

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

**Computer Law
&
Security Review**



CookieConsumer: Tracking online behavioural advertising in Australia

Kate Mathews-Hunt *

School of Law, Bond University, Gold Coast, Australia

A B S T R A C T

Keywords:

Online behavioural advertising
Online advertising
Privacy
Misleading and deceptive conduct
Unconscionable conduct
Unfair contract terms
Australia

Online behavioural advertising (OBA) comes to consumers at a price. Often unknowingly, people deliver up commercially-valuable personal information as a condition of online user experience, functionality and access. Websites are increasingly tracking user behaviours for commercial purposes and social media derives its income largely from data collection and advertising targeted to the personal disclosures and behavioural attributes which are its data-production mainstay. In this context, consumers face a plethora of information collection practices, all designed to generate data analytics including inferential and predictive profiling to create a 'digital identity' for OBA purposes. In this subterranean exchange, consumers are economically redefined as data subjects and advertising targets; a reframing which is perhaps why the OBA industry faces a crisis in consumer concern, both as to privacy and trust.

This paper proposes that the regulatory control of OBA in Australia is in disarray. Consumer ignorance of online privacy management and OBA practices is demonstrable. Industry transparency, disclosure, consent processes and compliance practices are questionable. Regulator interest is minimal, industry self-regulation is weak and consumer technical ability and personal responsibility is a last fragile line of defence. Data breaches are ubiquitous in a crowded and poorly-audited supply chain, and entail significant adverse consumer consequences. Yet despite these serious concerns, Australian regulators are failing to respond to OBA issues, either through mandating greater industry disclosure or through regulatory action. The author seeks to expose these weaknesses in calling for consumer and privacy regulators to take more meaningful action to better protect consumers' interests online.

© 2015 Kate Mathews-Hunt. Published by Elsevier Ltd. All rights reserved.

Reader Note: This paper is a 'lawyer's look' at online behavioural advertising from a consumer perspective; it does not purport to offer a technical, industry-based or practical analysis of online advertising and the data analytics industries or any inherent privacy and consumer law issues. These technical issues are better dealt with by experts in these fields and the author does not pretend to have any computing expertise beyond that of an average Australian consumer. As such, technical or industry-related errors are intended to be avoided, but may be inevitable.

Acronyms pepper the advertising industry; please see **Appendix** for assistance in this regard. Please note that the Bibliography is available online as "supplementary material" on ScienceDirect.

Consistent with leading journalistic style guides and modern practice, the terms 'data' and 'social media' are generally used in the singular (e.g. data is. . .), rather than the arguably more correct Latin plural context (i.e. data are).

The phrase 'online behavioural advertising' is referred to in long form or as 'OBA' throughout for syntax reasons. Note also that 'consumer' is used in a colloquial sense to mean any Internet user, unless the context indicates otherwise, but does have a legal definition under the Australian Consumer Law which is cited in part 4.

* Faculty of Law, Law Building, Bond University, University Drive, Robina, Queensland 4229, Australia.

E-mail address: kmathews@bond.edu.au.

<http://dx.doi.org/10.1016/j.clsr.2015.12.006>

0267-3649/© 2015 Kate Mathews-Hunt. Published by Elsevier Ltd. All rights reserved.

1. Introduction

*Online behavioural advertising is safe and transparent. Advertisers don't know who you are. . .*¹

*. . . underscoring all the debates about online privacy, behavioural targeting and internet advertising is a hard, cold reality: content costs money. . .*²

*You can make money without being evil. . .*³

Big data, digital advertising⁴ and consumer trust⁵ are about to collide. And online behavioural advertising – the use of tracking technologies, profiling and interest-based analytics to target online advertisements to consumers – may well be the point of intersect. In today's "quicksilver technological environment"⁶, the online horizon seems ever-expanding and of limitless potential. Digital data is the new "currency"⁷ of the digital economy,⁸ and online advertising holds the keys to both expanding data collection and monetising its targeted use in

advertising.⁹ OBA is hailed as enabling a "continuing dialogue"¹⁰; it is a "social utility"¹¹ which in its personalisation, is "respectful to. . . cultural norms"¹² while creating a connected universe where ". . . ads work around people. . ."¹³ Even regulators declare "no interest"¹⁴ in jeopardising the OBA business model, asserting that it benefits consumers with on-time purchase opportunities and supports diverse unpaid¹⁵ online content and services.¹⁶ But for others, OBA is "fraught with ethical and reputational risk"¹⁷ and constantly walks a fine line to avoid illegal or unethical privacy intrusions and consumer law breach. Advertisers fear targeted consumers being "creeped out"¹⁸ given online tracking is akin to being shadowed all day every day by someone you don't know, who notes down your every move and then markets products of inferred interest back at you. As one OBA advertiser admits, for that reason, ". . . a lot of what we do is behind the scenes. . ."¹⁹

While consumers have flocked to the Internet and social media, and clearly enjoy fast and sophisticated access to almost infinite information and social networking environments, OBA comes to them with a price. Often unknowingly,²⁰ consumers

¹ Australian Digital Advertising Alliance, 'Five Top Tips' (undated, accessed 2 Apr 2015) <<http://www.youonlinechoices.com.au/five-top-tips>>.

² Louise Story, 'Bits' *The New York Times* (5 Nov 2007) cited in Joseph Turow, Jennifer King and Chris Jay Hoofnagle et al., 'Americans Reject Tailored Advertising and Three Activities that Enable It' (September 29, 2009, accessed 10 Apr 2015) [8] <<http://ssrn.com/abstract=1478214>> or <<http://dx.doi.org/10.2139/ssrn.1478214>>.

³ Google, 'Ten things we know to be true' (undated, accessed 20 Apr 2015) <<http://www.google.com/about/company/philosophy/>>.

⁴ The term 'marcomm' refers to marketing and advertising communication in the digital space. This reflects Australian Association of National Advertisers (AANA) guideline use: AANA, 'Best Practice Guideline: Responsible Advertising in the Digital Space' (26 Nov 2013, accessed 5 Dec 2014). <<http://aana.com.au/content/uploads/2014/05/AANA-Best-Practice-Guideline-Responsible-Marketing-Communications-in-the-Digital-Space.pdf>>.

⁵ John Still, "Blake Cahill of Philips: the Marketer needs to be Digital. It's part of the DNA" *The Guardian* (21 Jan 2015, accessed 27 Mar 2015) <<http://www.theguardian.com/media/2015/jan/21/blake-cahill-philips-digital-marketing>>.

⁶ Urs Gasser, 'Cloud Innovation and the Law: Issues, Approaches and Interplay' *Harvard University – Berkman Center for Internet and Society & University of St Gallen* (17 Mar 2014, accessed 20 June 2014) [2] Berkman Center Research Publication No. 2014-7 <<http://cyber.law.harvard.edu/research/cloudcomputing>>.

⁷ Maglena Kuneva, European Consumer Commissioner (March 2009) cited in ACMA, 'The cloud: services, computing and digital data – Emerging Issues in media and Communications' *Occasional Paper 3* (June 2013, accessed 11 July 2014) [1] <<http://www.acma.gov.au/-/media/Regulatory%20Frameworks/pdf/The%20cloud%20services%20computing%20and%20digital%20data%20Emerging%20Issues%20in%20media%20and%20communications.pdf>>.

⁸ The term 'digital economy' means "the network of economic and social activity that is enabled by information and communication technologies, such as the internet, mobile and sensor networks." Department of Broadband, Communications & the Digital Economy, Australia's Digital Economy: Future Directions (July 2009, accessed 21 Feb 2014) <http://www.dbcde.gov.au/digital_economy/what_is_the_digital_economy/australias_digital_economy_future_directions/final_report/australias_digital_economy#digitaleconomy>.

⁹ Natasha Singer, "Wrangling Over 'Do Not Track' " *The New York Times* (15 July 2013, accessed 25 Mar 2015) <http://bits.blogs.nytimes.com/2013/07/15/wrangling-over-do-not-track/?_r=0>.

¹⁰ Brad Jakeman, President of PepsiCo Global Beverages Group, cited in Sydney Ember & Emily Steel, 'The Pepsi Challenge is Returning, but this Time for the Social Media Generation' *The New York Times* (11 March 2015, accessed 15 Mar 2015) <<http://www.nytimes.com/2015/03/11/business/media/the-pepsi-challenge-is-returning-but-this-time-for-the-social-media-generation.html>>.

¹¹ David Sze, a venture capitalist at Greylock Partners and a Nextdoor board member, cited in Mike Isaac, 'Nextdoor Social Network Digs Deep Into Neighborhoods' *The New York Times* (3 Mar 2015, accessed 15 Mar 2015) <<http://www.nytimes.com/2015/03/04/technology/nextdoor-a-start-up-social-network-digs-deep-into-neighborhoods.html>>.

¹² Carla Hassan, PepsiCo's chief marketing officer for the Middle East and Africa region: Above n 10.

¹³ AAMIA, "11th Annual The Future of Digital Advertising online flyer" 28 April 2015, accessed 30 Mar 2015 <<https://aimia.worldsecuresystems.com/BookingRetrieve.aspx?ID=312855>>.

¹⁴ Jessica L. Rich, 'Beyond Cookies: Privacy Lessons for Online Advertising' *AdExchanger Industry Preview* 2015 (21 January 2015, accessed 17 Mar 2015) <https://www.ftc.gov/system/files/documents/public_statements/620061/150121beyondcookies.pdf>.

¹⁵ See the discussion as to 'free' in Part 4.3 below.

¹⁶ At the same time, the FTC has prosecuted a range of OBA offenders and engaged in significant online privacy and related research: Above n 14.

¹⁷ Twitter data strategy chief Chris Moody cited in Garside, Juliette, 'Twitter puts trillions of tweets up for data miners' *The Guardian* (19 Mar 2015, accessed 22 Mar 2015) <<http://www.theguardian.com/technology/2015/mar/18/twitter-puts-trillions-tweets-for-sale-data-miners>>.

¹⁸ Romney campaign official cited in Charles Duhig, 'Campaigns mine personal lives to get out vote' *The New York Times* (14 Oct 2012, accessed 15 Mar 2014) [1] <http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?_r=0>.

¹⁹ *Ibid*.

