



2021

## The hidden harms of targeted advertising by algorithm and interventions from the Consumer Protection toolkit

Jeannie Marie Paterson Dr

*Professor of Law, Melbourne Law School, and Co-Director at the Centre for Artificial Intelligence and Digital Ethics at the University of Melbourne, Australia*

Shanton Chang

*Professor of Information Behaviour, School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.*

Marc Cheon

*Senior Fellow and Research Fellow in Digital Ethics, School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.*

Chris Culnane

*Honorary Fellow in the School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.*

Suelette Dreyfus

*Academic Specialist, School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia*

Follow this and additional works at: <https://repository.nls.ac.in/ijclp>

### Recommended Citation

Paterson, Jeannie Marie Dr; Chang, Shanton; Cheon, Marc; Culnane, Chris; and Dreyfus, Suelette (2021) "The hidden harms of targeted advertising by algorithm and interventions from the Consumer Protection toolkit," *International Journal on Consumer Law and Practice*: Vol. 9, Article 1.  
Available at: <https://repository.nls.ac.in/ijclp/vol9/iss1/1>

This Article is brought to you for free and open access by Scholarship Repository. It has been accepted for inclusion in International Journal on Consumer Law and Practice by an authorized editor of Scholarship Repository. For more information, please contact [library@nls.ac.in](mailto:library@nls.ac.in).

# THE HIDDEN HARMS OF TARGETED ADVERTISING BY ALGORITHM AND INTERVENTIONS FROM THE CONSUMER PROTECTION TOOLKIT

— Jeannie Marie Paterson\*, Shanton Chang†, Marc Cheong‡,  
Chris Culnane\*\*, Sulette Dreyfus††, and Dana McKay‡‡

***Abstract:** Developments in pervasive data collection and predictive data analytics are allowing firms to target consumers with increasingly precise personalised, behavioural and contextual advertising. These techniques give rise to new risks of harm in the attention economy by unduly influencing or manipulating consumers' decisions and choices, and by narrowing the product options visible and available to them. In many countries, the legal response to concerns about targeted advertising by algorithm has been focused on privacy protection and data rights.*

*These are important initiatives. However, consent-based data rights are unlikely to provide a comprehensive or even adequate response to the risks of harm to consumers occasioned by the kinds of algorithmically targeted advertising that are now possible. This paper suggests that a suite of responses from the consumer protection*

---

\* Dr. Jeannie Marie Paterson is a Professor of Law, Melbourne Law School, and Co-Director at the Centre for Artificial Intelligence and Digital Ethics at the University of Melbourne, Australia.

† Dr. Shanton Chang is a Professor of Information Behaviour, School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.

‡ Marc Cheong is a Senior Fellow and Research Fellow in Digital Ethics, School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.

\*\* Dr. Chris Culnane is a Honorary Fellow in the School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.

†† Dr. Sulette Dreyfus is an Academic Specialist, School of Computing and Information Systems, Faculty of Engineering and Information Technology, University of Melbourne, Australia.

‡‡ Dr. Dana McKay is a Senior Lecturer in Innovative Interactive Technologies, RMIT, Australia.

*toolkit are required to address the different and potentially harmful manifestations of algorithmically targeted advertising. These include bans and warnings as well as making use of standard safety-net prohibitions on misleading and unconscionable/unfair conduct already in place in many jurisdictions.*

**Keywords:** Algorithm, Behavioural Advertising, Consumer Protection, Data Privacy, Misleading Conduct, Profiling, Targeted Advertising, Unconscionable Conduct, Unfairness, Undue Influence.

Introduction .....	2	Bans and Warnings .....	17
Profiling in Consumer Markets .....	6	Prohibitions on Misleading and	
Is There any Harm in Algorithmic		Unconscionable/Unfair Conduct .....	20
Targeted Advertising?.....	9	Conclusion .....	24
Consumer data privacy rights and their			
limits.....	13		

## I. INTRODUCTION

As many of us are now aware, we are living in an age of pervasive digital monitoring.<sup>1</sup> Internet of Things devices,<sup>2</sup> apps,<sup>3</sup> loyalty cards, social media

<sup>1</sup> See Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2016); Daniel Susser, Beate Roessler and Helen Nissenbaum, ‘Technology, Autonomy and Manipulation’ (2019) 8 *Internet Policy Review* 1; Karen Yeung, ‘“Hypernudge”: Big Data as a Mode of Regulation by Design’ (2017) 20 *Information, Communication and Society* 118; Shoshana Zuboff, ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) 30 *Journal of Information Technology* 75; Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

<sup>2</sup> See eg, the Bluetooth enabled and cyber insecure children’s toy ‘Cayla’: Agata Dziedzic, ‘International: Connected Toys Cayla and i-Que Make It “Easy for Anyone to Eavesdrop” on Children’ (*OneTrust DataGuidance*, 8 December 2016) <<https://www.dataguidance.com/international-connected-toys-cayla-que-make-easy-anyone-eavesdrop-children/>> accessed 17 May 2021.

<sup>3</sup> Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 11 (ACCC Digital Platforms Inquiry Report); Joe Tidy, ‘Tik Tok: What is the App, and How Much Data Does it Collect’ (*BBC News*, 3 August 2020) <<https://www.bbc.com/news/technology-53476117>> accessed 17 May 2021; Pat McGrath, Clare Blumer and Jeremy Story Carter, ‘Medical Appointment Booking App HealthEngine Sharing Clients’ Personal Information with Lawyers’ (*ABC News*, 26 June 2018) <<https://www.abc.net.au/news/2018-06-25/healthengine-sharing-patients-information-with-lawyers/9894114>> accessed 17 May 2021. Also, Sarah Perez, ‘Following Apple’s Launch of Privacy Labels, Google to Add a “Safety” Section in Google Play’ (*TechCrunch*, 7 May 2021) <<https://techcrunch.com/2021/05/06/following-apples-launch-of-privacy-labels-google-to-add-a-safety-section-in-google-play/>> accessed 17 May 2021.

platforms,<sup>4</sup> and search engines<sup>5</sup> are engaged in extensive data mining: collecting and analysing vast amounts of data with every consumer interaction. The data collected are linked to individuals or their devices to create a digital profile of that person.<sup>6</sup> Algorithms are used to find correlations between these profiles and to make predictions about the future behaviour of similar individuals and groups. These predictions increasingly inform firms' decisions about who gets access to goods and services, and at what price;<sup>7</sup> with applications in determining access to credit,<sup>8</sup> the cost of insurance,<sup>9</sup> whether to interview a prospective employee,<sup>10</sup> and, the focus of this article, digital advertising.<sup>11</sup> In advertising, algorithmic processes allow firms to target consumers precisely with advertising material that is designed to catch their attention on the basis of their previous browsing habits, current location or predicted interests and

<sup>4</sup> See eg, the Cambridge Analytica saga discussed at: Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' (*The Guardian*, 18 March 2018) <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>> accessed 17 May 2021. See also Nathan Heller, 'Why the Life-Insurance Industry Wants to Creep on Your Instagram' (*The New Yorker*, 26 February 2019) <<https://www.newyorker.com/culture/cultural-comment/why-the-life-insurance-industry-wants-to-creep-on-your-instagram>> accessed 17 May 2021.

<sup>5</sup> See eg, Zoac Doffman, 'Why iPhone, iPad And Mac Users Should Avoid Google Photos' (*Forbes*, 8 May 2021) <<https://www.forbes.com/sites/zakdoffman/2021/05/08/why-you-should-never-use-google-photos-on-your-apple-iphone-ipad-imac-or-macbook/>> accessed 17 May 2021.

<sup>6</sup> See Salinger Privacy, 'Cookies and Other Online Identifiers: Research Paper for the Office of the Australian Information Commissioner' (15 June 2020) 3. See GDPR art 4(1): "'profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

<sup>7</sup> See generally Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing 2016).

<sup>8</sup> See eg, Nikita Aggarwal, 'Machine Learning, Big Data and the Regulation of Consumer Credit Markets: The Case of Algorithmic Credit Scoring' in Nikita Aggarwal and others (eds), *Autonomous Systems and the Law* (Beck 2019). See also Sian Townson, 'AI Can Make Bank Loans More Fair' (*Harvard Business Review*, 6 November 2020) <<https://hbr.org/2020/11/ai-can-make-bank-loans-more-fair#:~:text=AI%20and%20Equality&text=A%20landmark%202018%20study%20conducted,are%20members%20of%20protected%20classes.>> accessed 12 July 2021.

