17/286, 12 September 2017 at 5.
[210] *Healthy Auckland Together v Frucor, Pepsi Max* 17/302, 12 September 2017 at 17; *B Kidd v Hell Pizza* 18/405, 11 December 2018 at 4; *Members of Healthy Auckland Together v The Griffin's Food Company* 20/259, 27 July 2020 at 3; *Healthy Auckland Together v Hell Pizza* 20/260, 21 July 2020 at 1; and *Healthy Auckland Together v New Zealand Football/Nestlé* 20/262, 11 August 2020 at 5.

proportion of the viewing audience. Further, the majority of advertisers who have been subject to complaints have been compliant with the complaints process by providing Facebook viewing statistics,[211] and, if in breach, removing the ad.

The relevant rule for targeting young people (aged 14 to 18) is rule 1(j). It states that "a special duty of care must be applied to occasional food and beverage product advertising to young people". Although this does not ban advertisers from targeting food or drink ads at young people on Facebook, it is likely adequate in restricting their ability to do so. This is because allowing young people to be exposed to such ads, while still imposing a higher duty of care on advertisers to target them responsibly, acknowledges that young people are both more intelligent and independent than children and yet more vulnerable than adults. Further, the fact that only two Facebook-related targeting complaints have been made since 2017, both of which were not upheld due to appropriate age-gating,[212] suggests that a stricter enforcement approach is not required.

Although the Children and Young People's Code is the only ASA code dedicated to a specific vulnerable group, there are other provisions across the ASA codes that protect other vulnerable groups from wrongful targeting. For example, the Code for Advertising and Promotion of Alcohol, the Gambling Advertising Code, and the Therapeutic and Health Advertising Code each prohibit advertisers from targeting ads for alcohol,[213] gambling,[214] and weight management programmes[215] at children and young people. The Gambling and Health Codes also restrict advertisers' ability to target gambling and therapeutic and health ads at "vulnerable people" like the sick, elderly, pregnant, and overweight. These provisions reflect a strong intent to protect children and young people from targeted advertising – which is appropriate given that they are a particularly vulnerable group. That said, the fact that "vulnerable groups" are only mentioned three times across the six ASA codes, once in a rule and twice in guidelines, and tend to focus on the content of ads rather than their targeting, potentially renders the codes inadequate in protecting other vulnerable groups from wrongful targeting on Facebook.

This issue would likely be addressed if the ASA Codes Committee introduced a comprehensive rule that specifically restricts advertisers' ability to target vulnerable groups. This rule should be within the Advertising Standards Code's "social responsibility" principle because that principle regulates the placement of all ads.[216] Like rule 1(j) of the Children and Young People's Code, this rule should be titled "targeting vulnerable groups" and state that "advertisers must take special care when targeting ads at vulnerable groups". Its guidelines should include a non-exhaustive list of potential vulnerable groups such as the elderly, the sick, and the mentally ill, and the particular products and services in relation to which those groups

[211] *Healthy Auckland Together v Hell Pizza*, above n 210, at 9; and *Healthy Auckland Together v New Zealand Football/Nestlé,* above n 210, at 2.
[212] *S O'Connor and L Richardson v Red Bull* 18/179, 10 July 2018 at 1; and *Healthy Auckland Together v New Zealand Football/Nestlé*, above n 210, at 5.
[213] Code for Advertising and Promotion of Alcohol, principle 3.
[214] Gambling Advertising Code 2019, rule 1(a).
[215] Therapeutic and Health Advertising Code, guidance f.
[216] Advertising Standards Code, principle 1.

might be vulnerable. Such products and services might include targeting charity donation ads at the elderly or religious services ads at the terminally ill. This would recognise the fact that many vulnerable groups are vulnerable by reference to the product or service pitched at them, rather than being inherently vulnerable. I believe a restrictive, rather than prohibitive, provision is appropriate because it recognises the need to protect vulnerable consumers from wrongful targeting without unfairly limiting advertisers' ability to target ads. This will ensure that advertisers are held more accountable when targeting ads on Facebook and limit the potential harm caused to vulnerable groups. Although, like the codes, this rule would not be legally enforceable, advertisers' compliance with the current codes gives me confidence that such a provision would adequately regulate wrongful targeting on Facebook.