²⁰ That delivery may be voluntary – through website registration, user surveys, competitions and the like – or publicly disclosed through self-generated content such as LinkedIn profiles, tweets, Facebook posts or 'likes', but may also occur through potentially covert tracking technologies or analysis.

deliver up commercially-valuable personal information as a condition of user experience, functionality and access. Websites require registration and as studies show, almost universally embed cookies to enable user tracking.²¹ Social media derives its income largely from advertising targeted to the personal disclosures and behavioural attributes ('friends', 'likes', 'shares', etc) which are its data-production mainstay. In this context, consumers face a plethora of information collection²² practices, all designed to generate data analytics²³ including inferential and predictive²⁴ profiling to create a 'digital identity'²⁵ for OBA purposes. In this subterranean exchange, consumers are economically redefined as data subjects and advertising targets; a reframing which is perhaps why the OBA industry faces a crisis in consumer concern, both as to privacy and trust.

This paper puts the view that the regulatory control of online behavioural advertising in Australia is in disarray. Consumer ignorance of online privacy management and OBA practices is demonstrable. Industry transparency, disclosure, consent processes and compliance practices are questionable. Regulator interest is minimal, industry self-regulation is weak and consumer technical ability and personal responsibility are last fragile lines of defence.²⁶ Data breaches are ubiquitous in a crowded and poorly-audited supply chain, and entail significant adverse consumer consequences. Yet despite these serious issues, privacy and consumer regulators in Australia are failing to respond to online behavioural advertising issues. The result

is that consumers are caught in a gap; ill-equipped against significant information asymmetry²⁷ and technical complexity to responsibly understand or manage their online privacy, and yet, left by both industry and regulators to do just that.

Having briefly outlined the context, **part 2** of this paper briefly considers the commercial scale of the 'big data' and 'online advertising' industries, before re-defining OBA, and then discusses its prevalence and consumer awareness levels; while **part 3** exposes a range of privacy, contractual and consent-related OBA issues; **part 4** discusses privacy and consumer laws enlivened by recent international case examples; while **part 5** considers the Australian OBA *Guideline* by reference to best practice and other industry actions; and **part 6** looks beyond present regulatory approaches to ask what other options could be explored. **Part 7** then concludes that the industry has significant regulatory, risk management, technical innovation, contractual simplification and educative communication work to do to better engage consumer trust and potentially, improve attentional interest in online advertising.

Before delving into this increasingly complex online world, it is useful to gain a brief macro perspective of the digital ecosystem both in scale and as the context for OBA. It is also useful to try to better understand OBA itself, which is no simple task.

2. On big data, online advertising and defining online behavioural advertising

*People give out their data often without thinking about it. . . they have no idea that it will be sold to third parties.*²⁸

Data: Latin, dare, to give. . .

Online data mining provides the "new economic asset"²⁹ for a rapidly growing online behavioural advertising industry. It

²¹ Hoofnagle, Chris Jay & Nathan Good, 'The Web Privacy Census' (October 2012, accessed 10 Apr 2015) <<http://law.berkeley.edu/privacysensus.htm>>.

²² These might include registration requirements to access a website or a part thereof, or the exchange of such data as between a website and an advertiser or as between data brokers or different website owners, for example.

²³ Internationally, there are more than 6000 data centres managing international data flows: Executive Office of the President, 'Big Data Seizing Opportunities Preserving Values' (May 2014, accessed 25 Mar 2015) [49] <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

²⁴ Kate Crawford and Jason Schultz, 'Big data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' 55 BCL Rev 93 (2014, accessed 7 Apr 2015) [94] <<http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr>>.

²⁵ 'Digital identity' is defined as "the sum of all digitally-available data about an individual, irrespective of its validity, its form or its accessibility". It includes inherent and acquired characteristics, and individual preferences. 'Inherent' characteristics mean who a person is, where they come from and so on (e.g. address, medical record and purchase history). 'Acquired' characteristics mean a person's history – their story (e.g. address, medical and purchase history etc) and 'individual preferences' means what a person likes (e.g. hobbies, interests, favourite movies, music etc): Boston Consulting Group. 'The Value of our Digital Identity' *Liberty Global Policy Series* (Nov 2012, accessed 7 Apr 2015) [36] <<http://www.libertyglOBAI.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>>.

²⁶ Examples of consumer actions include using OBA opt-out tools, make informed choices as to the information provided online, adopting defensive browser settings and software, and genuinely reading and understanding privacy policies before accepting their content. Even then, consumers are still likely to experience some OBA, it is so ubiquitous.

²⁷ See Justin Malbon, 'Taking Fake Reviews Seriously', *Journal of Consumer Policy* (2012) 36(2):139–157. 'Information asymmetry' can prevent consumers in a market from making fully informed decisions, which in turn can result in market inefficiency, or at worst, failure. The term means where one party has more or better information than the other in a transaction. This may be harmful, as the party with information can take advantage of the other's lack of knowledge: Krishna Rupanagunta, Ajay Parasuraman and Sourav Banerjee, 'The information asymmetry problem: How decision science can help reduce market inefficiency.' *Informs* (Sept/Oct 2013, accessed 10 Apr 2015) <<http://www.analytics-magazine.org/septemberoctober-2013/874-behavioral-economics-bridging-the-information-gap>>.

²⁸ European Commission Vice-President Viviane Reding cited in Aleks Krotowski, 'Big Data age puts privacy in question as information becomes currency', *The Guardian* (22 April 2012, accessed 28 Mar 2015) <<http://www.theguardian.com/technology/2012/apr/22/big-data-privacy-information-currency>>.

²⁹ Saadati, Reyhaneh and Alec Christie, 'Big Data, Big issues? Is Australian Privacy Law Keeping Up?' *DLA Piper* (26 July 2013, accessed 25 Mar 2015) <https://www.dlapiper.com/en/australia/insights/publications/2013/07/big-data-big-issues-is-australian-privacy-law-ke_>.

is useful to put both big data³⁰ and the online advertising industry in figures, in order to better understand the nature of the digital ecosystem within which OBA flourishes.³¹

2.1. Online data and digital advertising – how BIG is ‘big’?

*Chasing data for the sake of data. You can get lost in it. . .*³²

Big data is “3 V”,³³ “near ubiquitous”³⁴ and is genuinely ‘big’. In 2013, over 4 zettabytes³⁵ of data was generated worldwide, including 500 million (+) photos and 288,000 hours of video uploaded online daily.³⁶ Google stores over a billion searches in the US alone – daily.³⁷ Over 90% of all world data has been gen-

erated since 2011,³⁸ created by an information ecosystem of web behaviour,³⁹ user generated content,⁴⁰ RFID data, location/geo data, environmental data,⁴¹ private/public organisational operational data and finally, statistics, census data and other research-based data.⁴² From a marketing and consumer analytics perspective, big data is a potential consumer-information “goldmine”.⁴³ So, too, are online advertising revenues. Globally, these topped US\$117 billion dollars in 2013, a 16% increase on the preceding year.⁴⁴ In 2014, US revenue topped \$42.8 billion and Australian revenue grew to \$4.6 billion.⁴⁵ By 2018, global online advertising revenue is projected to reach US\$252 billion.⁴⁶ All this money goes to few: the top ten corporate earners take 70% of all revenue,⁴⁷ led by the two largest OBA publisher/ad networks in the world – Google (\$45.06 billion)⁴⁸ and Facebook (\$17.23 billion).⁴⁹ These huge revenues are generated via websites, commercial online services, mobile devices, ad networks

³⁰ There is no one definition of big data, but it refers to the ability to “capture, aggregate and process an ever-growing volume, velocity and variety of data,” which in turn, presents in datasets which are “large, diverse, complex, longitudinal and/or distributed. . . generated from instruments, sensors, internet transactions, email video, click streams, and/or all other digital sources available today and into the future. . .”: Executive Office of the President, above n 23 [4].

³¹ The term ‘ecosystem’ is a buzzword in marketing and digital literature at the moment. It is used here metaphorically to refer to the entire, connected, digital consumer environment – the Internet and social media. A more technical (early) computer science definition is “. . . a distributed, adaptive, open socio-technical system with properties of self-organisation, scalability and sustainability inspired from natural ecosystems. . . informed by knowledge of natural ecosystems, especially for aspects related to competition and collaboration among diverse entities. . .”: see Gerard Briscoe & Philippe de Wild, “Digital Ecosystems: Evolving Service-Oriented Architectures”, *EU Digital Business Ecosystems Project* (2006, accessed 10 Apr 2015) <<http://arxiv.org/pdf/0712.4102v6.pdf>>; P Dini, N Rathbone, M Vidal, P Hernandez, P Ferronato, G Briscoe and S Hendryx. ‘The digital ecosystems research vision: 2010 and beyond’, *European Commission* (2005, accessed 9 Apr 2015) <http://www.digital-ecosystems.org/events/2005.05/de_position_paper_vf.pdf>.

³² Above n 5.

³³ “3V” means data that is large in volume, diverse in variety or moving with extreme velocity: Executive Office of the President, above n 23 [4].

³⁴ Executive Office of the President, above n 23 [4]. The full quote is: “*The declining cost of collection, storage and processing of data, combined with new sources of data like sensors, cameras, geospatial and other observational technologies, means that we live in a world of near-ubiquitous data collection. . .*”

³⁵ A zettabyte is one sextillion bytes; that is equivalent to every person in the US taking a photo every second for a month or every letter in the entire novel *War and Peace* multiplied 323 trillion times: Executive Office of the President, above n 23 [2].

³⁶ Executive Office of the President, above n 23 [2]. Another estimate suggests 2.5 exabytes globally per day which annually equates to filling 30,000 times the US Libraries of Congress: TechAmerica ‘Mining the Big Data Goldmine’, *Time News Group Advertising Feature* (2013, accessed 10 Apr 2015) <http://www.timeincnewsgrupecustompub.com/sections/120409_CloudComputing.pdf>.

³⁷ Kenneth Cukier cited in *EuroActiv.com*, ‘Economist editor: Big data is a goldmine for companies’ (6 May 2014, accessed 10 Apr 2015) <<http://www.euroactiv.com/sections/eskills-growth/economist-editor-big-data-goldmine-companies-301933>>.

³⁸ SINTEF. “Big Data, for better or worse: 90% of world’s data generated over last two years.” *ScienceDaily*, 22 May 2013. <www.sciencedaily.com/releases/2013/05/130522085217.htm>.

³⁹ This means over 5 billion web pages which yield statistics, traffic, search engine data etc.

⁴⁰ In the form of social media content in its many forms together with voice, text and image-based mobile communications and email.

⁴¹ The ADMA Report predicts that this will become a “major growth driver from wearables such as Apple bracelets, Google glasses, etc”.: Association for Data-driven Marketing and Advertising (ADMA), ‘Best Practice Guideline: Big Data’ (2013, accessed 28 Mar 2015) [6] <<http://www.adma.com.au/assets/Uploads/Downloads/Big-Data-Best-Practice-Guidelines.pdf>>.