<sup>9</sup> Michele Loi and Markus Christen, 'Insurance Discrimination and Fairness in Machine Learning: An Ethical Analysis' in Michele Loi and Markus Christen, 'Choosing How to Discriminate: Navigating Ethical Trade-Offs in Fair Algorithmic Design for the Insurance Sector' (2021) *Philosophy and Technology*. See also Liam Walsh, 'Bot-backed Suncorp Aims for 80pc Online Claims' (*Australian Financial Review*, 11 May 2021) <<https://www.afr.com/companies/financial-services/bot-backed-suncorp-aims-for-80pc-online-claims-20210511-p57qr2>> accessed 12 July 2021.

<sup>10</sup> Aislinn Kelly-Lyth, 'Challenging Biased Hiring Algorithms' (2021) *Oxford Journal of Legal Studies* (*forthcoming*).

<sup>11</sup> See Julian Thomas, 'Programming, Filtering, Adblocking: Advertising and Media Automation' (2018) 166 *Media International Australia* 34, 35.

behaviours.<sup>12</sup> Through these methods, firms aim to influence consumers' purchasing decisions, as well as to differentiate offers and the pricing of products between identified consumer cohorts or categories.<sup>13</sup>

The growth of algorithmically targeted advertising might initially appear a trivial concern: advertising has long aimed to target the consumers who will be receptive to its messages, and to steer consumers towards particular products and increased consumption. Some have argued that targeted advertising benefits consumers by showing them more relevant ads. However, the use of algorithmic processes to identify fine-grained distinctions between different categories of consumers and to make predictions about their behaviour has produced a fundamental change in the character of advertising in the attention<sup>14</sup> or information<sup>15</sup> economy. This change has a consequential impact on the risk of harm to consumer autonomy and welfare. One concern is that consumers may not be aware of the nature and scope of targeted advertising. Another concern is that algorithmically targeted advertising may unduly influence or manipulate consumer decision-making, as well as undermine their sense of well-being.<sup>16</sup> Concerns also arise over the degree to which algorithmically targeted advertising determines the products that are made visible to individual consumers.<sup>17</sup> What is filtered out as options for consumers may in this context be as significant as what is presented. This feature has the potential for reducing the scope of choice in the market and also for discriminating against individuals and groups. These harmful effects of targeted advertising by algorithm are, moreover, less easily avoided by consumers than might appear at first sight.

---

<sup>12</sup> See eg, 'Google Pay India Users to Start Getting Targeted Ads, Here is How You Can Opt Out' (*The Financial Express*, 12 March 2021) <<https://www.financialexpress.com/industry/technology/google-pay-india-users-to-start-getting-targeted-ads-here-is-how-you-can-opt-out/2211457/>> accessed 12 July 2021; Stuart A Thompson, 'These Ads Think They Know You' (*The New York Times*, 30 April 2019) <<https://www.nytimes.com/interactive/2019/04/30/opinion/privacy-targeted-advertising.html?mtrref=www.google.com&gwh=BC5DDB-91D5483424EFDB04440D2D8F14&gwt=pay>> accessed 12 July 2021; 'Ad Targeting' *Facebook for Business* <<https://www.facebook.com/business/ads/ad-targeting>> accessed 12 July 2021; Paul R. Milgrom and Steven Tadelis, 'How Artificial Intelligence and Machine Learning Can Impact Market Design' (National Bureau of Economic Research, Working Paper Series No 24282, February 2018) 21.

<sup>13</sup> See Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995.

<sup>14</sup> Tim Wu, 'Blind Spot: The Attention Economy and the Law' (2019) 82 *Antitrust Law Journal* 771.

<sup>15</sup> Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

<sup>16</sup> Göran Wågström, 'Why Behavioural Advertising Should be Illegal' (*Forbes*, 5 March 2019) <<https://www.forbes.com/sites/forbestechcouncil/2019/03/05/why-behavioral-advertising-should-be-illegal/?sh=40dd9c065b89>> accessed 12 July 2021.

<sup>17</sup> See generally DQUBE Solutions, Suelette Dreyfus, Shanton Chang and Andrew Clausen, *Drawing Back the Curtain: Consumer Choice Online in a Data Tracking World* (Report, July 2020).

These potentially adverse impacts of algorithmically targeted advertising have become the subject of regulatory attention in a number of countries.<sup>18</sup> Commonly, the regulatory response has been focused on strategies for protecting personal data, often through requiring consumers to be given notice of data collection, retention and use,<sup>19</sup> and buttressing the requirements for consumers to consent to, and withdraw from, these practices.<sup>20</sup> However, although notice and consent procedures may be useful in alerting consumers to data practices, and even act as some check on the unconstrained use of data by digital platforms and other firms, they should not be regarded as comprehensive measures for protecting the rights and interests of consumers. Realistically, consumers simply cannot read and respond to all of the information presented in data collection notices,<sup>21</sup> and firms deploy choice architecture and ‘dark patterns’ that push consumers towards privacy reducing options.<sup>22</sup> Additionally, the impact of individual decisions about data sharing on the collective interests of consumer means that there is a good case for treating algorithmically targeted advertising systematically, rather than leaving the responsibility to affected individuals. Thus, there is interest in some jurisdictions on placing substantive obligations on data controllers to treat data subjects fairly.<sup>23</sup> There has also been increased recognition of the complementary role of consumer protection law in curbing the worst excesses of data mining processes.<sup>24</sup>

<sup>18</sup> See eg, Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (2019) (ACCC Digital Platforms Report); Government of Canada, *Strengthening Privacy for the Digital Age* (Discussion Paper 2019); House of Lords Select Committee on Communications, *Regulating in a Digital World* (2nd Report of Session 2017-2019, March 2019); Competition and Markets Authority, United Kingdom, ‘Online Platforms and Digital Advertising: Market Study Final Report’ (2020).

<sup>19</sup> See eg, Privacy Act 1988 (Cth), Principles 1 and 5 (Australia); California Consumer Privacy Act (California) §§ 1798.100, 1978.130; GDPR arts 12-14 (EU).

<sup>20</sup> GDPR, art 6 (EU). See also Personal Data Protection Bill 2019 (India).

<sup>21</sup> See eg, David Berriby, ‘Click to Agree with What? No One Reads Terms of Service Studies Confirm’ (*The Guardian*, 4 March 2017) <<https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>> accessed 12 July 2021; Øyvind H. Kaldestad, ‘250,000 Words of App Terms and Conditions’ (Norwegian Consumer Council, 24 May 2016) <<https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions>> accessed 12 July 2021.

<sup>22</sup> See eg, Norwegian Consumer Council, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (June 2018); ACCC Digital Platforms Report (n 18) 399-434.

<sup>23</sup> See Mark J. Taylor and Jeannie Marie Paterson, *Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection* (2020) 16(1) IJLT 71 <[https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049\\_688f6d511e7b4119a0dfd2a51c62d319.pdf](https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_688f6d511e7b4119a0dfd2a51c62d319.pdf)> accessed 12 July 2021; Office of the Australian Information Commissioner, ‘Privacy Act Review Issues Paper Submission’ <<https://www.oaic.gov.au/privacy/the-privacy-act/review-of-the-privacy-act/privacy-act-review-issues-paper-submission/executive-summary/>> accessed 12 July 2021.

<sup>24</sup> Stephen Corones and Juliet Davis, ‘Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions’ (2017) 45 Federal Law Review 65;

This article considers the potential for harm to consumer autonomy and welfare from targeted advertising by algorithm and the range of protective strategies drawn from the consumer protection toolkit for responding to those concerns. It argues that there is unlikely to be one comprehensive intervention for protecting consumers from the risks associated with targeted advertising, given the complex technical and policy aspects of its regulation. Rather, the most effective outcomes are likely to be produced through a combination of responses. These include the possibility of bans, disclosure and warnings, and also in regulators making full use of the safety-net prohibitions on unconscionable and misleading conduct already found in most existing statutory regimes. Indeed, these open textured principles offer a flexibility in adapting to socio-technical change which may not be available under more rule-based approaches.

The article begins by considering the digital profiling and predictive analytics which increasingly inform targeted advertising. It considers the harms to consumers arising from these new manifestations of targeted advertising. It then moves to legal responses – noting the options available under data protection law before moving to the complementary opportunities offered by statutory consumer protection regimes. This suite of possible responses is considered with reference to legal regimes in place in India, Australia, the U.S. and the EU. It finishes by noting the need for decision-makers, judges, regulators and consumer advocates, to develop a fulsome understanding of the character, operation and uses of new advertising technologies and, indeed, of algorithmic influences on decision-making generally, recognising that this expertise may not yet exist and should be an ongoing aspiration. While we acknowledge that any attempt to address the extensive market power exercised by digital platforms may additionally require intervention from competition law, in this article we focus on concerns of consumer welfare from a perspective of consumer protection law.