2 Discriminatory targeting

The second type of wrongful targeting on Facebook this Section will focus on is discriminatory targeting. Accordingly, this Section will consider how adequately the Human Rights Act 1993 and the Advertising Standards Code restrict advertisers' ability to discriminate when targeting ads on Facebook. In doing so, it will discuss the need for a clearer regulatory approach and make recommendations about what this should entail.

(a) Human Rights Act 1993

The Human Rights Act (the Act) is New Zealand's primary statute dealing with unlawful discrimination. Its prohibited grounds of discrimination include sex, marital status, religious belief, colour, race, ethnicity, disability, age, political opinion, employment status, family status, and sexual orientation.[217] The section pertaining to advertising discrimination is s 67, which makes it unlawful for advertisers to publish or display any ad which indicates, or could reasonably be understood as indicating, an intention to breach any of the provisions in Part 2. This includes discrimination in the provision of goods, services, land, housing, and accommodation; discrimination in access to places, vehicles, facilities, and educational establishments; and discrimination in matters of employment. Although this section clearly applies to the content of ads that appear on Facebook, it does not apply to the process used to target these ads. This is because its title, wording, and litigation focus on what the ad itself indicates, rather than on what the manner of its publication indicates.[218] This is inadequate because it fails to recognise the harms posed by discriminatory targeting and does not provide a clear ground for individuals to lay such a complaint. Accordingly, I argue that this section ought to be amended to apply clearly to targeting ads. For example, a new subsection might be added to make it "unlawful to target any ad in a manner which indicates, or could reasonably be understood as indicating, an intention to breach any of the provisions in Part 2".

With this amendment, I believe the provision would set an adequate standard on advertisers when targeting ads. This is because the application of s 67 is limited to the types of

[217] Human Rights Act 1993, s 21(1).
[218] *Human Rights Commission v Eric Sides Motor Company Ltd* (1981) 2 NZAR 447 (EOT).

discriminatory targeting that are likely to result in particularly harmful inequalities, while nonetheless protecting a broad range of groups from discrimination in those harmful contexts. Restricting the type of targeting advertisers can be liable for in this way would protect Facebook users to the extent necessary without imposing an overly harsh standard on advertisers to comply with. For example, this would likely prohibit advertisers from targeting job ads at men in a manner that indicates an intention not to offer employment to women,[219] financial service ads at white people in a manner that indicates an intention not to offer equal credit to Māori people,[220] and housing ads at heterosexual couples in a manner that indicates an intention not to sell to homosexual applicants.[221] However, this would not prohibit advertisers from targeting such ads in contexts where the targeting neither indicates an intention to fail to provide to other groups, nor to treat other groups less favourably. This means that advertisers would still retain the ability to target sex-specific products like tampons at women, and age-related services like university ads at high school students, without being liable for unlawful discrimination.

Again subject to my proposed amendment, I also believe the Act's disputes resolution process would adequately regulate complaints about Facebook targeting. Under the Act, individuals who believe they have been discriminated against can complain to the Human Rights Commission, which may investigate and attempt to mediate the complaint.[222] Although the Commission does not have power to enforce these laws and cannot make any rulings, individuals who are unsatisfied with its mediatory approach may refer the complaint to the Director of Human Rights Proceedings, who can undertake proceedings in the Human Rights Review Tribunal (HRRT) on his or her behalf.[223] If the HRRT is satisfied on the balance of probabilities that an advertisers' targeting constitutes a breach, it may award remedies including declarations of breach, conduct restraint orders, and damages.[224] This process gives advertisers an opportunity to take remedial action to quickly and efficiently resolve complaints (which accords with the self-regulatory nature of New Zealand's advertising industry),[225] while still allowing individuals who are not satisfied with an advertiser's response, or who are unable to resolve the complaint, to take the complaint further. I believe this appropriately balances the right for individuals to be adequately compensated for discriminatory targeting against the right for advertisers to potentially mitigate the harms caused by their actions.