⁴² ADMA, above n 41 [5].

⁴³ Above n 37.

⁴⁴ IAB, ‘IAB advertising revenue report 2013 full year results’ (April 2014, accessed 4 Apr 2015):4 <http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2013.pdf>. In the US alone, online advertising spend topped \$42.8 billion in 2014.

⁴⁵ Mobile revenue was \$762 million (up 118%) and video was \$237 million (up 52%). IAB, ‘Mobile and video advertising continue to surge according to IAB Online Advertising Expenditure Report’, *Press Release* (26 Feb 2015, accessed 25 Mar 2015) <<http://www.iabaustralia.com.au/news-and-updates/iab-press-releases/item/1852-mobile-and-video-advertising-continue-to-surge-according-to-iab-online-advertising-expenditure-report>>.

⁴⁶ Statista, ‘Digital advertising spending worldwide from 2012 to 2018 (in billion U.S. dollars)’ (2015, accessed 7 Apr 2015) <<http://www.statista.com/statistics/237974/online-advertising-spending-worldwide/>>.

⁴⁷ Above n 44. The top ten online advertising companies earn over 70% of all online ad revenue: this figure has remained relatively stable for the decade to 2013 end, ranging from 69 to 74%.

⁴⁸ Total Google revenue was \$66 billion. Statista, ‘Advertising revenue of Google sites from 2001 to 2014 (in billion U.S. dollars)’ (2015, accessed 7 Apr 2015) <<http://www.statista.com/statistics/266242/advertising-revenue-of-google-sites/>>.

⁴⁹ Statista, ‘Facebook’s advertising revenue worldwide from 2012 to 2016 (in billion U.S. dollars)’ (2015, accessed 7 Apr 2015) <<http://www.statista.com/statistics/271258/facebook-advertising-revenue-worldwide/>>. Microsoft’s Bing was third with \$3.2 billion: Statista, ‘Facts on the Online Advertising Industry in the U.S.’ (2015, accessed 8 Apr 2015) <<http://www.statista.com/topics/1176/online-advertising/>>.

and exchanges, email providers and companies selling online advertising,⁵⁰ and include formats as diverse as search (41%),⁵¹ display-related ads⁵² (30%) and mobile (17%).⁵³ Australia is now the third largest⁵⁴ online advertising nation in the world and digital categories are seen as “comparable”⁵⁵ investments to offline advertising formats.⁵⁶

Big data and big advertising revenues suggest that consumers are being exposed to increasing volumes of online advertising, which carries with it an increasing exposure to OBA and data mining – as does increasing consumer presence online. In 2014, around 99% of Australians have Internet access⁵⁷ and in January 2015 alone, over 18 million consumers were actively surfing online, viewing some 28 billion webpages, over

some 39 million minutes.⁵⁸ Social media use reveals similar figures: 95%⁵⁹ of Australians⁶⁰ are among the 1.23 billion global users of Facebook⁶¹: 9 million use the platform daily, contributing to its 3.4 trillion tracked ‘likes’⁶² and to the mass of ‘personal information’ shared every second around the world.⁶³

It seems reasonable to conclude that, given increasing consumer use of the Internet and social media, and given the correlation between extensive online advertising and online tracking, Australians are being exposed to a significant amount of both – on a daily basis.

2.2. So what is online behavioural advertising?

There is no internationally-agreed legal or industry definition of OBA. The 2011 *Australian Best Practice Guideline for Online Behavioural Advertising*⁶⁴ (OBA Guideline) provides as follows:

⁵⁰ Statista, ‘Facts’ Ibid: 3.

⁵¹ Note that online search and mobile search are in separate categories – so it is clearly the leading format, and represents most of the next two formats combined. However, this may change as mobile revenues are gaining greater share quickly, growing from 5% (2011) to 12% (2012) to 17% (2013).

⁵² ‘Display-related’ ads are defined to include display/banner ads (19%), digital video (7%), rich media which refer to ads which incorporate streaming interactivity (3%) and sponsorship (2%), where percentages are of total online ad annual revenue: Statista, ‘Facts’ above n 49 [12]. For detailed definitions of each category, see IAB, above n 44:23–24.

⁵³ Mobile formats are the fastest growth segment, increasing 12% in less than two years. Others are classifieds (6%) and ad lead generation (4%).

⁵⁴ The three top online ad spending countries per capita are Norway (\$209), the US (\$201) and Australia (\$191): Felix Richter, ‘Norway tops the US in Digital Ad Spend per person’, *eMarketer* (25 Sept 2015, accessed 7 Apr 2015) <<http://www.statista.com/chart/1493/digital-ad-spend-per-person/>>.

⁵⁵ Campaign Brief, ‘IAB Online Advertising Expenditure Report: Mobile + video advertising continues to surge’ (26 Feb 2015, accessed 15 Apr 2015) <<http://www.campaignbrief.com/2015/02/iab-online-advertising-expendi.html>> citing Alice Manners, IAB (Australia) CEO who says that digital ad categories have just started aligning to market share.

⁵⁶ For the first time in 2013, Internet advertising revenues exceeded those of television in the US: Richter above n 54. Note that online ad spend does not correlate to online purchasing behaviours: retail advertising remains the highest spend of any product or service on the Internet but online sales are relatively low: IAB & PwC, ‘IAB internet advertising revenue report, 2012 full year results’ (April 2013, accessed 31 March 2014) [16] <http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2012_rev.pdf>. Online sales figures are 6.4% in Australia – which means that online sales remain a relatively low proportion of retail revenue overall: NAB Group Economics, ‘Online Retail Sales Index: In-depth & Special Report – January 2014’, *National Australia Bank* (5 March 2014, accessed 9 April 2014) <<http://business.nab.com.au/online-retail-sales-index-indepth-special-report-january-2014-5869/>>. For a discussion of this in a different context, see Kate Mathews Hunt, ‘Gaming the System: Fake online reviews v. consumer law’, *Computer Law & Security Review* 31(1) (2015) 1–25.

⁵⁷ Sensis, ‘Yellow Social Media Report’ (May 2015, accessed 29 Mar 2015) [11] <<https://www.sensis.com.au/learn/yellow-social-media-report-2014/>>. While the survey figure may be a little high, ABS statistics show that 12.7 million Australian Internet subscribers by 2014 end: Australian Bureau of Statistics, *Internet Activity – Dec 2014* <<http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/>>.

⁵⁸ In January 2015, Google had a total active reach of almost 84%: Nielsen, ‘The Australian Online Landscape Review’ (Jan 2015, accessed 15 Mar 2015) [4] <http://www.iabaustralia.com.au/uploads/uploads/2015-02/1424642400_d9371e6886fcee7b6731413517a15ecb.pdf>.

⁵⁹ Sensis, above n 57: 17. Other social media usage figures were LinkedIn (24%), Instagram (21%), Twitter (19%), Google+ (19%), Snapchat (16%), Pinterest (12%) and Tumblr (6%). The trend suggests that Facebook use is declining slightly (down 2%) over the past two years while others have grown: LinkedIn (+8%), Instagram (+5%), Twitter (+5%) and Google+ (+11%).

⁶⁰ In January 2015 alone, Facebook has almost 11 million active users, 2,058,334 page views, a 60% active reach and an average of 7 hours 42 minutes per user for the month: Nielsen, above n 58: 4.

⁶¹ Monique Ross, ‘Facebook turns 10: the world’s largest social network in numbers’ *ABC News* (4 Feb 2014, accessed 2 Apr 2015) <<http://www.abc.net.au/news/2014-02-04/facebook-turns-10-the-social-network-in-numbers/5237128>>.

⁶² The ‘like’ function was introduced in 2009.

⁶³ There may be a demographic shift in users according to a 2014 survey which indicated that 3 million US teenagers (25.3% decrease) had ‘left’ Facebook 2011–2014 whereas the greatest growth segment were 55+ (with an 80.4% increase). It is notable that a range of other teen-popular platforms emerged within this time – Snapchat and Instagram for example, so youth exposure to social media advertising may fluctuate a little within this time until advertising is established on these platforms: DJ Saul ‘3 million teens leave Facebook in three years: the demographic report’ (15 Jan 2014, accessed 3 Apr 2015) <<http://istrategylabs.com/2014/01/3-million-teens-leave-facebook-in-3-years-the-2014-facebook-demographic-report/>>.

⁶⁴ Australian Digital Advertising Alliance (ADAA) ‘Australian Best Practice Guideline for Online Behavioural Advertising’ (Mar 2011, accessed 3 Apr 2015) <<http://www.communicationscouncil.org.au/public/content/ViewCategory.aspx?id=931>>. The ADAA consists of Australian Association of National Advertisers (AANA), Australian Direct Marketing Association (ADMA), Interactive Advertising Board (IAB), Internet Industry Association, Media Federation of Australia (MFA) and The Communications Council. Note that by 26 April 2015, the IAB link <<http://www.iabaustralia.com.au/guidelines-and-best-practice/privacy/item/23-adaa-s-australian-best-practice-guideline-for-online-behavioural-advertising>> to this Guideline was disabled.

Online Behavioural Advertising . . . Means the collection and use of data on web browsing activity of an internet-enabled device, which allows the device to be added to one or more pre-defined interest categories, to serve advertising based on those . . . categories. No personal information is collected or used for OBA. . . [it] does not include Contextual Advertising (based on the subject matter of the web page on which the advertisement is served), customer profile advertising (based on the personal information of the individual user) or Geo-targeting.