## II. PROFILING IN CONSUMER MARKETS

Advances in digital technologies have allowed consumer behaviour to be incessantly monitored.<sup>25</sup> Data is collected using a range of methods including store and loyalty cards, cookies, web and audio beacons, device or browser fingerprinting and identifiers, and digital platform.<sup>26</sup> Increasingly sophisticated

---

Damian Clifford and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94 Australian Law Journal 741.

<sup>25</sup> Dana McKay, *State of the Art in Data Tracking Technology* (Report, November 2019) 5.

<sup>26</sup> ACCC Digital Platforms Report (n 18) 387-9; Salinger Privacy, *Cookies and Other Online Identifiers: Research Paper for the Office of the Australian Information Commissioner* (15 June 2020) 8, ch 2.

algorithmic processes allow the data collected from these discrete consumer interactions to inform targeted advertising strategies. This is done by combining the data collected from discrete sources to create digital profiles of consumers which are linked to some form of individual or device identifier. These identifiers can then be used to track consumers across their in-store and online interactions to build the richness of the profiles. These consumer profiles can be categorised into groups or segments based on correlations within the different data sets identified by algorithms, and then sold to advertisers. Consumer profiles can further be analysed by statistical methods to find correlations between profiles and preferences, and to make predictions about future behaviour.<sup>27</sup> These findings can also inform advertising.

Importantly, consumer profiling goes deeper than straightforward identifying information such as consumers' names, addresses and birthdates. It includes information about who consumers socialise with, what websites and online material they look at or click on, and their sources of news and other media.<sup>28</sup> Indeed, from an advertising perspective, the traditional identifying details of a consumer may be less important than the information collected about their behaviour. Data profiles are not based on an intimate or relational knowledge of individual consumers. Put another way algorithms do not 'see' into consumers' minds. Rather the digital consumer is an identity constructed from data, what Yeung terms a 'data derivative', namely 'abstractions of an individual made up of fragments of correlated variables identified from a match between some of her attributes with the profiles inferred from masses of attributes from masses of individuals'.<sup>29</sup>

Digital consumer profiles are used as the basis for targeted advertising strategies. The methods range in sophistication and in the degree to which they may assist, annoy or harm consumers. Although descriptions of the different kinds of targeted advertising vary, it is useful to understand the main approaches in order to better target regulatory responses, as well as identify any gaps in that response. One of the most common and well-recognised manifestations of targeted advertising is *retargeting*, which involves sending advertisements that follow consumers across their online browsing about products they may have clicked on earlier. *Contextual advertising* uses the context in which consumer view material to send relevant advertising to them.<sup>30</sup> For

---

<sup>27</sup> See also *ibid* 40.

<sup>28</sup> See also Mariam Nadeem and others, 'Australia v Facebook: Regulating the Market for Attention' (Pursuit, 18 February 2021).

<sup>29</sup> Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 *Regulation and Governance* 505, 515 citing Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Duke University Press 2013).

<sup>30</sup> Privacy (n 26) 39.



example, contextual advertising might show consumers marketing material for raincoats when they browse a weather channel showing a forecast of rain.

*Demographic advertising* targets consumers on the basis of identified consumer segments built from individual profiles. For example, Facebook offers firms the ability to advertise directly to customer lists, either held by the firm or provided by a data firm, and to ‘look alike audiences’ based on the demographic features of their current customers.<sup>31</sup> More subtle characteristics may also be selected. The US Federal Trade Commission revealed some named lists traded between data brokers and suppliers as including “Diabetes Interest”; “Cholesterol Focus”; “Financially Challenged”; and “Urban Scramble”.<sup>32</sup> The ACCC pointed out in its Digital Platforms Report that Facebook advertising categories in Australia included “opposition to immigration”; “far left politics”; “vaccine controversies; and “climate change denial”.<sup>33</sup>

Demographic advertising targets consumers on the basis of categories built from their exhibited behaviours and traits. By contrast, *behavioural advertising* targets consumers on the basis of their predicted interests or behaviours, which are derived from correlations between their digital profile and the behaviour of consumers with similar profiles.<sup>34</sup> An infamous example of behavioural advertising involved Target identifying historical patterns of purchasing behaviour of pregnant women and then sending women who exhibited these behaviours advertisements for baby products.<sup>35</sup> *Differential pricing* is an application of this process which allows firms to differentiate prices between customers according to their predicted ability and willingness to pay.<sup>36</sup>

---

<sup>31</sup> ACCC Digital Platforms Inquiry Report (n 18) 387.

<sup>32</sup> Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability Report* (2014) 117, quoted in Katharine Kemp, ‘Concealed Data Practices and Competition Law: Why Privacy Matters’ (2020) 16 *European Competition Journal* 628, 649.

<sup>33</sup> ACCC Digital Platforms Inquiry Report (n 18) 446.

<sup>34</sup> See eg, Alyssa Foote, ‘Online Ad Targeting Does Work: As Long as It’s Not Creepy’ (*Wired*, 5 November 2018) <<https://www.wired.com/story/online-ad-targeting-does-work-as-long-as-its-not-creepy/>> accessed 12 July 2021; Klint Finley, ‘Facebook and IBM Team Up to Supercharge Personalized Ads’ (*Wired*, 5 June 2015) <<https://www.wired.com/2015/05/facebook-ibm-team-supercharge-personalized-ads/>> accessed 12 July 2021.

<sup>35</sup> Charles Duhigg, ‘How Companies Learn Your Secrets’ (*The New York Times*, 16 February 2012) <<https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>> accessed 12 July 2021. See also the harmful outcomes where the prediction is wrong: Siobhan Smith, ‘I had a Miscarriage but the Targeted Pregnancy Adverts keep Coming’ (*Metro*, 21 April 2021) <<https://metro.co.uk/2021/04/21/i-had-a-miscarriage-but-the-targeted-pregnancy-adverts-keep-coming-14427222/>> accessed 12 July 2021.

<sup>36</sup> Frederik Zuiderveen Borgesius and Joost Poort, ‘Online Price Discrimination and EU Data Privacy Law’ (2017) 40 *Journal of Consumer Policy* 347, 351; Maurice E. Stucke and Ariel Ezrachi, ‘How Digital Assistants Can Harm Our Economy, Privacy, and Democracy’ (2017) 32 *Berkeley Technology Law Journal* 1239, 1264. Also N. Levy, ‘Online Sales and Differential Pricing’ (2018) *Practical Ethics* <<http://blog.practicaethics.ox.ac.uk/2018/10/online-sales-and-differential-pricing/>> accessed 12 July 2021.

*Location tracking* adds value to these other kinds of targeted advertising, particularly when combined with Bluetooth beacons that allow precise and indoor identification of location. Location data links information about actual behaviour to digital profiles.<sup>37</sup> It also allows advertising to be directed to consumers in specific locations with the possibility of linking the context created by consumers' location to predictions about what they might want in that location,<sup>38</sup> for example, cafes in a fashionable inner-city area.

### III. IS THERE ANY HARM IN ALGORITHMIC TARGETED ADVERTISING?

On one view, algorithmically targeted advertising is just a continuation of established practices. It might be argued that firms have always tried to influence consumer preferences. All marketing has the aim of influencing consumers' purchasing decisions and it has long sought to optimise its outreach to its intended audience. Bricks-and-mortar stores aim to influence consumer choice through their advertising, by the very way in which they display their products, and the ambience they create inside the store.<sup>39</sup> By and large these practices are not prohibited under existing law. Indeed, on one view, targeted advertising may make life easier for consumers. In an age where consumers are overloaded by information, the promise of targeted advertising is that it filters out irrelevant material and assists us to make choices that may otherwise be overwhelming.<sup>40</sup>

However, the uses of algorithmic processes in advertising allow firms to go well beyond what has been possible in the past. Although there is little empirical data on the effectiveness of targeted advertising, and it has been suggested that the influence of such methods may be exaggerated,<sup>41</sup> there remain ongoing concerns about the risk of harm to consumers these approaches may generate.

---

<sup>37</sup> Privacy (n 26) 39.

<sup>38</sup> ACCC (n 26) 385-386.

<sup>39</sup> cf Shmuel I. Becher, Yuval Feldman and Meirav Furth, 'Seductive Oral Deals' (2020) Law & Psychology eJournal.