Although I have argued that the NZ$10,000 maximum penalty under the Privacy Act[226] inadequately protects privacy rights, I nonetheless believe that the NZ$3,000 maximum penalty under the Human Rights Act[227] is adequate in regulating discriminatory targeting on Facebook. Comparing the frequency with which the relevant sections in each Act have been litigated

[219] Human Rights Act, s 23.
[220] Section 44(1)(b).
[221] Section 53(1)(a).
[222] Section 76.
[223] Section 84.
[224] Section 92I.
[225] Advertising Standards Authority, above n 147.
[226] Privacy Bill, cl 212.
[227] Human Rights Act, s 143.

demonstrates that enforcing privacy rights is currently harder and more urgent than enforcing advertising discrimination rights, and that it therefore warrants steeper penalties. Discrimination issues are likely more self-regulating because the financial and reputational consequences for a company caught discriminating are worse than for a company caught mishandling personal information. This is demonstrated by the fact that Facebook's "largest ever advertiser boycott" resulted from its failure to police racist information and hate-speech, and not from its frequent privacy breaches.[228] Advertisers' fear of being associated with discriminatory practices is driven by a simple commercial calculus – consumers are more likely to boycott a purportedly racist, sexist, or homophobic company than they are an intrusive company. This shows that advertisers do not need the same financial incentive to comply with the Human Rights Act as they do the Privacy Act, and suggests that the current penalty is adequate in regulating discriminatory targeting.

(b) Advertising Standards Code

Discriminatory targeting on Facebook is also regulated by rule 1(c) of the Advertising Standards Code. This states that ads must not "contain anything that is indecent, exploitative, or degrading, or likely to cause harm, or serious or widespread offence, or give rise to hostility, contempt, abuse or ridicule". Although this does not explicitly refer to discrimination, the harm caused by disproportionately exposing privileged groups to opportunities is likely captured by the words "likely to cause harm". The prohibited grounds for offence include "gender; race; colour; ethnic or national origin; age; cultural, religious, political or ethical belief; sexual orientation; gender identification; marital status; family status; disability; occupational or employment status". This is similar to, and therefore reinforces, the grounds of discrimination in Human Rights Act, and effectively recognises the extensive range of factors that can be discriminatory and offensive within advertising.

Although the rule's explicit wording and associated complaints both pertain to ad content, it likely also applies to ad targeting on Facebook. This is because the rule operates within the "social responsibility" principle that requires ads to be "prepared and *placed* with a due sense of social responsibility" and because the Code is interpreted based on its "spirit and intention" rather than its specific wording. That said, I believe amending the rule to explicitly state its application to ad targeting would nonetheless be helpful to clarify its scope and to recognise the harm posed by discriminatory targeting. For example, an amended rule might instead state that ads "must not contain anything, *or be targeted in a way*, that is indecent…". I believe this would adequately regulate discriminatory targeting on Facebook by explicitly prohibiting advertisers from targeting based on discriminatory factors in problematic contexts, and by giving consumers a clear ground on which to raise such complaints. Further, despite this rule's lack of legal force, I believe its operation alongside the Human Rights Act and the dearth of

[228] Alex Hern "Facebook to be hit by its largest ever advertiser boycott over racism" (24 June 2020) The Guardian <www.theguardian.com/business/2020/jun/24/ben-and-jerrys-joins-facebook-advertising-boycott-racism>.

complaints in this area demonstrate that a stricter enforcement approach is not required to ensure advertisers comply with these provisions.

Part IV: Banning targeted advertising?

So far, this dissertation has discussed a number of issues that arise from targeted advertising on Facebook – ranging from privacy to wrongful targeting. It has analysed the applicability and adequacy of New Zealand's laws in regulating these processes and made suggestions on how these laws could be improved to better protect New Zealand Facebook users within this system. However, some believe that to truly address these issues, the necessary response is not to adapt our laws to targeted advertising, but rather to ban targeted advertising altogether.[229] Although this would likely be more effective than my proposed solutions, I believe banning all targeted advertising is neither realistic nor worth the costs. Accordingly, this Part will outline the potential benefits of such an approach in relation to issues of privacy and wrongful targeting, and ultimately explain why the most viable solution to these issues nonetheless remains regulating Facebook's processes rather than banning them.