From a legal and consumer perspective this definition is problematic. It defines OBA restrictively by excluding 'personal information' covered under the Privacy Act 1988 (Cth), 'First Party OBA' and each of the increasingly large categories of contextual, profile and geo-targeted⁶⁵ advertising. This means that the Guideline does not cover OBA drawn from 'information or an opinion' about either an identified or reasonably identifiable individual; it does not cover advertising targeted based upon the page being viewed (for example, a google search) or based on the browsing history on that page alone⁶⁶ (which is relatively uncontroversial),⁶⁷ and it does not cover content served specific to the geographic location tagged to user IP address. The definitions also exclude as 'First Party OBA'⁶⁸ any OBA

Data⁶⁹ based on the browsing history of a device on a website, or that of a Related or Associated Entity.⁷⁰ This means that browsing history can be shared from or with any Related Company⁷¹ plus any entity which ". . . a Web User would be reasonably likely to regard as closely related by product, branding or some other apparent way. . ." ⁷² There is no guidance as to what 'closely related' means in this context,⁷³ and it is also questionable how and by whom an average web user's views are to be discerned.⁷⁴ In summary, the OBA Guideline only applies to Third Party OBA⁷⁵ ". . . which occurs when (non-personally identifiable) browsing behaviour is used to deliver advertisements across unrelated Websites."⁷⁶ It is difficult not to regard the definition as deliberately framed to minimise the perceived risk of OBA, to inform its detractors that 'personal information' is not used and to artificially restrict its meanings to reflect industry perceptions of consumer tolerance.⁷⁷

⁶⁵ 'Geo-targeting' is defined to mean the 'serving of content or advertising specific to the geographic location of the server through which the IP address is served'. The US Future of Privacy Forum has a 2013 code applicable to mobile analytics companies providing services to retailers, but Australia has no equivalent: Future of Privacy Forum, 'Mobile Location Analytics Code of Conduct' (2012, accessed 25 Mar 2015) <<http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf>>; see also the US Digital Advertising Alliance, 'Application of the Self-Regulatory principles to the Mobile Environment' (July 2013, accessed 2 Apr 2015) <<http://www.digitaladvertisingalliance.org/content.aspx?page=principle>>. Again, Australia has not adopted an equivalent.

⁶⁶ Note though that 'First Party OBA' as defined extends to include any web pages belonging to an 'Associated' or 'Related Entity', which is arguably controversial in effect and is discussed below.

⁶⁷ The industry maintains that the use of tracking cookies to record user preferences for individual websites is "well established and generally accepted" by consumers and so excludes first party OBA and 'contextual advertising' from the Guideline, but has greatly expanded the definition as indicated: above n 64: 2. The 2009 FTC Report definition reveals this: OBA is behavioural advertising by and at a single website and "contextual advertising" is defined as advertising based upon a user's current visit to a single web site or single search query involving no data retention as to browsing history other than that necessary to deliver the search or ad: Federal Trade Commission (FTC), 'Self-Regulatory Principles for Online Behavioural Advertising' (Feb 2009, accessed 15 Mar 2015) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>>.

⁶⁸ 'Contextual advertising' is defined in the Guideline as "advertising that is targeted based on the content of the web page being viewed, but does not include advertising targeted through the use of third party OBA". For example, if a web user goes to a travel web page, he/she is served an advertisement for luggage or travel insurance. Contextual advertising can also occur for searches through search engines (see the Google Adwords case discussed below for an example: Above n 64: 5.

⁶⁹ The means "data on web browsing activity of an internet-enabled device which allows the device to be added to one or more pre-defined interest categories": Above n 64: 6.

⁷⁰ "First Party OBA is OBA served to an Internet-enabled device on a Website based on the browsing history of the device on that Website and Associated Website or Related Entity Website": Above n 64: 5.

⁷¹ As defined under section 50AAA of the Corporations Act (Cth) 2001: Above n 64: 5.

⁷² Above n 64: 6.

⁷³ For example, is it intended to have some loose correlation to the 'related' company concept or is an entirely independent issue?

⁷⁴ It is difficult not to conclude the clause to be so potentially wide that (for example) Dell can engage in OBA to a consumer based upon their browsing history visit to Apple's website, without the Guideline or its provisions as to consent taking effect. Further, complaints management and dispute resolution processes are unclear under the Guideline. Principle D. Handling Consumer Complaints requires signatories to use independent, ADR mechanisms such as independent Complaint Handling Bodies (a body which has nominated itself to handle OBA complaints: Above n 64:5). There are no publicly available reports as to complaints under the Guideline. Recourse to the youronlinechoices.com.au website suggests that disputes are resolved directly with the signatory, subject to ADAA involvement if it is not resolved. There are no rules or time frames or any clear indication of how this process might work in practice. Given these are not in the Guideline, they constitute a public representation of the ADAA but may not bind a Guideline signatory in any case.

⁷⁵ "Third Party OBA" means OBA "served on an Internet-enabled device on a Website based on the browsing history of the device on Websites that are not Associated Websites or Related Websites": Above n 64: 7. All capitalised terms are defined.

⁷⁶ Above n 64: 2.

⁷⁷ "There is an industry-maintained 'dividing line' between first party OBA and third party OBA, personally identifiable information and anonymous data which although not personally identifiable in isolation, could become so readily. . ." (e.g. the combining of website registration information with a related "click-stream"): D. Reed Freeman, Julie O'Neill and Nicholas Datlowe, 'Online Behavioural Advertising: Trends and Developments' Morrison & Foerster LLP (2012, accessed 4 Apr 2015) <<http://media.mofo.com/files/Uploads/Images/110624-Online-Behavioral-Advertising-PLI.pdf>>.

This paper does not limit its inquiry to the industry definition for a range of reasons. The dominant consumer issue surrounding OBA is the use or potential use of personal data, and the use of surveillance-style tracking technologies without informed, express consumer consent to create such data – and the associated profiling and targeting of consumers. It is artificial to limit the definition to preclude that discussion. Secondly, the definition is also designed to circumvent prior informed consent⁷⁸; absent ‘explicit consent’, it allows OBA through information provision via links to web notices which most consumers would never notice, much less click.⁷⁹ Thirdly, there is significant practical evidence that OBA is implicated⁸⁰ in the breach of consumers’ personal information – so the Guideline should, like those in the US for example,⁸¹ guide industry privacy law responses too.⁸² Finally, from a consumer perspective, privacy law enforcement in Australia has to date, failed to either examine or capture the sorts of practices which have been exposed internationally. Industry bona fides would better be represented by a Guideline which constitutes a comprehensive self-regulatory instrument for OBA rather than one designed to avoid the big issues.

This paper considers OBA as the sum of its parts in a big data context; that is *the practice of tracking the online activities of a consumer for data-gathering and analytic purposes, in order to deliver online advertising tailored to that consumer’s inferred*⁸³ interests.⁸⁴ It does not include ‘first party’ advertising (OBA by and at one single site) or ‘contextual advertising’ (concurrent OBA based on one current visit to a single web page or a single search, where no data is retained beyond that required for the purpose of that visit or search).

⁷⁸ This issue is discussed further under part 3.3.

⁷⁹ Principle II requires notice on the third party OBA entity’s website plus either explicit consent OR an in-ad link to the notice or a notice on the webpage on which the ad appears linked to an industry-developed website.

⁸⁰ This includes any supply chain issues; for example, information may be anonymous in one entity’s hands, but data sharing practices may mean that ‘personal information’ may become readily ‘identifiable’ in the hands of another industry participant with a second strand of data.

⁸¹ Digital Advertising Alliance (US), ‘DAA Self-Regulatory Principles for Online Behavioral Advertising’ (July 2009, accessed 17 Mar 2015) [25] <<http://www.digitaladvertisingalliance.org/content.aspx?page=principle>> <<http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>>.

⁸² Note the OBA Guideline does refer to sensitive market segments and children in Principle V, so it makes little sense to touch on Privacy Act issues there as to “sensitive information” but not with respect to other forms of “personal information”.

⁸³ The word “perceived” is omitted in the OBA Guideline. Note that the fact a consumer visits a particular website or researches a particular area may not evidence a purchase-related ‘interest’ in that subject matter. For example, an anti-cruise ship campaigner may research cruise ships, but may not wish to ‘buy’ a cruise.

⁸⁴ Such a broad definition better fits the FTC (2009) description of OBA, that is, “. . . the tracking of a consumer’s activities online – including the searches the consumer has conducted, the web pages visited and the content viewed – in order to deliver advertising targeted to the individual consumer’s interests”: FTC, above n 67.

This is perhaps controversial,⁸⁵ but OBA needs accurate scoping before it can be properly assessed, and this cannot be done in piecemeal; either by adopting a small target definition or by a Guideline which fails to comprehensively address the issue. How OBA works – and its escalating prevalence are considered next.

2.3. OBA prevalence, practices, risks – and the cookie monster

*Looking under the hood of the tracking technology and practices used by companies is critical to examining the role this data plays in our economy and our private lives. . .*⁸⁶

A 2012 UC Berkeley study⁸⁷ revealed that online tracking was “growing at a startling pace” and projected a doubling in the amount of online tracking within two years.⁸⁸ The study also showed that 85% of the 100 most popular US websites embedded third party cookies on users’ browsers and concluded that “. . .online tracking is growing in both pervasiveness and sophistication.”⁸⁹

In Australia, OBA is dominated by *ad publishing networks* such as Google,⁹⁰ Yahoo, News Digital and Fairfax – and in social media,

⁸⁵ In the US, the self-regulatory principles refer to “. . . the collection of data from a particular computer or device regarding Web viewing behaviours over time and across non-Affiliate sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviours. OBA does not include the activities of First Parties, Ad Delivery or Ad reporting, or contextual advertising (i.e. advertising based on the content of the Web page being visited, a consumer’s current visit to a Web page, or a search query). . .”: DAA, above n 81: 10–11.

⁸⁶ Ashkan Soltani, ‘Wall Street Journal’s What they Know Series’, Blog (accessed 15 Apr 2015) <<http://ashkansoltani.org/work/what-they-know/>>.

⁸⁷ Hoofnagle, above n 21.

⁸⁸ Hoofnagle, above n 21. The study showed that numbers of third party tracking cookies on the 100 most popular websites increased 11% in just six months and that Google and Facebook were responsible for 20.28% and 18.84% of all tracking requests on the web. The study compared May: October and showed an increase in first party cookies from 932: 992, third party cookies 4963: 5493 and a final total of 6495 cookies across 100 sites. All sites had cookies, 85% of which were set by third party hosts and only 5 sites (for example, Wikipedia) had no third party cookies at all. The study also noted a diminution in flash cookies to HTML5 storage which was perhaps explained by the fact that iOS technologies do not support the former. See the discussion in Sarah A Downey, “Our second web privacy census with UC Berkeley shows online tracking is at an all-time high” Abine blog (8 Nov 2012, accessed 28 Mar 2015) <<http://www.abine.com/blog/2012/abine-privacy-study-with-uc-berkeley/>>.

⁸⁹ Hoofnagle, above n 87: 111. A crawl of the top 1000 website homepages revealed 65,381 cookies of which 56,723 were third party (OBA implicated) cookies. Ninety-eight percent of all sites had cookies and Google had a presence on 73% of all sites.

⁹⁰ Google can offer potential advertisers access to “YouTube, Google properties such as Google Finance, Gmail, Google Maps, Blogger, as well as over one million Web, video, gaming, and mobile display partners. . .”: <<https://www.google.com.au/ads/displaynetwork/find-your-audience/partner-sites.html>>.