<sup>40</sup> Gerhard Wagner and Horst Eidenmuller, 'Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions' (2019) 86 The University of Chicago Law Review 581 ('Down by Algorithms?'). Also, Melanie Heck and others, 'Exploring Gaze-Based Prediction Strategies for Preference Detection in Dynamic Interface Elements' in Proceedings of the 2021 Conference on Human Information Interaction and Retrieval (Association for Computing Machinery, New York, NY, USA) 129-139 <<https://doi.org/10.1145/3406522.3446013>> accessed 12 July 2021.

<sup>41</sup> Natasha Lomas, 'The Case against Behavioral Advertising is Stacking Up' (*TechCrunch*, 21 January 2019) <<https://techcrunch.com/2019/01/20/dont-be-creepy/>> accessed 12 July 2021; Gilad Edelman, 'Why Don't we Just Ban Targeted Advertising' (*Wired*, 22 March 2020) <<https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/>> accessed 12 July 2021.

These concerns arise from the very features that make targeted advertising by algorithm attractive to firms, namely the opportunity to target advertising to narrowly drawn consumer profiles, with different consumers seeing different material and others not seeing some content or prices at all. These features raise significant potential risks to consumer autonomy and welfare, including through a lack of transparency, constraining consumer choice, the manipulation of purchasing decisions and the exclusion of certain consumers and groups of consumers.<sup>42</sup>

Working through these concerns, the most immediate objection to algorithmically targeted advertising lies in the lack of transparency and accountability.<sup>43</sup> Consumer yield the data that fuels this form of advertising, yet many consumers are unaware of the extent of the use made of that data in curating what they see.<sup>44</sup> In this sense, the fundamental data for access deal underlying many consumer interactions with digital platforms involves an element of trickery or even deception. Consumers may be unaware that an advertisement they see online is seen only by them, or people thought to be like them, and that other consumers see different options.

Additionally, by removing alternative options from consumers' sight, targeted advertising narrows their opportunities for choice.<sup>45</sup> This means consumers are making decisions from a position of less than full information, undermining the preconditions for the exercise of autonomy. This may well lead to a reduced number of and variation in the overall options presented to consumers. In other words, consumers may be constrained in their own echo-chambers of advertising that constrain their world view on the basis of their constructed digital profiles.<sup>46</sup>

Targeted advertising may, moreover, exercise considerable and possibly undue influence on consumer preferences, including by triggering pre-existing sensitivities or making use of unconscious biases to the detriment of consumers. Indeed, scholars describe the process as involving as involving

---

<sup>42</sup> See In particular, Eliza Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8 *Law, Innovation and Technology* 1; Gerhard Wagner, 'Down by Algorithms? Siphoning Rents, Exploiting Biases and Shaping Preferences the Dark Side of Personalized Transactions' (2019) 86 *University of Chicago Law Review* 581.

<sup>43</sup> Jeannie Paterson, Gabby Bush and Tim Miller, 'Transparency to Contest Differential Pricing' (2021) 93 *Computers and Law* 49.

<sup>44</sup> ACCC Digital Platforms Inquiry Report (n 18) 383.

<sup>45</sup> Calo (n 13) 1002-3; Eliza Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8 *Law, Innovation and Technology* 1, 7.

<sup>46</sup> Roger Brownsword, 'From Erehwon to AlphaGo: For the Sake of Human Dignity, Should We Destroy the Machines?' (2017) 9 *Law, Innovation and Technology* 117.

‘manipulation’,<sup>47</sup> a ‘hypernudge’,<sup>48</sup> ‘unfair persuasion’,<sup>49</sup> and consumers as being ‘drawn down by algorithms.’<sup>50</sup> This concern is most immediately apparent in behavioural advertising which seeks to link advertising to consumers’ predicted interests or behaviours in order to promote products that may attract attention without actually benefiting them. For example, rich foods or expensive cosmetics might be advertised at times of day when consumers are predicted to be feeling tired or stressed or people exhibiting low self-esteem might be targeted with advertisements for diet products, or cosmetic surgery.<sup>51</sup> Demographic advertising might work to similar effect, for example, by advertising alcohol to vulnerable teens.<sup>52</sup> Even contextual advertising, which is less dependent on consumer digital profiles, may work to similar effect where the context of consumers’ online search is used to send advertisements for products that are palpably unlikely to promote their welfare. Examples might include advertisements for expensive funeral insurance shown to consumers seeking information about bereavement support groups, payday loans to consumers seeking information about gambling help<sup>53</sup> or opioids to consumers experiencing back pain.<sup>54</sup>

Algorithmically targeted advertising further has the potential to entrench existing inequalities by allowing firms to discriminate between different consumer profiles. This creates particular risks for vulnerable and marginalised consumers who may disproportionately be restricted in their purchasing choices and subject to unfavourable pricing. For example, there is potential for

---

<sup>47</sup> Calo (n 13); Damian Clifford, ‘Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?’ in Lilian Edwards, Burkhard Schafer and Edina Harbinja (eds), *Future Law: Emerging Technology, Regulation and Ethics* (Edinburgh University Press 2020).

<sup>48</sup> Yeung (n 29).

<sup>49</sup> Natali Helberger, ‘Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law’ in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Hart Publishing 2016) 135.

<sup>50</sup> Wagner and Eidenmuller (n 42).

<sup>51</sup> Rebecca Rosen, ‘Is This the Grossest Advertising Strategy of All Time’ (*The Atlantic*, 4 October 2013) <<https://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/>> accessed 12 July 2021; ‘Emotional and Sentiment Targeting’ (*AdmantX*) <<https://www.admantx.com/emotional-and-sentiment-targeting/>> accessed 12 July 2021.

<sup>52</sup> ‘Facebook Told Advertisers It Can Identify Teens Feeling “Insecure” and “Worthless”’ (*The Guardian*, 1 May 2017); Sidney Fussell, ‘Facebook Allow Drug Ads to Target Teens, Activists Say’ (*Wired*, 4 May 2021). See also DQUBE Solutions (n 17) 45-6.

<sup>53</sup> See also ‘Video Games You Play Are Using Sneaky Tactics’ (*ABC News*, 3 May 2021) <<https://www.abc.net.au/news/2021-05-03/video-games-you-play-are-using-sneaky-tactics-four-corners/100098826>> accessed 12 July 2021.

<sup>54</sup> Alison Branley, ‘Google Search Data Used by Pharma Giant to Bombard Users with Ads for Addictive Opioids’ (*ABC News*, 13 July 2019) <<https://www.abc.net.au/news/2019-07-13/searches-data-mined-by-pharma-giant-to-promote-new-opioid/11300396>> accessed 12 July 2021.

discrimination through mechanisms such as Facebook’s advertising categories, which allows targeting on the basis of features that may characterise disadvantaged groups.<sup>55</sup> In addition, targeted advertising creates the potential to exclude social groups from particular markets altogether.<sup>56</sup> For example, in the U.S. Facebook has been criticised for allowing advertisers to exclude certain groups based on ‘racial affinity’.<sup>57</sup>

Reliance on inaccurate and incomplete data may further produce inequitable outcomes that reinforce the existing marginalisation of individuals or groups.<sup>58</sup> This is a particular concern where automated processes are premised on unrepresentative data, such as where particular social groups are missing because historically, they have not participated in the spaces from which the data is collected.<sup>59</sup> Inaccurate and incomplete data risk recommendations that are not welfare enhancing for people whose preferences and profiles are not included in the data set on which recommendation are based. Where there is no data on a group, there will be no products identified as suitable for them — they simply miss out or must make do with suboptimal results. There is also a risk that data sets will become skewed as between those who actively do and do not exercise rights over their personal data. If those who exercise control over data are viewed as more savvy, then those who do not do this may be left at the disadvantageous end of differential pricing.

In response to these various concerns, it might be commented that consumers can simply choose not to be influenced by targeted advertising: they

---

<sup>55</sup> See DQUBE Solutions (n 17). Also, Samuel Gibbs, ‘Women Less Likely to Be Shown Ads for High-Paid Jobs on Google, Study Shows’ (*The Guardian*, 8 July 2015) <<https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>> accessed 12 July 2021; Karen Hao, ‘Facebooks Ad-Serving Algorithm Discriminates by Gender and Race’ (*MIT Review*, 5 April 2019) <<https://www.technologyreview.com/2019/04/05/1175/facebook-algorithm-discriminates-ai-bias/>> accessed 12 July 2021.

<sup>56</sup> Nicholas Davis, ‘The Future Relationship between Technology and Inequality’, *How Unequal? Insights on Inequality* (Report, Committee for Economic Development of Australia, April 2018) 110; Select Committee on Artificial Intelligence, *AI in the UK: Ready, Willing and Able?* (House of Lords Paper No 100, Session 2017-2019) 108; *The Future Computed: Artificial Intelligence and Its Role in Society* (Microsoft, 2018) 58-9.