There are two key reasons why banning targeted advertising would address many of the privacy issues associated with targeted advertising on Facebook. The first is that, if Facebook could no longer make money from targeted advertising, there would be less financial incentive to collect and store as much user information, and therefore less risk of this information being misused. This would make Facebook's information handling function more comparable to a company like Vodafone – which, despite having access to a great deal of personal information about its customers, does not collect and store it because its revenue streams are based on a paid subscription rather than the use of information to target ads. Although Facebook would likely still collect and store information to personalise user content, it would be to a far lesser extent than under its current model. The second is that, if advertisers could no longer target ads at custom audiences on Facebook, there would be no financial incentive to disclose customer information to Facebook, and therefore less risk of this information being misused. This would more effectively deter privacy breaches than the enforceability mechanisms I propose because it would fundamentally change the incentives which lead to privacy breaches in the first place.

Banning targeted advertising would also address many of the issues around targeting vulnerable groups on Facebook. This is because, if advertisers could no longer select target audiences on Facebook, they could no longer target vulnerable groups. Accordingly, there would be less risk of vulnerable groups being manipulated by predatory advertising. However, banning targeted advertising would also remove advertisers' ability to exclude these groups from this kind of advertising. This could negatively impact vulnerable groups, who might be exposed to more problematic or inappropriate ads than before, and advertisers, whose ability to advertise certain products or services might become more tightly regulated to mitigate this. That said, banning targeted advertising would likely still have a net benefit in this area because it would prevent vulnerable groups from being disproportionately targeted. As with privacy, this comprehensive ban would likely deter wrongful targeting of vulnerable groups more

[229] Edelman, above n 166.

effectively than my proposed amendments to the Advertising Standards Code because it would remove the mechanism by which such targeting is possible in the first place. This is also because no matter the thoroughness of a solution that bans some – but not all – targeting, increasingly sophisticated algorithms will likely enable advertisers to get around such a solution via proxy variables.

Banning targeted advertising would also address the issues around discriminatory targeting on Facebook. This is because, if advertisers could no longer select target audiences on Facebook, they could no longer target groups based on discriminatory factors. This means that people might be exposed to opportunities, like ads for jobs and houses, more equitably than they were previously. As with the targeting of vulnerable groups, I believe this approach would more effectively regulate discriminatory targeting than any amendment to the Human Rights Act or Advertising Standards Code because it would remove the mechanism by which discriminatory targeting is possible in the first place, and because it could not be circumvented by targeting proxy variables.

Despite these benefits, the reason New Zealand cannot ban targeted advertising is simple – it does not have the power to do so. If New Zealand were to impose such a ban, Facebook would likely stop operating in New Zealand. This is because leaving would be easier than amending its entire business model for the sake of one small market. There are two key reasons why such an outcome would not be in the public interest. The first is that this would disconnect New Zealanders from the rest of the world. Facebook is the largest social media platform in the world, which makes it an essential hub for connecting New Zealanders with friends, family, businesses, groups, events, and news from around the world. Its loss would be particularly harmful for a geographically isolated country like New Zealand that relies heavily on technology to stay connected. The second is that this would remove individuals' right to make their own decisions about whether to use Facebook. This would be particularly egregious given that the high use of Facebook in New Zealand suggests that New Zealanders generally think that the benefits of Facebook as outweigh the risks around privacy and wrongful targeting.[230]

Moreover, even if overseas regulators successfully imposed an international ban on targeted advertising that forced Facebook to change its business model, I still do not believe such an outcome would be in the public interest. This is because, despite effectively mitigating issues around privacy and wrongful targeting, banning targeted advertising would go against the interests of consumers and advertisers alike. For consumers, a ban on targeted advertising would result in exposure to less relevant ads and a diminished user experience. This is because depriving Facebook of the revenue it collects from targeted advertising, i.e., 98.5 per cent of its yearly revenue,[231] would almost certainly require the company to adopt a paywall to offset this cost. Not only would most users likely prefer to be subjected to targeted ads than be forced to pay for Facebook's service, but the value of the social media network Facebook provides