Facebook is dominant. The OBA industry⁹¹ consists of *publisher* website owners who sell website ad space; *advertising network providers* who collaborate with other networks⁹² and connect publishers with advertisers and finally, the *advertisers* who contract ad networks to place their online advertisements.⁹³ OBA works through the *publisher* offering visitor IP address details⁹⁴ to *ad network(s)* such as Google's AdSense, which optimise ad placement through consumer targeting technology and database information. Ad networks target advertising by placing cookies and related tracking technologies⁹⁵ on a user's browser⁹⁶ which invisibly track that user's Internet activity over time on a device, recording and cross-referencing data against that already held by the network and its broadly-defined related entities/partners.⁹⁷ This enables interest categorisation of, and ad targeting to, users visiting network websites, through online display advertising and website user customisation. The whole process operates via an ad network bidding system⁹⁸ – and user identification, profile retrieval, locating a targeted ad and display to the user – occurs in less than a half of one second.⁹⁹ It targets a web user for potentially millions of website advertisers and their ad networks,¹⁰⁰ almost instantaneously.

⁹¹ Examples of industry participants include data brokers, advertisers, ad agencies, ad networks, search engines, website operators/publishers, Internet service providers, social media platforms and app providers.

⁹² The FTC states data are collected about users as they unknowingly travel across different websites in the same ad network. "An individual network may include hundreds or thousands of different, unrelated websites and an individual website may belong to multiple networks. . .": FTC: above n 67. For example, a recent US case involved an ad network with 45,000 websites: *In the Matter of Epic Marketplace Inc. and Epic Media Group LLC*. Docket No. C4389, USA Federal Trade Commission, Complaint 13 March 2013, accessed 18 Feb 2015 <<http://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf>>.

⁹³ EU, 'Opinion 2/2010 on online behavioral advertising' Article 29 Data Protection Working Party (22 June 2010, accessed 9 Apr 2015) [5] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>.

⁹⁴ *Ibid*: 23.

⁹⁵ Other technologies use IP addresses and browser signatures.

⁹⁶ Users may use multiple browsers in which case their cookie configuration will reflect the ad networks visited via websites on those browsers. Examples of browsers include Internet Explorer, Mozilla, Google Chrome, Safari and so on. Note also that cookies are attached to a specific *device* which means that user tracking cookies on a user's laptop will be different to those on their desktop computer, for example. This means any 'opt out' of OBA – whether by website system or through the use of browser settings – must be repeated for each device a user may employ.

⁹⁷ ADMA, above n 41: 13.

⁹⁸ The primary ad network puts the website ad space up for bidding among ad networks and takes the best offer: EU Opinion, above n 93: 5 [fn 6].

⁹⁹ ADMA, above n 41: 13.

¹⁰⁰ "An individual network may include hundreds or thousands of different, unrelated websites and an individual website may belong to multiple networks. . .": FTC, above n 67.

OBA is enabled by the "humble" cookie¹⁰¹ (regular, 'flash',¹⁰² super¹⁰³ or zombie cookies)¹⁰⁴ which is both one of the "great enabling technologies" and "one of the most invasive tracking instruments"¹⁰⁵ of the digital age.¹⁰⁶ Other tracking technologies include web bugs (beacons, pixel tags, action tags, web tags, clear GIFs, etc)¹⁰⁷ and practices such as IP address monitoring,¹⁰⁸

¹⁰¹ Or amusingly, the "internet's favourite moustachioed villain": Kevin Partner, 'How to Stop online advertisers following you', PC & Tech Authority (19 April 2013, accessed 11 Apr 2015) <<http://www.pcauthority.com.au/Feature/341456/how-to-stop-online-advertisers-following-you.aspx>>. In the EU regulations, the word 'cookie' includes all similar information-storing technologies such as local shared objects (flash cookies, web bugs or beacons) Regulations: 4.

¹⁰² "Flash" cookies are 'saved' as a "local shared object" on an individual's device and can save information and preferences persistently. They are harder to delete and have been used to overcome consumer privacy attempts. There is a suggestion that they are less useful given they are incompatible with iOS, such that their use may decline: Turow, above n 2.

¹⁰³ Super cookies use new browser storage locations which are larger and more flexible, enabling more information storage. Consumers generally do not realise these exist: Office of the Privacy Commissioner (Canada), 'Cookies Following the Crumbs: FAQs' <https://www.priv.gc.ca/resource/fs-fi/02_05_d_49_01_e.pdf>.

¹⁰⁴ *Ibid*.

¹⁰⁵ Ronald Leenes and Eleni Kosta, 'Taming the cookie monster with Dutch law – A tale of regulatory failure', *Computer Law & Security Review* XXX (2015, accessed 3 Apr 2015) [1–19] <<http://dx.org/10.1016/j.clsr.2015.01.004>>.

¹⁰⁶ Recent industry concerns have emerged as to the limited future of cookies. The IAB (US) reports that the "costly, persistent and high volume deployment" of cookies is resulting in costs such as excessive network traffic, 'internet bloat' and consumer/publisher anxiety. As such, cookie technology has been "pushed beyond its useful and intended purpose." The IAB report the challenge is to create a replacement technology that meets the criteria to 'remember' user, device and software information over time and thereby enable more personalised web content, services and user preferences, and which is capable of meeting the growing diversity of Internet-connected devices consistent with extant privacy, consumer and industry needs. The IAB working group concluded that at present, there is no solution available which meets stakeholder criteria, and which is available as an open standard: IAB (US), 'Privacy and Tracking in a Post Cookie World' *White Paper* (Jan 2014, accessed 9 Apr 2015) [15] <http://www.iabaustralia.com.au/uploads/uploads/2014-11/1415289600_3ee3de01b67c04945704bce1e7964095.pdf>.

¹⁰⁷ Web Bugs (and the bracketed synonyms) are small and invisible non-cookie image files which may be included in an email or on a web page. When a consumer visits that webpage, the image is downloaded and this enables tracking of personal information, such as IP Address, location, the page being viewed and so on: Above n 103.

¹⁰⁸ An Internet protocol or 'IP' address refers to the numerical number assigned to a device which websites visited can track over time, particularly if the address is static. Catherine Tucker, "The Economics Value of Online Customer Data", *OECD Conference: The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines* [3] (2010, accessed 7 Apr 2015) <<http://www.oecd.org/sti/ieconomy/46968839.pdf>>.

click stream data analysis,¹⁰⁹ deep packet inspection,¹¹⁰ single universe identifier tracking,¹¹¹ device fingerprinting,¹¹² history sniffing and mobile location analytics. Cookies are a “short, alphanumeric text” string which is stored on a user’s browser and are classified by lifespan¹¹³ or domain (first¹¹⁴ or third party). Third party (OBA) cookies are those placed by an ad network when the user first visits a network website and capture a user’s browsing profile on that device over time, which is then used for targeted advertising.¹¹⁵ But *ad networks* use other data too and that, combined with tracking over time, is where the serious risks of personal information uses and abuses accelerate. This issue, and legal concerns as to consumer consent online and industry disclosure online are discussed in **part 3** below.

The oft-repeated industry arguments to justify OBA practices are that advertising subsidises free online content, benefits consumers through enabling personalised online advertising of “value, relevance and connection”,¹¹⁶ reduces obtrusive advertising and benefits advertisers through increased ad spend efficiency.¹¹⁷ In reality, OBA is the matching of inferred¹¹⁸ personal interests, captured online behaviours and likely buying habits linked to one device. Whether or not

this enhances user experience or narrows consumer options as to viewing the full variety of Internet advertising is an interesting economic question,¹¹⁹ but the industry seem convinced that targeted advertising works better.¹²⁰ From a consumer’s viewpoint, OBA presents serious questions as to disclosure and trust, consent, unfair contractual terms and data breach or misuse.

These issues are considered next.

3. Online behavioural advertising has its ‘issues’

*As you browse we’re able to categorise all of your internet actions. . .*¹²¹

This part considers some increasingly significant consumer issues which challenge the legitimacy and future of OBA in its present form. It also initiates the discussion as to why this internationally¹²² contentious area of online marketing

¹⁰⁹ A clickstream is a list of all website pages viewed by a visitor – the ‘succession of mouse clicks’ which form browsing history: Opentracker, ‘Click stream or click data analysis’ <<http://www.opentracker.net/article/clickstream-or-clickpath-analysis>>.

¹¹⁰ This occurs where an Internet Service Provider (ISP) inspects for content data packets sent between a user and the websites visited. It enables a universal picture of client’s browsing behaviour (c/f click stream data): Klaus Mochalski and Hendrik Schulze, “Deep Packet Inspection”, *White Paper* (2009, accessed 9 Apr 2015) <<http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf>>.

¹¹¹ Rich, above n 14.2.

¹¹² ‘Device fingerprinting’ may be defined as “the process of gathering device information to generate device-specific signatures and using them to identify individual devices. . .”: Quiang Xu, Rong Zheng et al., ‘Device Fingerprinting in Wireless Networks: Challenges and Opportunities’, *Cornell University Library* (8 Jan 2015, accessed 3 Apr 2015) <<http://arxiv.org/abs/1501.01367>>.

¹¹³ They may be sessional or persistent. Sessional cookies are erased when a user closes a browser whereas persistent cookies remain on a user’s device for a set period of time: EU ‘Cookies’ *Information Provider’s Guide* (accessed 9 Apr 2015) <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm>.

¹¹⁴ First party cookies are placed by the actual website visited and are usually sessional, which makes them less privacy intrusive. They are not usually regarded as problematic by experts as they expire as soon as a web user logs off.

¹¹⁵ The industry claim this relates solely to large interest categories and is therefore anonymous. See the *OBA Guideline* for an example.

¹¹⁶ Danah Boyd, web theorist cited in Krotoski, above n 28.

¹¹⁷ Tucker, above n 108: 14–16.

¹¹⁸ IAB (UK), ‘A Guide to Online Behavioural Advertising’, *Internet Marketing Handbook Series* (undated, accessed 10 Apr 2015) <http://www.iabuk.net/sites/default/files/publication-download/OnlineBehaviouralAdvertisingHandbook_5455.pdf>.