<sup>57</sup> Julia Angwin, Ariana Tobin and Madeleine Varner, ‘Facebook (Still) Letting Housing Advertisers Exclude Users by Race’ (*Pro Publica*, 17 November 2017) <<https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>> accessed 12 July 2021; Alex Hern, ‘Facebook Lets Advertisers Target Users Based on Sensitive Interests’ (*The Guardian*, 16 May 2018) <<https://www.theguardian.com/technology/2018/may/16/facebook-lets-advertisers-target-users-based-on-sensitive-interests>> accessed 12 July 2021.

<sup>58</sup> Select Committee on Artificial Intelligence (n 56) 119.

<sup>59</sup> Lilian Edwards and Michael Veale, ‘Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For’ (2017) 16 *Duke Law and Technology Review* 18. See also, generally, Matt J. Kusner and Joshua R. Loftus, ‘The Long Road to Fairer Algorithms’ (2020) 578 *Nature* 34.

can tighten privacy settings, disable settings allowing personalised advertising, look in several sources for products and compare bricks and mortar stores. However, this response is practically unrealistic. Given the current lack of transparency, and likely lack of understanding about algorithmic targeted advertising, it is not straightforward for consumers to step out of the ‘bubble’ of personalisation created around them to access other opportunities, particularly in circumstances where going ‘out to shop’ is not safe or viable. Navigating online privacy controls is commonly time-consuming and sometimes tricky. The hurdles for consumers taking control of their data privacy are amplified by the common use of choice architecture in the display of privacy notices and contract terms. These may use ‘dark patterns’ which confuse consumers and steer them towards data sharing options.<sup>60</sup> Privacy enhancing and data preserving self-help technologies are available but may require a certain level of technical knowledge and expertise to identify and install.<sup>61</sup> Even the results of search engine inquiries or comparison websites may be tainted, with the ranking of results in some cases determined by payments or commissions<sup>62</sup> or personalisation based on consumers’ digital profiles.<sup>63</sup>

#### IV. CONSUMER DATA PRIVACY RIGHTS AND THEIR LIMITS

Regulators and legislators have responded in different ways to concerns about algorithmically targeted advertising.<sup>64</sup> One of the most common responses is through reform to data privacy law, primarily through provisions insisting on through robust mechanisms for obtaining consent to data collection and use. The most prominent example of such as this kind of regime is the General Data Protection Regulation (“GDPR”).<sup>65</sup> Consent is a central tenet of the GDPR.<sup>66</sup> Under Art 6(1), personal data may not be processed unless under

<sup>60</sup> Forbruker Rådet, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (Report, 27 June 2018); Shayne Bowman and Chris Willis, ‘We Media: How Audiences Are Shaping the Future of News and Information’ (The Media Center at the American Press Institute, 2003) Jamie Luguri and Lior Jacob Strahilevitz, ‘Shining a Light on Dark Patterns’ (2021) 13 *Journal of Legal Analysis* 43.

<sup>61</sup> See eg, The Royal Society, ‘Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis’ (March 2019) 10.

<sup>62</sup> See Google Ads, ‘What is Paid Search?’ <[https://ads.google.com/intl/en\\_au/home/resources/what-is-paid-search/](https://ads.google.com/intl/en_au/home/resources/what-is-paid-search/)> accessed 12 July 2021.

<sup>63</sup> See ACCC Digital Platforms Inquiry (n 18) 23.

<sup>64</sup> Helberger (n 49).

<sup>65</sup> Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (‘GDPR’) art 25. See generally Lee A. Bygrave, ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 4 *Oslo Law Review* 105.

<sup>66</sup> See Inge Graef, Damian Clifford and Peggy Valcke, ‘Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law (2018) 8 *International Data Privacy Law* 200.

a lawful basis specified by the regulation or the data subject has given consented to the use. Art 4 defines operative consent as:

any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by affirmative action, signifies agreement to the processing of personal data relating to him or her.

These processes mean that under the GDPR, consent must be given to each of the purposes for which data may be processed, the consumer must have the option not to consent to these purposes and may revoke consent at any time.<sup>67</sup> Information about the processes for which consent is being given must be 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'.<sup>68</sup>

Law reform initiatives in India have proposed similar levels of safeguard for consent to data collection and processing.<sup>69</sup> In India, the Personal Data Protection Bill 2019 (India)<sup>70</sup> seeks to provide for protection of personal data of individuals.<sup>71</sup> Under section 11, personal data 'shall not be processed, except on the consent given by the data principal at the commencement of its processing' or one of the other legal bases for processing is met. Section 11(2) of the Bill sets out criteria for valid consent, including requiring consent to be free, informed, specific and clear. In addition, the Bill proposes a considerable governance role for 'data fiduciary' who is 'any person ... who alone or in conjunction with others determines the purpose and means of processing of personal data'.<sup>72</sup> The data fiduciary under the Bill is under a responsibility to process personal data 'in a fair and reasonable manner and ensure the privacy of the data principal'.<sup>73</sup> Algorithmically targeted advertising raises the tension between a statutory appropriation of the concept of a fiduciary who is supposed to act in the best interests of beneficiaries, and a context where the very

---

<sup>67</sup> GDPR, art 13.

<sup>68</sup> *ibid* art 12.

<sup>69</sup> See 'The Evils of Online Targeted Advertising' (*One India One People*, 1 August 2020) <<https://oneindiaonepeople.com/the-evils-of-online-targeted-advertising/>> accessed 12 July 2021.

<sup>70</sup> Following recommendations in the Report of the Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India 2018).

<sup>71</sup> See also Taylor and Paterson (n 23).

<sup>72</sup> Personal Data Protection Bill 2019 (India), s 3. There is a further category of 'significant data fiduciary'. The Personal Data Protection Bill 2019 (India), s 26 establishes the conditions under which a data fiduciary may be defined as a significant data fiduciary, and thus subject to additional responsibilities.

<sup>73</sup> Personal Data Protection Bill 2019 (India), s 5(a).

purpose of that collection is to inform commercial advertising.<sup>74</sup> Nonetheless, the proposal represents recognition that consent-based mechanisms are not on their own sufficient to protect consumers' interests. A more substantive regulatory standard is required.<sup>75</sup> Consistently, in Australia, a review of the Privacy Act 1988 has also raised the possibility of measures for introducing more robust requirements for consent to the collection and use of personal data, as well as a general fairness obligation on data controllers.<sup>76</sup>

Processes for obtaining consent that meet the standards of 'freely given, specific, informed and unambiguous' or 'voluntary, express and informed' will not necessarily ensure that consumers read and accurately assess the guidance they are given on the purposes of the data processing for which consent is sought. The requirements do demand a more rigorous verification of something closer to informed consumer consent than currently exists in private law. This may stem the flow of data that feeds algorithmic advertising. However, it is increasingly recognised by scholars and lawmakers that these reforms will not provide a complete or even adequate response to concerns over algorithmic advertising.<sup>77</sup>

Seeking consent, usually preceded by mandatory disclosure of the information deemed relevant to decision-making, is of course the classic neoliberal response to consumer protection. It seeks to correct the imperfections of the market by empowering consumers to themselves manifest better choices.<sup>78</sup> As in other fields, it is clear that requirements to seek consent to data use, even though more robust and rigorous processes are not the entire solution to the problem of significant information asymmetry in the consumer market. The challenges of relying on individual consent-based processes for data collection and processing are particularly germane in contexts where consumers have low or uneven literacy rates, or poor awareness of their consumer rights.<sup>79</sup>

Consumers cannot meaningfully be asked to give up their data without some understanding of what may be done with that data, the inferences

---

<sup>74</sup> See Lina M. Khan and David E. Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133 *Harvard Law Review* 497.

<sup>75</sup> See Dennis D. Hirsch, 'From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics' (2020) 79 *Maryland Law Review* 439.

<sup>76</sup> See Office of the Australian Information Commissioner, 'Privacy Reform Crucial to Building Public Trust' (14 December 2020) <<https://www.oaic.gov.au/updates/news-and-media/privacy-act-reform-crucial-to-building-public-trust/>> accessed 12 July 2021.

<sup>77</sup> Corones and Davis (n 24); Clifford and Paterson (n 24); Yeung (n 29).

<sup>78</sup> Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.