[230] "Facebook users in New Zealand" (August 2020) NapoleonCat <https://napoleoncat.com/stats/facebook-users-in-new_zealand/2020/08>.
[231] Facebook, above n 6, at 1.

would be greatly diminished by the ensuing unequal access to, and participation in, that network. For advertisers, a ban on targeted advertising would result in less efficient and more expensive advertising. This would be particularly harmful for small businesses, many of which lack the necessary capital and name recognition to compete with larger advertisers in a market without targeted advertising. Accordingly, I believe it is better to regulate these processes and mitigate the potential harms so that consumers and advertisers can still reap the benefits of targeted advertising on Facebook, rather than throwing the baby out with the bathwater.

Conclusion

In today's technological environment, personal information has become the new oil – the "fuel [of] the digital economy".[232] Of particular relevance to this dissertation, it has facilitated the rise and ongoing success of today's multi-billion-dollar advertising industry. Given that it is neither realistic nor in the public interest to ban targeted advertising, it follows that targeted advertising on Facebook is not going away anytime soon – and thus, neither are the associated issues around privacy and wrongful targeting. This means it is the job of regulators to ensure that these processes are adequately regulated to protect consumers without unduly stifling the New Zealand advertising industry. As discussed throughout this dissertation, there are several amendments necessary to accomplish this. The first is to increase the maximum penalties available under the Privacy Act, and the Privacy Commissioner's powers under it, in order to meaningfully enforce its standards against both Facebook and advertisers. The second is to add a new rule to the Advertising Standards Code to protect vulnerable groups from wrongful targeting. The third is to amend the scope of the Human Rights Act and the Advertising Standards Code to explicitly prevent advertisers' from targeting certain ads in a manner that is likely to discriminate.

As with many of the issues raised by targeted advertising on Facebook – the fact that they are not currently being complained about or discussed in New Zealand does not mean that these issues do not exist, or that they will not persist and develop into the future. This means we need to ensure that our law is up to scratch, both the recognise the harms posed by privacy and wrongful targeting and to enforce these rights when and if they become more pressing. Although no one solution can perfectly resolve every aspect of every issue, I believe my proposed amendments will go a long way towards addressing these issues, protecting New Zealand Facebook users, and future-proofing New Zealand's laws.

[232] Louise Matsakis "The WIRED Guide to Your Personal Data (and Who Is Using It)" (15 February 2019) Wired <www.wired.com/story/wired-guide-personal-data-collection/>.

Bibliography

A Cases

1 New Zealand

A Morris v Netflix 19/046, 26 March 2019.

B Kidd v Hell Pizza 18/405, 11 December 2018.

Case Note 2976 [1996] NZPrivCmr 1 (1 November 1996).

Chief Executive of the Department of Internal Affairs v Mansfield [2013] NZHC 2064.

Commissioner of Police v Ombudsman [1988] 1 NZLR 385.

Healthy Auckland Together v Frucor, Pepsi Max 17/302, 12 September 2017.

Healthy Auckland Together v Hell Pizza 20/260, 21 July 2020.

Healthy Auckland Together v New Zealand Football/Nestlé 20/262, 11 August 2020.

Human Rights Commission v Eric Sides Motor Company Ltd (1981) 2 NZAR 447 (EOT).

Members of Healthy Auckland Together v The Griffin's Food Company 20/259, 27 July 2020.

NZ Dental Association v Frucor, Pepsi Max 17/286, 12 September 2017.

Poynter v Commerce Commission [2010] NZSC 38.

Proceedings Commissioner v Commissioner of Police [2000] NZAR 277.

R v Brooker [2007] NZSC 30.

S O'Connor and L Richardson v Red Bull 18/179, 10 July 2018.

2 United States

Department of Housing and Urban Development v Facebook [2019] ALJ No. 01-18-0323-8 (Charge of Discrimination).

B Legislation

1 New Zealand

Commerce Act 1986.

Human Rights Act 1993.

Privacy Act 1993.

Privacy Bill 2020 (34-3).

Advertising Standards Code 2018.

Children and Young People's Advertising Code.