¹¹⁹ The EU has raised this issue in relation to its present misuse of market power action against Google; one of their arguments as to Google manipulating search results (to benefit its own businesses such as *GoogleShop*) is that this process narrows consumer choice because it affects the way search results (and related advertising) is presented to the consumer: James Kanter and Mark Scott, *Europe Challenges Google, Seeing Violations of Its Antitrust Law*, *The New York Times* (15 Apr 2015, accessed 15 Apr 2015) <http://www.nytimes.com/2015/04/16/business/international/european-union-google-antitrust-case.html?_r=0>.

¹²⁰ Evidence either way depends on the validity of the metrics used: see Ayman Farahat and Michael Bailey, “How Effective is Targeted Advertising?” (16 Apr 2012, accessed 20 Apr 2015) <<http://www.2012.org/proceedings/proceedings/p111.pdf>> which generally concludes it is more effective c/f a 2014 eBay study concluded that paid OBA search ad spending was simply targeting consumers who would buy anyway (*endogeneity*) and as such resulted in “negative returns”: Tom Blake, Steven Tadelis and Chris Nosko, ‘Consumer Heterogeneity and Paid Search Effectiveness: A Large Scale Field Experiment’, *Econometrica* Vol 83 (1) [155–174] (January 2015, accessed 10 Apr 2015) <<http://onlinelibrary.wiley.com.ezproxy.bond.edu.au/doi/10.3982/ECTA12423/epdf>>. It concluded that less frequent purchasers may be influenced, but that was not sufficient to overcome the negative cost effect of the more frequent purchasers not being influenced. See also Derek Thompson, ‘A Dangerous Question: Does Internet Advertising Work at All?’, *The Atlantic* (13 June 2014, accessed 3 Apr 2015) <<http://www.theatlantic.com/business/archive/2014/06/a-dangerous-question-does-internet-advertising-work-at-all/372704/>>. In 2012, ad click throughs for online advertising were plummeting with Google (1/1000) and Facebook (5/10,000): Bob Hoffman, ‘Does Targeting Work?’, *The Ad Contrarian Blog* (1 Feb 2012, accessed 15 Apr 2015) <<http://adcontrarian.blogspot.com.au/2012/02/does-targeting-work.html>>.

¹²¹ Phorm COO Virasb Vahidi cited in Louise Story, “A Company Promises the Deepest Data Mining Yet”, *The New York Times* (20 Mar 2010, accessed 10 Apr 2015) <http://www.nytimes.com/2008/03/20/business/media/20adcoside.html?ref=business&_r=0>.

¹²² Leenes, above n 105: 1–19.

practice is largely left to consumer self-responsibility and industry self-regulation in Australia.¹²³

3.1. Consumer trust: an OBA industry PR crisis?

*The trust a consumer invests in a brand will be embodied . . . increasingly via an emotional bond borne out of how data is collated, stored and used – what we call trust capital. . .*¹²⁴

OBA has failed to earn consumer trust. In 2014, Pew Research Centre reported that 91% of American respondents say that consumers have ‘lost control’ of the online use and collection of personal information.¹²⁵ Of those, 88% agree it is “very difficult” to remove inaccurate online information and 80% are “concerned” that third party advertisers are accessing their shared data online.¹²⁶ In terms of online advertising, 64% said that the government should monitor what online advertisers ‘do’ with personal information and the survey implies a positive relationship between trust and government regulation.¹²⁷ The Australian picture is similar: **consumers do NOT like OBA**. An Australian Communications Media Authority (ACMA) survey in 2013 shows that 78% do not want covert monitoring of their Internet activity and 77% do not want their online behavioural information stored to enable interest-based advertising.¹²⁸ On social media, 58% are not “. . .happy” to see ads, only 35% “sometimes” click on ads, 83% ignore sponsored posts and only 19% “take notice” of ads on social networking sites.¹²⁹

These findings are replicated elsewhere.¹³⁰ Even the Internet Advertising Bureau (IAB) (US) acknowledge that behavioural tracking “. . .increases public anxiety over online privacy, transparency and control. . .”¹³¹ Consumers clearly do not believe industry assurances that no personal data is being collected or used and that data is de-identified (see part 3.2)

¹²³ It is notable that a highly criticised OBA firm such as Phorm made significant money out of their alleged “spyware” in the late nineties, though faced threatened litigation and spawned regulatory concerns (including threatened state-based EU proceedings against the UK), but is still trading today, albeit at a loss. Their latest product *Webwise* is a behavioural targeting system based on deep packet inspection technology, which the ICO have indicated must be an “opt in” system. A number of larger UK entities such as Amazon have opted-out, presumably for customer data protection reasons.

¹²⁴ Blake Cahill, ‘Successful brands of the future are building trust capital now’, *The Guardian* (24 April 2014, accessed 28 Mar 2015) <<http://www.theguardian.com/media-network/media-network-blog/2014/apr/24/brands-trust-future-internet-things>>.

¹²⁵ This percentage agreed or strongly agreed with the proposition. Mary Madden, ‘Public perceptions of privacy and security in the post Snowden Era’, *Pew Research Centre* (2014, accessed 17 Mar 2015) <<http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>>.

¹²⁶ *Ibid.*

¹²⁷ *Ibid.* Surprisingly, it shows that the telephone remains the most trusted form of communications technology.

¹²⁸ OAIC, ‘Community Attitudes to Privacy’, *Research Report* (2013, accessed 30 Mar 2015) 4 <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/Final_report_for_WEB.pdf>.

¹²⁹ Sensis, above n 57: 49.

¹³⁰ See for example, Turow, above n 2; IAB (UK) above n 118.

¹³¹ IAB (US), above n 106: 7.

– and with good reason. The industry is well aware of these vulnerabilities; one UK IAB Guide refers to the industry *challenge* to “increase the likeability” of online advertising and to increase the “sense of control” as factors which the industry should “capitalise on” in explaining OBA to consumers.¹³²

Clearly consumer mistrust of OBA has been on the industry radar for years, but remarkably, despite all of the powerful players involved, the industry has failed to disprove its consumer costs, market its benefits or to enhance the image of targeted advertising with consumers.

3.2. Major (very public) data ‘misuse’

*It should come as no surprise that data thieves target data brokers. . . [which]. . . make big profits by systematically assembling names, addresses, property records and vital statistics. After tapping free public sources for such data, data brokers turn around and sell the data . . .*¹³³

Data breach¹³⁴ – and misuse – happens.¹³⁵ It is expensive,¹³⁶ technologically challenging,¹³⁷ damaging to consumer trust¹³⁸ and can occur at any link in the online advertising supply

¹³² Amy Keen and Marc Dautlich, ‘Consumers attitudes and behaviour’ in IAB (UK), above n 118: 20.

¹³³ Byron Acohido, ‘LexisNexis, Dunn & Bradstreet, Kroll hacked’, *USA Today* (26 Sept 2013, accessed 9 Apr 2015) <<http://www.usatoday.com/story/cybertruth/2013/09/26/lexisnexis-dunn-bradstreet-altegrity-hacked/2878769/>>.

¹³⁴ “Data breach”, in the context of Australian government agencies and private sector organisations that handle ‘personal information’ under the *Privacy Act 1988* (Cth), means “. . .when personal information . . . is lost or subjected to unauthorised access, modification, disclosure, or other misuse of interference. . .”: OAIC, ‘Guide to information security’ (April 2013, accessed 10 Apr 2015) [2] <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information>>.

¹³⁵ Breach may arise through accidental disclosure, hacking, poor employee training or misconduct, lost or stolen computers, or through latent system vulnerabilities and poor security practices.

¹³⁶ Ponemon Institute reports that the costs of data breach in Australia are increasing annually: the cost per disclosed record (\$141) has increased to \$145, organisation cost increased to \$2.8 million (\$2.72 million in 2013), customer ‘churn rates’ increased to 5%, detection and escalation costs increased to 1.07 million (\$1.03 million in 2013); post data breach cost rose to \$0.82 million and lost business costs increased to \$0.85 million. Aside from cost to industry, data breach costs consumers in terms of lost privacy and potential economic exposure to identity theft and other criminal activity. Note that a ‘record’ refers to information which “. . .identifies a person whose confidential information has been compromised in a data breach”: Ponemon, ‘Cost of Data Breach Study’ (May 2013, accessed 9 Apr 2015) [1] <http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-australia-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach>.

¹³⁷ OAIC, above n 134: 16.

¹³⁸ OAIC, ‘Data Breach Notification Guide: A Guide to handling personal information security breaches’ (Aug 2014, accessed 3 Apr 2015) [9] <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>>.

chain.¹³⁹ The Australian Digital Advertisers Association (ADAA) publicly represent that “no personal information is collected or used” and that OBA is “safe and transparent” – assurances which case law disproves and which seem justified only by their own *Guideline* definition. ADAA go further: “. . .advertisers don’t know who you are. . .”¹⁴⁰ But of course, that is not strictly so – and consumers know it.

3.2.1. Data breach

*There are two types of companies. Those that have been hacked and know it and those that have been hacked and don’t know it. . .*¹⁴¹

In the past decade, database breaches of personal and sensitive data are at pandemic levels.¹⁴² Governments,¹⁴³ the world’s largest companies and supposedly, the most secure entities in

the world¹⁴⁴ have fallen victim – as have consumers. Examples in 2013 alone include the following: *SnapChat* lost 4.7 million user details¹⁴⁵; *eBay* lost 145 thousand member details; *Adobe* lost 38 million customer IDs¹⁴⁶; *Apple* lost 12 million user details¹⁴⁷; America’s second largest insurer lost 80 million health records¹⁴⁸ and in 2014, retailer *Target* lost 40 million credit card numbers.¹⁴⁹ Shortly after, *Sony* lost 100 terrabytes of data¹⁵⁰ and top US data brokers, *Lexis Nexis*, *D & B* and *Altegrity* each lost millions of social security records¹⁵¹ – despite “. . .iron-clad means of protecting their data.”¹⁵²

Clearly data breach is a probability, not a possibility – and personal data collected, collated and created for OBA purposes is both highly attractive – and susceptible.

3.2.2. Data ‘misuse’

*. . .guess what everybody: if you use the Internet, you’re the subject of hundreds of experiments at any given time, on every site. That’s how websites work.*¹⁵³

¹³⁹ Randall Rothenberg, “IAB Head: ‘The Digital Advertising Industry Must Stop Having Unprotected Sex’” *Business Insider* (6 Feb 2014, accessed 9 Apr 2015) <<http://www.businessinsider.com.au/iab-randall-rothenberg-supply-chain-2014-2>>.

¹⁴⁰ ADAA, above n 1.

¹⁴¹ Andreas Baumhof, *ThreatMetrix* chief technology officer quoted in Acohido, above n 133.