<sup>79</sup> S. Mutyala, M. Reddy and K. Reddy, 'Consumer Protection in India: Some Challenges and Measures in Global Market Milieu' (2020) 10 *Journal of Research in IT and Management* 19, 31.



that may be drawn about them, the ways in which their data may be combined with other sources and the consequences for their market interactions. Yet it seems likely that consumers are currently largely unaware of these processes,<sup>80</sup> and indeed misunderstand the purpose of privacy policies.<sup>81</sup> Some form of consumer education strategy might assist in narrowing this information gap. However, ultimately, problems of information overload and inaccessibility, along with the pressures of time, limit the use that most consumers can make of privacy policies in providing informed consent to data collection and processing practices they deal with on a daily basis.<sup>82</sup> There can be little real expectation that consumers will make use of privacy policies<sup>83</sup> in circumstances where they struggle to read the disclosure statements associated with financial products,<sup>84</sup> are confused by contract boilerplate<sup>85</sup> and cannot hope to read the terms of online retailers to know their rights to return.<sup>86</sup> There is also the risk of developing fatigue on the part of consumers following from constant request for consent,<sup>87</sup> which undermines the faith put on privacy notices and policies in protecting consumer data privacy.

Moreover, the very digital form of privacy policies enables firms to deploy significant hurdles to consumers trying to exercise control over data privacy.

---

<sup>80</sup> Lina M. Khan and David E. Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133 *Harvard Law Review* 497, 519-520.

<sup>81</sup> See eg, ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) 174; Policy and Research Group, Office of the Privacy Commissioner of Canada, 'Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act' (Discussion Paper, 2016) 9; Competition and Markets Authority, United Kingdom, 'Online Platforms and Digital Advertising: Market Study Final Report' (2020) 166-72: generally reporting consumers assume privacy policies are about restricting use of data.

<sup>82</sup> See eg, Russell Korobkin, 'Bounded Rationality, Standard Form Contracts, and Unconscionability' (2003) 70 *University of Chicago Law Review* 1203; Australian Securities and Investments Commission, *Financial Literacy and Behavioural Change* (Report REP 230, March 2011).

<sup>83</sup> Schmuell I. Becher and Uri Benoliel, 'Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR' in Klaus Mathis and Avishalom Tor (eds), *Consumer Law and Economics* (Springer 2020) 179-204.

<sup>84</sup> Australian Treasury, *Financial System Inquiry* (Final Report, 2014) 193.

<sup>85</sup> Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013); Uri Benoliel and Schmuell I. Becher, 'The Duty to Read the Unreadable' (2019) 60 *Boston College Law Review* 2255.

<sup>86</sup> David Berreby, 'Click to Agree with What? No One Reads Terms of Service, Studies Confirm' (*The Guardian*, 4 March 2017) <<https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>> accessed 12 July 2021. See also Aleecia M. McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) *I/S A Journal of Law and Policy for the Information Society*.

<sup>87</sup> ACCC Digital Platforms Inquiry (n 18) 463. cf the do not track proposal at: <<https://www.eff.org/issues/do-not-track>> accessed 12 July 2021.

Privacy policies are complex and opaque.<sup>88</sup> Studies have found that representations about how to opt out of data collection practices by digital platforms and other entities collecting information about consumers are often unhelpfully oblique, and the options difficult to access.<sup>89</sup> Choice architecture further steers consumers away from making choices that would restrict data flows and are counter to the interests of firms using that data.<sup>90</sup>

## V. BANS AND WARNINGS

There are other available strategies that might be utilised to complement data privacy reforms and thereby provide more comprehensive protection to consumers than through consent mechanisms and their consequent individualism of responsibility. Which of these might be adopted will depend on policy choices and regulatory decisions about how compelling the case for consumer protection is considered to be within the social and cultural context in question.

The most robust response would be to ban algorithmically targeted advertising altogether.<sup>91</sup> There have been suggestions from some regulators, scholars and consumers advocates for comprehensive bans on targeted advertising using pervasive tracking or profiling techniques, because of its significant potential to harm consumers with particular sensitivities and situational vulnerabilities.<sup>92</sup> There have also been proposals to ban specific applications of targeted advertising, such as advertising involving the profiling of children.<sup>93</sup> This may appear a considerable intervention in the operation of the market, but equally

<sup>88</sup> See eg, Norwegian Consumer Council, ‘Out of Control: How Consumers are Exploited by the Online Advertising Industry’ (2020) 60ff; ACCC Digital Platforms Inquiry (n 18) 403ff.

<sup>89</sup> ACCC Digital Platforms Inquiry (n 18) 723.

<sup>90</sup> On the information asymmetry between consumers and digital service providers and the use of design strategies to nudge consumers away from privacy protection online, see: Norwegian Consumer Council, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (Report, 27 June 2018). See also Katharine Kemp, ‘Concealed Data Practices and Competition Law: Why Privacy Matters’ (2020) 16 *European Competition Journal* 628; Lauren E. Willis, ‘Deception by Design’ (2020) 34 *Harvard Journal of Law and Technology* 115.

<sup>91</sup> See also Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, 17/EN, WP251 (3 October 2017); Margot E. Kaminski, ‘The Right to Explanation, Explained’ (2018) 34 *Berkeley Technology Law Journal* 189: discussing whether personalised advertising may be prohibited under art 22 of the GDPR.

<sup>92</sup> Emma Wollacott, ‘European Regulator Calls for Ad Targeting Ban’ (*Forbes*, 11 February 2021) <<https://www.forbes.com/sites/emmawollacott/2021/02/11/european-regulator-calls-for-ad-targeting-ban/?sh=6504969a2523>> accessed 12 July 2021. See also Gilad Edelman, ‘Why Don’t We Just Ban Targeted Advertising’ (*Wired*, 22 March 2020) <<https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/>> accessed 12 July 2021, also suggesting that such a ban may not reduce revenue for advertisers.

<sup>93</sup> ACCC Digital Platforms Inquiry (n 18) 34-6.

what is contemplated is not a ban on all advertising. There have, moreover, been doubts raised about the effectiveness of targeted advertising,<sup>94</sup> especially given an overall lack of transparency in the online platform market.<sup>95</sup> So the loss to the industry from a ban on some forms of targeted advertising may not be too great.

We might also expect discriminatory or unfounded differential pricing to come under scrutiny, also with possible bans. An exemplar may be the Indian Consumer Protection E-Commerce Rules 2020, s 4(11)(b) which preclude an e-commerce entity from manipulating price offerings or discriminating between consumers on the basis of arbitrary classifications.<sup>96</sup>

An alternative, or indeed complement, to bans is to assist consumers in better understanding the breadth of deployment of algorithmic advertising, and the associated phenomenon of differential pricing.<sup>97</sup> Here it might be possible to demand that consumers be provided with warnings when these strategies are deployed. The goal would not be to provide full disclosure of all relevant terms and conditions but to draw consumers' attention to unfamiliar or possibly harmful advertising practices, for example 'this price is personalised to you and other consumers may be offered different prices'.

The efficacy of regulatory reliance on mandatory disclosure as a central strategy of consumer protection has been challenged in a number of ways.<sup>98</sup> As we have seen with privacy policies, often the information provided is simply too complex and confusing for consumers to make sense of it. One response is to emphasise the role of focused warnings as opposed to lengthy disclosures.<sup>99</sup> We know that concise, targeted information is generally a more effective way of communicating with individuals than generalised high-volume information.<sup>100</sup> A simple stark warning about personalisation or micro-targeting in advertising offerings may be sufficient to prompt consumers to look further

---

<sup>94</sup> Edelman (n 92).

<sup>95</sup> Kemp (n 32).

<sup>96</sup> See also Manoranjan Ayilyath, 'Consumer Protection in E-Commerce Transactions in India: Need for Reforms' (*SSRN*, 8 April 2020) <<http://dx.doi.org/10.2139/ssrn.3571069>> accessed 12 July 2021.

<sup>97</sup> A technique called 'boosting': See eg, Phillip Lorenz-Spreen and others, 'How Behavioural Sciences Can Promote Truth, Autonomy and Democratic Discourse Online' (2020) 4 *Nature Human Behaviour* 1102.

<sup>98</sup> Geraint Howells, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32 *Journal of Law and Society* 349.

<sup>99</sup> See Anthony Duggan and Iain Ramsay, 'Front-End Strategies for Improving Consumer Access to Justice' in Michael Trebilcock, Anthony Duggan and Lorne Sossin (eds), *Middle Income Access to Justice* (University of Toronto Press 2014) 95.