Code for Advertising and Promotion of Alcohol.

Gambling Advertising Code 2019.

Therapeutic and Health Advertising Code.

2 Australia

Privacy Act 1988 (Cth).

3 European Union

Regulation 2016/679 on the General Data Protection Regulation [2018] OJ L 127.

C Official Sources

Colmar Brunton "*New Zealand's Internet Insights 2019*" (InternetNZ, December 2019).

Commonwealth of Australia *Budget 2019-20* (Budget Paper No. 2, 2 April 2019).

Letter from Elizabeth Denham (Information Commissioner of the Information Commissioner's Office) to Facebook Ireland Ltd and Facebook Inc regarding the issuing of a monetary penalty notice under the Data Protection Act 1998 (24 October 2018).

Facebook Reports First Quarter 2020 Results (29 April 2020).

Facebook Reports Fourth Quarter and Full Year 2019 Results (29 January 2020).

Facebook Reports Second Quarter 2018 Results (Facebook, 25 July 2018).

Kensington Swan "Submissions on the Privacy Bill".

Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011).

Privacy Commissioner "Background paper: Including provision for the Commissioner to seek imposition of a civil penalty for serious privacy breaches".

Privacy Commissioner "Submission on the Privacy Bill to the Justice and Electoral Select Committee".

Michael Stelzner *2020 Social Media Marketing Industry Report* (Social Media Examiner, May 2020).

D Secondary Sources

Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove and Aaron Rieke "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes" (2019) 3 PACM HCI 2.

George G. Brenkert "Marketing and the Vulnerable" (1998) Business Ethics Quarterly 7.

Nina Gerber, Paul Gerber and Melanie Volkamer "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behaviour" (2018) 77 COSE 226.

Elleen Pan, Jingjing Ren, Martina Lindorfer, Christo Wilson and David Choffnes "Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications" (2018) 18(4) PoPETs 1.

Frank Presbrey "The history and development of advertising" (2000) 1(1) ASQ.

Paul Roth *Privacy Law and Practice* (online looseleaf ed, LexisNexis).

Christian Schlee *Targeted Advertising Technologies in the ICT Space* (Springer Vieweg, Darmstadt, 2013).

E Other Sources

1 Internet Materials

"Codes" Advertising Standards Authority <www.asa.co.nz/codes/>.

"Complaints Board (ASCB) Members" Advertising Standards Authority <www.asa.co.nz/about-us/complaints-board-ascb-members/>.

"Frequently Asked Questions" Advertising Standards Authority <www.asa.co.nz/resources/faqs/>.

"Search/browse decisions" Advertising Standards Authority <www.asa.co.nz/decisions/search-browse-decisions/>.

"Self-regulation and the Industry Levy" Advertising Standards Authority <www.asa.co.nz/industry/self-regulation-industry-levy/>.

"The complaint decision process" Advertising Standards Authority <www.asa.co.nz/complaints/the-complaints-board-decision-process/>.

Julia Angwin and Terry Parris Jr. "Facebook Lets Advertisers Exclude Users by Race" (28 October 2016) ProPublica <www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>.

Matt Burgess "What is GDPR? The summary guide to GDPR compliance in the UK (24 March 2020) Wired <www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018#:~:text=The%20EU's%20says%20GDPR%20was,those%20that%20interact%20with%20them.>.

Josh Constine "Facebook and Instagram change to crack down on underage children" (20 July 2018) Tech Crunch <https://techcrunch.com/2018/07/19/facebok-under-13/>.

Luke Dale, Daniel Kiley and Kelly Williamson "This is your private life: Facebook faces privacy law enforcement proceedings" (16 March 2020) HWL Ebsworth <https://hwlebsworth.com.au/this-is-your-private-life-facebook-faces-privacy-law-enforcement-proceedings/>.

Data Protection Commission Ireland (@DPCIreland) "@DPCIreland is awaiting from Facebook further urgent details of the security breach impacting some 50m users, including details of EU users which have been affected, so that we can properly assess the nature of the breach and risk to users" <https://twitter.com/DPCIreland/status/1046417378236608512>.