¹⁴² See Information is Beautiful, ‘World’s Biggest Data Breaches: selected losses greater than 30,000 records’ (updated 30th Mar 2015, accessed 18 Apr 2015) <<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>> for an interactive infographic, which is supported by a spreadsheet of the data.

¹⁴³ In 2012, the Australian Government leaked almost 10,000 asylum seekers’ details online, in “one of the most serious privacy breaches in Australian history”: Paul Farrell and Oliver Laughland, ‘Asylum-seeker data breach to be investigated by privacy commissioner’, *The Guardian* (19 Feb 2014, accessed 9 Apr 2015) <<http://www.theguardian.com/world/2014/feb/19/asylum-seeker-data-breach-to-be-investigated-by-privacy-commissioner>>. Then in 2014, it emailed world leader’s passport and other personal details (e.g. including passport details, date of birth and visa details of the leaders of the US, Russia, Germany, India, Japan, China, Indonesia and the UK) to the wrong entity: Paul Farrell, Oliver Laughland and Asher Wolf, ‘Immigration Department data lapse reveals asylum seekers’ personal data’, *The Guardian* (19 Feb 2014, accessed 9 Jul 2015) <<http://www.theguardian.com/world/2014/feb/19/asylum-seekers-identities-revealed-in-immigration-department-data-lapse>>. Note in the latter case, the Department, in conjunction with the Privacy Commissioner (it seems) elected not to notify world leaders affected of the breach due to its ‘low risk’ assessment – the justification being that the breach was caused by human error and was not systemic, the received email and deleted mail box content was (it was claimed) deleted, and the recipients deemed it “unlikely” that the email would be “. . .accessible, recoverable or stored elsewhere on their system”. The breach allegedly occurred because the sender failed to check Outlook autofill had entered the correct recipient’s details. Within 48 hours of the G20 data breach becoming public, the Immigration Department announced a “Taskforce” to investigate its handling of sensitive information: Paul Farrell, ‘New privacy taskforce announced after leak of G20 leaders’ details’, *The Guardian* (1 Apr 2015, accessed 9 Apr 2015) <<http://www.theguardian.com/world/2015/apr/01/g20-leaders-details-leak-new-privacy-taskforce-announced>>.

¹⁴⁴ The online surveillance activities of the US NSA which were exposed by Edward Snowden. See for example the seminal series of articles by Glenn Greenwald in *The Guardian*: <<http://www.theguardian.com/profile/glenn-greenwald>>. Snowden’s revelations have affected consumers’ confidence in online privacy and data security: Martin Shelton, Lee Rainey and Mary Madden, ‘American’s Privacy Strategies Post Snowden’, *Pew Research Centre* (Mar 2015, accessed 17 Apr 2015) <http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf>.

¹⁴⁵ This included user phone numbers.

¹⁴⁶ This included encrypted passwords and sensitive information (e.g. names, credit card details).

¹⁴⁷ This included name and address and over one million were posted online.

¹⁴⁸ Member data accessed included name, date of birth, address, phone number, email address, social security number and employment information: see <<https://www.anthemfacts.com/faq>>.

¹⁴⁹ Of these, 9200 were used fraudulently post the attack. The FBI is investigating both the *Target* and *Neiman Marcus* hacks.

¹⁵⁰ The Sony attack results were leaked to Wikileaks and included sensitive corporate and systems architecture information, as well as masses of sensitive personal information such as employee salaries/bonuses; social security numbers; dates of birth; HR documents (performance reviews, criminal background checks and termination records); employee medical condition information; passport/visa information of movie stars and crew; as well as internal email spoofs: Kim Zetter, ‘Sony got Hacked Hard: what we know and don’t know yet’, *Wired* (12 Mar 2014, accessed 17 Apr 2015) <<http://www.wired.com/2014/12/sony-hack-what-we-know/>>. See also Information is Beautiful, above n 142.

¹⁵¹ Enigma Software, ‘Cyber Attacks Aimed at Data Brokers D&B, Altegrity and LexisNexis Claim Theft of Important Data’ (2013, accessed 9 Apr 2015) <<http://www.enigmasoftware.com/cyber-attacks-data-brokers-db-altegrity-lexisnexis-theft-important-data/>>. These included social security number, name, and other personal data. Stolen records included those of America’s first lady, Michelle Obama. The sale occurred via a website for 50 cents to \$2.50 per record.

¹⁵² Above n 151.

¹⁵³ Christian Rudder of *OkCupid* in Rudder, Christian, ‘We experiment on human beings’, *OkData* (28 July 2014, accessed 9 Nov 2014) <<http://blog.okcupid.com/index.php/we-experiment-on-human-beings/>>.

Deliberate or unethical corporate data (mis)use is another aspect of data collection online. In one infamous predictive advertising case, retailer *Target* devised a pregnancy prediction model, mailed catalogues out accordingly and faced an irate parent who learned of his teenage daughter's pregnancy – via behavioural advertising.¹⁵⁴ Social media – and especially Facebook – has also been implicated in this area¹⁵⁵: it has tracked user web purchases and posted purchase information on that user's friend's newsfeeds,¹⁵⁶ and conducted 'emotional contagion' experiments on 689,003 users, which led to complaints to the US Federal Trade Commission.¹⁵⁷ Facebook also provides advertisers with a framework enabling randomised controlled experiments on its users.¹⁵⁸ None of this "research" is conducted with explicit user consent beyond the usual platform terms and conditions.¹⁵⁹ It seems unlikely that consumers knew or expected that their online behaviour was Facebook's to (mis)use – or that Facebook makes millions from OBA annually.

OBA data misuse has other adverse consumer implications. There are four main concerns: firstly, algorithmic profiling

enables digital "redlining" through its categorisation practices; that is, discrimination against the vulnerable. This may occur through differential pricing¹⁶⁰ or through automated products which 'score' customers based upon real and inferred attributes relating to neighbourhoods, housing, job security, health and payment capacity.¹⁶¹ Consumers have no control over the facts or inferences¹⁶² or how the OBA industry categorises them – or the often hidden consequences. Secondly, targeted ads enable price discrimination based upon past purchase-inferred 'pain points'. This advantages sellers and creates both "market power in product markets" and overall market inefficiency¹⁶³ as consumers are not informed of all pricing options.¹⁶⁴ Thirdly, the risk of database error is serious: it defeats any 'relevance' in targeted advertising and may impact consumers through inequity and inefficiency.¹⁶⁵ Finally, targeted advertising enables online scammers to target the vulnerable,¹⁶⁶ which is a serious public policy issue, and one

¹⁵⁴ The model was based upon consumer spending patterns, applied to its customer database and used to target catalogue coupons: Duhig, above n 18.

¹⁵⁵ Another famous example is dating website *OkCupid*, which experimented on user suggestibility – by telling 'incompatible' people they were a 'match'.

¹⁵⁶ Due to adverse public reaction, Facebook changed its policy to enable express consent (opt in) before activities on other sites can be shared with friends. See Benjamin R. Mulcahy and Dante M. DiPasquale, 'Efficiency v. Privacy: is online behavioral advertising capable of self-regulation?' (14 April 2010, accessed 15 Mar 2015) <<http://documents.lexology.com/f7f5451b-f755-4c1e-b855-521f924ee99b.pdf>>.

¹⁵⁷ Adam D. I. Kramer, Julie E. Guillory and Jeffery T. Hancock, 'Experimental Evidence of Massive-Scale Emotional contagion through Social Networks' 111 Proc. Natl. Acad. Sci. U.S.A. 8788 (2014). Note there was also no capacity for Facebook to exclude minors from its sample, which added to allegations that the study was unethical: Kashmir Hill, 'Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study', *Forbes* (30 June 2014, accessed 30 July 2014) <<http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/>>. Facebook has also done research to determine if its users are lonely and whether ads perform better with algorithmically-generated (i.e. fake) friend 'endorsements': James Grimmelmann, 'The Law and Ethics of Experimenting on Social Media Users', unpublished working paper provided to the author by email, Mar 2015: manuscript page 4. Professor Grimmelmann formally complained to the FTC but there has been no public outcome to date.

¹⁵⁸ Cade Metz, 'Facebook rolls out a Tool for Testing Ads with control groups', *Wired* (27 Jan 2010) cited in Grimmelmann, *Ibid*.

¹⁵⁹ Facebook changed their user terms in 2014, for the purposes (allegedly) of retrospectively covering up that they did not have sufficiently broad terms and conditions to authorise the study when performed, absent specific user consent. Nor did the study enable them to remove minors from the sample which added to allegations that the study was unethical. Hill commented: "Some critics don't think that throwing the word 'research' into a many-thousands-word-long data use policy is adequate for performing psychological experiments on users, but now it seems that Facebook hadn't even done that.": Hill, above n 157.

¹⁶⁰ The study showed that people in higher-income areas received greater discounts: Jennifer Valentino-Devries and Jeremy Singer-Vine, 'Websites vary prices, deals based on User's information', *The Wall Street Journal* (24 Dec 2012, accessed 20 Apr 2015) <<http://www.wsj.com/articles/SB1000142412788732377204578189391813881534>>. Note this may have been due to differing levels of competition within those areas which is a legitimate pricing consideration.

¹⁶¹ For example, a US businessman had his credit limit reduced after holidaying and shopping in stores where patrons exhibited a "poor repayment history": N. Newman, 'How big data enables economic harm to consumers, especially to low-income and other vulnerable sectors of the population', *Journal of Internet Law*, 18(6):11-23 (2014, accessed 3 Apr 2015) <<http://search.proquest.com/docview/1639829818?accountid=26503>>. This also enables more targeted scams through search ad links; an example is where Google was found to have knowingly allowed illegal pharmacies to target ill people through its *Adwords* search engine function.

¹⁶² Newman, *Ibid*. For example, one broker classified those who responded to sweepstakes offers on a "sucker list" which it promoted as an ideal "subprime credit offer" grouping. Titles, however, evidence the concern: "... ethnic second-city strugglers', 'retiring on empty: singles', 'tough start: young single parents', 'credit crunched city families', and 'rural and barely making it'...".

¹⁶³ Newman, *Ibid*. Note that it enables sellers to increase profits but buyers lose out. "Economic models generally show that overall prices in the economy will end up higher than any model where consumers know all prices. . .".

¹⁶⁴ Joseph Stiglitz cited in Newman, *Ibid*.

¹⁶⁵ The US 'e-verify' system as to the right to work in the US is cited as an example where inaccurate results may have dire consequences. Errors arise due to multiple surnames, surname changes and the like. However, the system has reduced error rates for US citizens over 60% in the past five years – which suggests it may originally have caused significant problems: Office of the President: above n 23: 52.