<sup>100</sup> Andrew Godwin and Ian Ramsay, 'Financial Products and Short-Form Disclosure Documents: An Empirical Study' (2016) 10 *Capital Markets Journal* 212.

afield before making a purchasing decision. It might even lead them reflect on their data privacy choices, and the value of enhancing privacy by refusing to share data for advertising purposes.<sup>101</sup> This kind of approach has, for example, been utilised in recent reforms in consumer credit law in Australia by requiring warnings about financial risk and alternative sources of credit to be displayed alongside offers of high cost ‘payday’ loans.<sup>102</sup> The EU already requires traders to inform consumers about differential pricing.<sup>103</sup> Under the proposed EU Digital Services Act, greater transparency measures would apply to online advertising including a requirement for platforms to display ‘meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed’.<sup>104</sup>

Digital technology may be used to improve the disclosure of information relevant to the consumer consent process, and also the saliency of particular kinds of information such as warnings.<sup>105</sup> Technology might also be utilised to allow consumers to understand and exercise their rights under law more easily. For example, the California Consumer Privacy Act of 2018 requires businesses to incorporate a ‘Do Not Sell My Personal Information’ link on their website homepage,<sup>106</sup> which takes consumers to a designated webpage which enables them to ‘opt-out’.<sup>107</sup> It is further possible to envisage technology being used to assist consumers in decision-making, not by deciding for them, but by guiding them through the decision-making process to an optimal outcome. What is sometimes termed ‘layered’ or ‘smart’ disclosure allows for the possibility of ‘data to be generated and analysed by, or tailored to the specific needs of, the reader who is accessing it’.<sup>108</sup> This process allows consumers to access

---

<sup>101</sup> See also Wagner and Eidenmuller (n 42).

<sup>102</sup> National Consumer Credit Protection Act 2009 (Cth), ss 124B(1)(a), 133CB(1)(a); National Consumer Credit Protection Regulations 2010 (Cth) regs 28LCA, B(1)(c). Australian Treasury, *Financial System Inquiry* (n 86) 195.

<sup>103</sup> Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, art 6(1)(ea) requiring consumers to be informed where the price of goods was ‘targeted on the basis of automated decision making’.

<sup>104</sup> European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC’ (15 December 2020): <<https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>> accessed 12 July 2021.

<sup>105</sup> ACCC Digital Platforms Inquiry (n 18) 35 (Recommendation 16(b)), 463. See also Xing He and others, ‘When Text Simplification is not Enough: Could a Graph-Based Visualization Facilitate Consumers’ Comprehension of Dietary Supplement Information?’ (2021) 4(1) JAMIA Open <<https://doi.org/10.1093/jamiaopen/oaab026>> accessed 12 July 2021.

<sup>106</sup> California Consumer Privacy Act of 2018, 1.81.5 Cal Civil Code §§ 1798.135 (2018).

<sup>107</sup> See ‘Why Australian Businesses Should Care about the California Consumer Privacy Act’ (*Gilbert and Tobin*, 25 March 2020) <<https://www.gtlaw.com.au/insights/why-australian-businesses-should-care-about-california-consumer-privacy-act>> accessed 12 July 2021.

<sup>108</sup> Andrew Godwin, ‘Brave New World: Digital Disclosure of Financial Products and Services’ (2016) 11 *Capital Markets Law Journal* 442, 455.

the information that is relevant to their own needs,<sup>109</sup> and to use self-assessment tools to direct them to the information most likely to be pertinent to their circumstances.<sup>110</sup>

These ideas are attractive as placing control back with consumers. However, they are not absolute solutions. Warnings may not entirely overcome the issues around information overload, referred to earlier, which inclines consumers against reading information relevant but not central to their purchasing decisions.<sup>111</sup> There may also be distributive concerns about relying on private sector responses to consumer protection. Not all consumers will have access to the kinds of device or data that would make these kinds of digital solutions possible. It is also possible to envisage online traders being able to discriminate in their tech enabled ‘transparency’ responses between classes of high and low value consumers.<sup>112</sup> Therefore more substantive protections should be seen as complementing measures such as warnings, by setting the boundaries as to what is acceptable in dealings with consumers.

## **VI. PROHIBITIONS ON MISLEADING AND UNCONSCIONABLE/UNFAIR CONDUCT**

Outside law reform with a specific focus on algorithmically targeted advertising, we think that considerable work in complementing data privacy regimes may be done by the key ‘safety-net’ or general prohibitions that exist in most statutory consumer protection regimes, primarily on false or misleading conduct, and unconscionable or unfair conduct.<sup>113</sup> Drawing the line between more and less acceptable forms of targeted advertising, according to the degree to which information is distorted and the extent of manipulation of consumers’ situational vulnerabilities is precisely the task that the open textured nature of these kinds of prohibitions makes them capable of performing.<sup>114</sup> We suggest moreover, that a generous approach should be taken to the operation of these prohibitions in applying to algorithmically targeted advertising because, given their relatively recent development, consumers are themselves likely to be

---

<sup>109</sup> On layering information for artificial intelligence explainability, see Ronal Singh and others, ‘“LEx: A Framework for Operationalising Layers of AI Explanations’ (2021) <<https://arxiv.org/pdf/2104.09612.pdf>> accessed 12 July 2021.

<sup>110</sup> See also Jeannie Paterson, ‘Consumer Contracting in the Age of the Digital Natives’ (2011) 27 *Journal of Contract Law* 152.

<sup>111</sup> See above discussion at (n 83).

<sup>112</sup> See also Jane Winn, ‘The Secession of The Successful: The Rise of Amazon as Private Global Consumer Protection Regulator’ (2016) 58 *Arizona Law Review* 193, 196: comparing access to digital platforms dispute resolution to ‘gated communities’.

<sup>113</sup> See Competition and Consumer Act 2010 (Cth), sch 2 ss 18 (Australian Consumer Law) 20.

<sup>114</sup> Willis (n 89) 169 ff.

unaware of the scope of the reach and influence of these processes, and hence more vulnerable to their operation.

Egregious instances of manipulative or predatory targeted advertising might be met through prohibitions on unconscionable conduct<sup>115</sup> which apply to conduct that takes advantage of consumers' lack of bargaining power or a position of disadvantage, in a manner that is contrary to established community values.<sup>116</sup> For example, it may be unconscionable, and unfair, to target advertising to consumers who have been identified through their online conduct or digital profiles as experiencing a personal crisis or subject to some form of situational vulnerability, in order to promote expensive products superficially responding to those circumstances, but in reality offering little utility to them.<sup>117</sup> Prohibitions on unfair trading practices<sup>118</sup> might further extend to more subtle forms of manipulation through advertising that targets behavioural biases or emotional traits in order to produce sales.<sup>119</sup> Discriminatory strategies should also fall foul of these prohibitions, as well as being caught by anti-discrimination law.

More generally, we suggest that statutory prohibitions on misleading conduct<sup>120</sup> have as yet unrealised potential in responding to instances of targeted

<sup>115</sup> See Jeannie Marie Paterson, 'Regulating Consumer Contracts in ASEAN' in Luke Nottage and others (eds), *ASEAN Consumer Law Harmonisation and Cooperation: Achievements and Challenges* (Cambridge University Press 2019).

<sup>116</sup> See eg, *Jams 2 Pty Ltd v Stubbings* [2020] VSCA 200, [90] (Beach, Kyrrou, Hargrave JJA). Also compare Shiv Swaminathan, 'Coercion, Undue Influence and Unconscionability' in Mindy Chen-Wishart, Stefan Vogenauer and Hiroo Sono (eds), *Studies in the Contract Laws of Asia IV: Validity* (Oxford University Press: forthcoming).

<sup>117</sup> See eg, Matt Day, 'Amazon is Working on a Device That Can Read Human Emotions' (*Bloomberg*, 23 May 2019) <<https://www.bloomberg.com/news/articles/2019-05-23/amazon-is-working-on-a-wearable-device-that-reads-human-emotions>> accessed 12 July 2021; Emily Bell, 'How Ethical is it for Advertisers to Target Your Mood?' (*The Guardian*, 5 May 2019) <<https://www.theguardian.com/media/commentisfree/2019/may/05/how-ethical-is-it-for-advertisers-to-target-your-mood>> accessed 12 July 2021; Andrea Peterson, 'Watch Out, Ladies: Your Period-Tracking App Could Be Leaking Personal Data' (*The Washington Post*, 4 August 2016) <[https://www.washingtonpost.com/news/the-switch/wp/2016/08/03/how-your-period-tracking-app-could-leak-your-most-intimate-information/?utm\\_term=.2cfe585dd363](https://www.washingtonpost.com/news/the-switch/wp/2016/08/03/how-your-period-tracking-app-could-leak-your-most-intimate-information/?utm_term=.2cfe585dd363)> accessed 12 July 2021.