"The essential guide to social media targeting" Digital Marketing Institute <https://digitalmarketinginstitute.com/blog/the-essential-guide-to-social-media-targeting>.

Gilad Edelman "Why Don't We Just Ban Targeted Advertising?" (22 March 2020) Wired <www.wired.com/story/why-dont-we-just-ban-targeted-advertising/>.

"About Facebook Ads" Facebook <www.facebook.com/ads/about/?entry_product=ad_preferences>.

"Accessing & Downloading Your Information" Facebook <www.facebook.com/help/1701730696756992?helpref=hc_global_nav>.

"Ad targeting" Facebook <www.facebook.com/business/ads/ad-targeting>.

"Advertising Policies" Facebook <www.facebook.com/policies/ads/>.

"Commercial Terms" (31 August) Facebook <www.facebook.com/legal/commercial_terms/update>.

"Company Info" Facebook <https://about.fb.com/company-info/>.

"Customer List Custom Audiences Terms" (31 August 2020) Facebook <www.facebook.com/legal/terms/customaudience/update>.

"Data Policy" Facebook (21 August 2020) <www.facebook.com/about/privacy/update>.

"Marketing" Facebook <www.facebook.com/business/marketing/facebook>.

"Terms of Service" Facebook (31 July 2019) <www.facebook.com/terms.php>.

"The Facebook pixel" Facebook <www.facebook.com/business/learn/facebook-ads-pixel>.

"What is the General Data Protection Regulation (GDPR)?" Facebook <www.facebook.com/business/gdpr>.

"Your ad preferences" Facebook <www.facebook.com/ads/preferences/edit/>.

Angela Flannery and Sarah Cass "Liability for breaches of Australia's Privacy Act to increase but class actions unlikely to be supported" (20 May 2020) Holding Redlich <www.holdingredlich.com/liability-for-breaches-of-australia-s-privacy-act-to-increase-but-class-actions-unlikely-to-be-supported>.

Ross Gerber “Snapchat Is Fun, But Facebook Is The King Of Social Media” (13 May 2017) Forbes <www.forbes.com/sites/greatspeculations/2017/03/13/snapchat-is-fun-but-facebook-is-the-king-of-social-media/#4338bad37ccd>.

Alex Hern “Cambridge Analytica: how did it turn clicks into votes?” (6 May 2018) The Guardian <www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.

Alex Hern “Facebook to be hit by its largest ever advertiser boycott over racism” (24 June 2020) The Guardian <www.theguardian.com/business/2020/jun/24/ben-and-jerrys-joins-facebook-advertising-boycott-racism>.

David Ingram “Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law” (19 April 2018) Thompson Reuters <www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P>.

Katie Kenny “All you need to know about the proposed privacy laws” (23 May 2018) Stuff <www.stuff.co.nz/national/104126249/all-you-need-to-know-about-the-proposed-privacy-laws>.

Liarna La Porta “Is your phone always listening to you? (5 September 2019) Wandera <www.wandera.com/phone-listening/>.

Kalev Leetaru “Facebook’s Latest Breach Illustrates The Limits Of GDPR” (14 December 2018) Forbes <www.forbes.com/sites/kalevleetaru/2018/12/14/facebooks-latest-breach-illustrates-the-limits-of-gdpr/#26a2659974a5>.

Antonio Garcia Martinez “Facebook’s Not Listening Through Your Phone. It Doesn’t Have To” (10 November 2017) Wired <www.wired.com/story/facebooks-listening-smartphone-microphone/>.

Louise Matsakis “Facebook’s Targeted Ads Are More Complex Than It Lets On” (25 April 2018) Wired <www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/>.

Louise Matsakis “The WIRED Guide to Your Personal Data (and Who Is Using It)” (15 February 2019) Wired <www.wired.com/story/wired-guide-personal-data-collection/>.

“Obesity statistics” (12 November 2019) Ministry of Health <www.health.govt.nz/nz-health-statistics/health-statistics-and-data-sets/obesity-statistics#:~:text=Child%20obesity%20statistics,8.2%25%20of%20European%2FOther%20children>.

"Facebook users in New Zealand" (August 2020) NapoleonCat <https://napoleoncat.com/stats/facebook-users-in-new_zealand/2020/08>.