<sup>118</sup> Directive on Unfair Commercial Practices (Directive 2005/29/EC), art 5(1) (unfair commercial practices); Federal Trade Commission Act § 5(a), 15 U.S.C. § 45(a) (prohibiting '[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce'); Consumer Protection Act 2019 (India), ss 2(6), 20, 47, 58 (practices that are unfair and prejudicial to consumers' interests); Australian Consumer Law (n 113) s 21.

<sup>119</sup> See Willis (n 89) 176: arguing that courts should treat conduct that exploits consumers' pre-existing false beliefs as unfair'. See also Hirsch (n 75).

<sup>120</sup> Directive on Unfair Commercial Practices (Directive 2005/29/EC), art 6; Federal Trade Commission Act § 5(a), 15 USC § 45(a); Australian Consumer Law (n 113) s 18; Consumer Protection Act 2019 (India), ss 2(28), 21: outlining the power of the Central Authority to issue directions and penalties against false or misleading advertisements. See also discussion in

advertising that, although not reaching the threshold for an unfair practice, undermine consumer welfare by leveraging general consumer ignorance about online advertising practices. Promoting a ‘best price guarantee’ for a product may be misleading if different consumers are, for no good reason, presented with differential pricing.<sup>121</sup> The potential of the prohibition might further be pushed past blatantly untruthful strategies to respond to algorithmic advertising that lacks a baseline level of transparency. Prohibitions on misleading conduct may cover omissions as well as positive statements.<sup>122</sup> This is relevant in a context where consumers do not understand algorithmic advertising and have few mechanisms for identifying its application. In this context, it might therefore be possible to argue that targeted advertising or differential pricing is misleading if presented without clarification of its personalised character or that some options may not be visible to consumers through not being highlighted in search results or because that consumer is excluded from the target categories.

Of course, the differential and detrimental effects on individual consumers of targeted advertising may be difficult to prove in practice precisely because of the personalised and therefore variable nature of the advertising.<sup>123</sup> Another strategy, therefore, that may have wider effects in constraining digital targeted advertising is robust regulatory enforcement of privacy policies and notices. While consumers have limited capacity to police privacy policies, robust regulatory scrutiny of the veracity and transparency of such policies may go some way to constraining untrammelled and unauthorised data uses.<sup>124</sup>

Prohibitions on misleading conduct have already been used by regulators to sanction digital platforms that misled consumers over the scope of their data rights, such as by making assertions in contracts or privacy policies that are not true, subsequently departed from or confusing to consumers.<sup>125</sup> The Federal Trade Commission in the U.S. has fined Facebook for misrepresenting to consumers the extent to which they could exercise control over the collection and use of personal data.<sup>126</sup> The Australian Competition and Consumer

---

Vipan Kumar and Adya Sharma, ‘Strengthening Consumer Rights: The Advent of Consumer Protection Act, 2019’ (2019) 156 SEBI and Corporate Laws 7.

<sup>121</sup> See, eg, *Australian Competition and Consumer Commission v Trivago N.V.* [2020] FCA 16.

<sup>122</sup> Liability for misleading omissions is expressly acknowledged in the EU: Directive on Unfair Commercial Practices (Directive 2005/29/EC), art 7.

<sup>123</sup> See Willis (n 89) 165: noted the ‘overwhelming number of bespoke versions presents a looming impracticability problem for proving digital deception’.

<sup>124</sup> Compare E. Fosch-Villaronga, and M. Heldeweg, “‘Regulation, I Presume?’ said the Robot—Towards an Iterative Regulatory Process for Robot Governance’ (2018) 34(6) Computer Law & Security Review 1258.

<sup>125</sup> See Corones and Davis (n 24) 85-6.

<sup>126</sup> Federal Trade Commission, ‘FTC’s \$5 Billion Facebook Settlement: Record-Breaking and History-Making’ (24 July 2019) <[www.ftc.gov/news-events/blogs/business-blog/2019/07/](http://www.ftc.gov/news-events/blogs/business-blog/2019/07/)

Commission has commenced enforcement action against Google for misleading conduct in departing from the expectations created by its own privacy notices.<sup>127</sup> It has, moreover, been successful in a claim against Google for misleading conduct by reason of the very design of the information presented to consumers about the steps that might be taken to protect their data privacy through disabling location tracking.<sup>128</sup> In jurisdictions with statutory control over unfair contract terms,<sup>129</sup> those regimes might be used by regulators to curb some of the excesses of privacy and data collection statements, although as yet this remains an undeveloped jurisdiction.<sup>130</sup>

These possible responses require relevant stakeholders – consumer advocates, regulators, and particularly judges and decision makers – genuinely to understand the scope and consequences of new technologies from a consumer perspective. It is possible, as Tim Wu observes, that courts may be unwilling to acknowledge the harm that can be done through conduct that manages consumers’ ‘attention’, as opposed to directly inflicting physical or financial harm.<sup>131</sup> If algorithmic targeted advertising techniques are seen as a mere continuation of previous advertising practices, then courts in particular may be less sympathetic to the subtle influences these exert on consumer decision-making being worthy of a legal sanction.<sup>132</sup> This requires regulators to be scrupulously rigorous in creating their case theory and garnering evidence to establish that case. Thus, for example, in the recent Australian litigation against Google, the Australian Competition and Consumer Commission presented comprehensive evidence including screenshots, flow charts and different use scenarios of the choice architecture presented to consumers of android phones concerned to limit location tracking.<sup>133</sup>

---

fits-5-billion-facebooksettlement-record-breaking-history> accessed 12 July 2021.

<sup>127</sup> Australian Competition and Consumer Commission, ‘ACCC Alleges Google Misled Consumers about Expanded Use of Personal Data’ (*Media Release*, 27 July 2020) <<https://www.accc.gov.au/media-release/correction-acc-acc-alleges-google-misled-consumers-about-expanded-use-of-personal-data>> accessed 12 July 2021.

<sup>128</sup> *Australian Competition and Consumer Commission v Google LLC [No 2]*, [2021] FCA 367.

<sup>129</sup> See, eg, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; Australian Consumer Law (n 115) s 24; Consumer Protection Act 2019 (India), ss 2(6), 47, 58.

<sup>130</sup> Clifford and Paterson (n 24).

<sup>131</sup> Tim Wu, ‘Blind Spot: The Attention Economy and the Law’ (2019) 82 *Antitrust Law Journal* 771. See generally Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf Doubleday 2016).

<sup>132</sup> See Willis (n 89) 161: arguing judges may lack the ‘personal experience and social knowledge that will inform customers of [advertised] products’.

<sup>133</sup> Drawing on the work of the ACCC, *Digital Platforms Inquiry* and the Norwegian Consumer Council, ‘Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy’ (June 2018).



There is, moreover, a potential synergy that could be created between regulators in different countries in terms of enforcement and litigation strategies.<sup>134</sup> Technology evolves so quickly that law reform is always likely to lag behind market practices. Thus, it will be increasingly beholden on those interested in consumer protection to stay informed about these developments and to be prepared to push the application of traditional forms of legal protection to respond to new harms.

## VII. CONCLUSION

It is important in considering the regulation of any emerging technology to balance concerns about the use of the technology against the benefits it undoubtedly offers to consumers. However, we should not be so bedazzled by the newness of the technology that we fail to scrutinise its effect on core social values of consumer autonomy and welfare. Targeted advertising is the output of endemic consumer surveillance and holds the potential to constrain and reprioritise consumer choice, especially for marginalised groups. Better outcomes for consumers subject to algorithmically targeted advertising requires a change in the current and foreseeable future practices of digital platforms and the AdTech industry. Individual consumers cannot force this change, and indeed nor can individual regulators. What is needed therefore is a coordinated approach between the regulators responsible for privacy, competition and consumer protection, and between regulators in different jurisdictions.

As a way of contributing to this discussion, this article has canvassed a suite of possible regulatory tools for responding to these risks of harm from targeted digital advertising enabled by algorithmic processes. It has noted the regulatory focus on data rights protections, principally through consent processes, as well as the possible role for bans and disclosure mechanisms. It has also advocated for making better use of traditional consumer protection tools, namely on prohibition misleading, unconscionable and unfair conduct. The point is to recognise the need for a suite of regulatory responses to the impact of emerging technologies so as to both inform *and* protect consumer choice.

---

<sup>134</sup> See generally Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' (Report 108, vol 1, May 2008) 104: '[t]he ALRC's work [on privacy] not only led to domestic legislation but also *strongly influenced the international development of this field*' (emphasis added).