Casey Newton "The Trauma Floor: The secret lives of Facebook moderators in America" (25 February 2019) The Verge <www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona>.

"Christchurch shootings prompt new laws for social media platforms in Australia" (26 March 2019) Radio New Zealand <www.radionz.co.nz/news/world/385639/christchurch-shootings-prompt-new-laws-for-social-media-platforms-in-australia>.

Madison Reidy "Cambridge Analytica 'misuse' may affect nearly 64,000 Kiwis, Facebook says" (9 April 2018) Stuff <www.stuff.co.nz/business/102928825/facebook-estimates-63724-kiwis-may-be-affected-by-cambridge-analytica-data-misuse->.

Oscar Schwartz "Digital ads are starting to feel psychic" (13 July 2018) The Outline <https://theoutline.com/post/5380/targeted-ad-creepy-surveillance-facebook-instagram-google-listening-not-alone?zd=1&zi=7awbjkxo>.

Gavin Smith, David Roundtree and Claudia Hall "OAIC's landmark case against Facebook to have major implications on Privacy Act" (12 May 2020) Allens <www.allens.com.au/insights-news/insights/2020/05/oaic-landmark-case-facebook/>.

Nitasha Tiku "What's *Not* Included in Facebook's 'Download Your Data' (23 April 2018) Wired <www.wired.com/story/whats-not-included-in-facebooks-download-your-data/>.

"Losing Face: Two More Cases of Third-Party Facebook App Data Exposure" (3 April 2019) UpGuard <www.upguard.com/breaches/facebook-user-data-leak>.

Jim Waterson "UK fines Facebook £500,000 for failing to protect user data" (25 October 2018) The Guardian <www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica>.

Ben Wolford "What is GDPR, the EU's new data protection law?" GDPR.EU <https://gdpr.eu/what-is-gdpr/>.

2 Press Releases

Consumer Reports "CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms" (press release, 5 October 2011).

Court of Justice of the European Union "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield" (press release No 91/20, 16 July 2020).

Data Protection Commission “Irish DPC submits Article 60 draft decision on inquiry into Twitter International Company’s compliance with Articles 33(1) and 33(5) of the GDPR” (press release, 22 May 2020).

Facebook “An Update on Our Plans to Restrict Data Access on Facebook” (press release, 4 April 2018).

Facebook “Changes to Groups API Access” (press release, 6 November 2019).

Facebook “Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising” (press release, 19 March 2019).

Facebook “Facebook’s commitment to data protection and privacy in compliance with the GDPR” (press release, 30 January 2018).

Facebook “Hard Questions: What Information Do Facebook Advertisers Know About Me?” (press release, 23 April 2018).

Facebook “Our Advertising Principles” (press release, 27 November 2017).

Facebook “Security Update” (press release, 28 September 2018).

Garante Per La Protezione Dei Dati Personali “Cambridge Analytica: the Privacy Guarantor fines Facebook for 1 million euros” (press release, 28 June 2019).

Internet & Jurisdiction Policy Network “More coordination or a less cross-border internet, shows world’s first Internet & Jurisdiction Global Status Report” (press release, 27 November 2019).

Office of the Australian Information Commissioner “Commissioner launches Federal Court action against Facebook” (media release, 9 March 2020).

Office of the Privacy Commissioner “Privacy Commissioner: Facebook must comply with NZ Privacy Act” (media release, 28 March 2018).

Office of the Privacy Commissioner “Privacy Commissioner recommends data portability, brakes on data re-identification and fines up to $1 million” (press release, 3 February 2017).

Christian Porter and Mitch Fifield “Tougher penalties to keep Australians safe online” (media release, 24 March 2019).

3 Other Resources

Naomi Campbell "I'm a big fan of targeted marketing because I am tres lazy and prefer my shopping to come to me, than for me to have to search for it" <www.facebook.com/groups/227268451176371/permalink/640067259896486>.

John Edwards, Privacy Commissioner "My Role, The Privacy Bill and Emerging Challenges" (guest lecture to LAWS423 class, Dunedin, 28 March 2019).