¹⁶⁶ An example is where Google was found to have knowingly allowed illegal pharmacies to target ill people through its *Adwords* search engine function. This cost Google a \$500 million civil forfeiture settlement, representing gross advertising revenue plus gross revenue made by Canadian online pharmacies from illegal drug sales in the US: US Department of Justice, 'Google Forfeits \$500 Million Generated by Online Ads and Prescription Drug Sales by Canadian Online Pharmacies' (24 Aug 2011, accessed 25 April 2015) <<http://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-Canadian-online>>.

which like these other concerns, the industry tends not to address publicly.

3.2.3. Strategic acquisition and inter-company data sharing
Strategic corporate acquisition can also yield potential data (mis)use results. Both Australian privacy law¹⁶⁷ and the OBA Guideline permit use of data passed between related bodies corporate.¹⁶⁸ For example, a popular Facebook app, *Social Calendar*, was purchased by Walmart in 2012. This meant that 15 million registered users, 110 million personal notifications (such as date of birth, anniversary date and the like) and 10 million monthly reminders were suddenly able to be combined with Walmart's already extensive customer databases, as well as any others to which they had access.¹⁶⁹ This data was used in OBA recommending Walmart gift purchases to users based upon their friends' Facebook page content. Similarly, Google purchased *DoubleClick* in 2008 to feed data into its AdSense advertising network for OBA purposes which by 2011, made Google some \$36.5 billion.¹⁷⁰

3.2.4. Data anonymity – no one will know!
Twitter sells data: it makes \$70 million annually from a daily data stream of half-a-billion public tweets.¹⁷¹ It also matches profiles to an advertiser's database using email addresses to enable targeted advertising, but claims: “. . . it's done in a completely anonymised fashion”.¹⁷²

¹⁶⁷ Privacy Act 1988 (Cth) section 13B provides that collection of “personal information” (PI) (but not “sensitive information” as defined) between related bodies corporate is not generally an interference with the privacy of an individual. APP 6.6 says PI shared between related bodies corporate has the same “primary purpose” for both as at collection. PA Guideline page 18 [para 6.77] ‘Related bodies corporate’ is defined in the Corporations Law.

¹⁶⁸ This may also expose data to state abuse: In *Schrems*, the applicant seeks to prevent his data being transferred from Facebook Ireland to the US under a self-certified privacy safe harbour scheme on the basis that US laws expose his data to “mass and indiscriminate surveillance” such that the US no longer qualifies for the scheme: *Schrems v Data Commissioner & Digital Rights Ireland*, Court of Justice of the EU, Case No: C-362/14 *Oral Speaking Notes of Maximilian Schrems* (24 Mar 2015, accessed 10 Apr 2015) <http://www.europe-v-facebook.org/CJEU_spaking_notes.pdf>. There is also a class action impugning Facebook's data handling and privacy practices including its terms and conditions: <http://europe-v-facebook.org/EN/en.html> [para 1].

¹⁶⁹ “A reminder of a friend's birthday. . . is a strong psychological gift moment. To then make a truly personalized recommendation at that same instant is going to have huge potential.” Sean Gallagher, ‘Walmart buys a Facebook-based calendar app to get a look at customers' dates’, *Ars Technica* (17 Mar 2012, accessed 12 Apr 2015) <<http://arstechnica.com/business/2012/03/wal-mart-buys-a-facebook-app-to-get-a-look-at-customers-calendars/>>.

¹⁷⁰ The purchase price was US\$3.1 billion. Data taken from *Google v Vidal-Hall, Hann and Bradshaw* [2015] EWHC Civ 311 [para 6.1].

¹⁷¹ Garside, above n 17.

¹⁷² Garside, above n 17 citing Chris Moody, Twitter data strategy chief.

Consumers are justifiably wary of such claims.¹⁷³ In Australia, the use of de-identified¹⁷⁴ or anonymised¹⁷⁵ data is largely unregulated. The problem in a big data context with constant technological advances is that data from multiple sources may be combined, and arguably “. . . will almost certainly” enable re-identification.¹⁷⁶ Infamous examples of this abound: AOL released 19 million web searches of 700,000 anonymised consumers, only to find many of them re-identified publicly.¹⁷⁷ A researcher identified a US state governor from supposedly de-identified public health data.¹⁷⁸ The Wall

¹⁷³ See the numerous examples cited in Bruce Schneier, “Why ‘Anonymous’ Data Sometimes Isn't”, *Wired* (13 Dec 2007, accessed 15 Apr 2015) <http://archive.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213>.

¹⁷⁴ ‘De-identification’ means that the information is no longer about an identified individual or one who is reasonably identifiable: section 6(1) Privacy Act 1988 (Cth). It usually includes two aspects: firstly, removing personal identifiers (name, address, dob etc) and secondly, removal/alteration of other information which may allow identification (e.g. rare characteristics or a combination thereof): OAIC, ‘De-identification of Data and Information’, *Privacy Business Resource 4* (April 2014, accessed 20 Apr 2015) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy_business_resource_4.pdf>.

¹⁷⁵ ‘Anonymisation’ means processing personal data so as to irreversibly prevent identification. Methods include randomisation, generalisation, pseudonymisation, noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity and t-closeness.: EU, ‘Opinion 05/2014 on Anonymisation techniques’, Article 29 Data Protection Working Party (adopted 10 Apr 2014, accessed 15 Apr 2015) [3] <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

¹⁷⁶ As this authors point out, this may lead to the need for Privacy Act consents to be obtained post data collection (at the time of re-identification) which is so administratively difficult that businesses may either ‘lock up’ their data or ignore the Act: Saadati, above n 29.

¹⁷⁷ Numeric IDs were attached to each of the 658,000 subscribers whose searches (as they do) contained identifying personal information; e.g. name, location and social security data: Anick Jesdanun, ‘AOL: Breach of Privacy Was a Mistake’, *The Washington Post* (7 Aug 2006, accessed 15 Apr 2015) <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700790_2.html>.

¹⁷⁸ The Massachusetts Group Insurance Commission (GIC) released anonymised data as to state employee hospital visits for researcher use – which the Governor assured everyone were private as identifiers had been removed. Latanya Sweeney decided to test that proposition; she knew the governor's city, purchased the voting roll and combined the voter information – name, address, postcode and dob – with the GIC records. Her study revealed 6 people with his dob, 3 were male and only he had the right postcode. She thus located the Governor's data, which she sent to his office: Nate Anderson, ‘“Anonymized” data really isn't – and here's why not’, *Ars Technica* (8 Sept 2009, accessed 15 Apr 2015) <http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/>.

Street Journal found that 25% of websites studied passed on personal login details (name, email address, etc) to third party companies, including sexual orientation and drug use habits,¹⁷⁹ and that retailers and data brokers combine information – to attach an identified individual to their anonymised browsing history. Then both are delivered-up to the retailer.¹⁸⁰ Facebook for example, serves ads to consumers “based upon their identity” for advertisers who already have the user email address. As such, “data fusion”¹⁸¹ through combining dataset analytics with broad privacy statement-enabled uses, and the “mosaic effect”,¹⁸² mean that data de-identification is a “limited proposition”¹⁸³ and “. . . an illusion,”¹⁸⁴ entailing ongoing “residual risks” to consumer privacy.¹⁸⁵

This blurring of the boundaries of personal and non-personal information online is problematic for the OBA industry¹⁸⁶ and challenges industry data privacy compliance practices. Despite allowing de-identified data release in certain

circumstances,¹⁸⁷ the Office of the Australian Information Commissioner (OAIC) warns that the risk may require constant re-assessment and minimisation to prevent re-identification of already published information. It seems questionable in the highly dynamic OBA context if this requirement, much less auditing and compliance of this regime, is either practical or possible.

3.3. Consent and contractual nightmares: reading the terms and conditions

. . . more than 60% of respondents rarely or never read website privacy policies. . .¹⁸⁸

Consumer contracts are at the heart of both personal information collection online and its consensual use for online behavioural advertising. Website or social media platform terms and conditions, privacy policies, data policies, tracking policies and pop-up boxes use methods of acceptance as diverse as mandatory notice,¹⁸⁹ ‘take it or leave it’,¹⁹⁰ opt-in or opt-out,¹⁹¹ tick a box¹⁹² or privacy-linked warnings deeming consent

¹⁷⁹ Jennifer Valentino-DeVries and Jeremy Singer-Vine, ‘They Know What You’re Shopping For’, *The Wall Street Journal* (7 Dec 2012, accessed 28 Mar 2015) <<http://www.wsj.com/articles/SB10001424127887324784404578143144132736214>>. OkCupid sent user names to one company, gender, age and postcode data to seven companies, drug use to six companies and sexual orientation to two companies – but claims that as sent, it is all ‘anonymized’. Clearly this does not mean that the recipient or its agencies cannot re-identify the data.

¹⁸⁰ Ibid. For example, a consumer fills in an online enquiry form to a car dealer giving name and email address. That information is collected based upon terms and conditions which enable it to be on-sent to the dealer’s contractors such as the data broker. The form is sent to the broker, who provides a ‘de-identified’ browsing history of that consumer back to the dealer. The dealer is then of course in possession of both pieces of information, and may market to that consumer using their browsing history as background information. The broker claims it only provided ‘anonymised’ information.

¹⁸¹ Executive Office of the President, above n 23.

¹⁸² Ibid: this means the integration of big data whereby personally identifiable information can be derived or inferred from supposedly de-identified datasets.

¹⁸³ PCAST Report, ‘Big Data and Privacy’ Harvard Law Petrie-Flom Center, *Online Symposium on the Law, Ethics and Science of Re-identification Demonstrations* (2013) cited Ibid: 8 [fn 19].

¹⁸⁴ Data from just four ‘anonymous’ credit card purchases can identify 90% of people: Jamie Condliffe, ‘Anonymised Credit Card Data Really Isn’t Very Anonymous’, *Gizmodo* (31 Jan 2015, accessed 15 Apr 2015) <<http://www.gizmodo.com.au/2015/01/anonymized-credit-card-data-really-isnt-very-anonymous/>>.

¹⁸⁵ The EU opinion concluded that unless engineered properly and constantly revised to reflect latest technology developments, anonymisation presents “residual risks” to consumers: EU, above n 175.

¹⁸⁶ In 2009, the FTC concluded that “. . . rapidly changing technologies and other factors. . .” have blurred the lines as to what constitutes personally identifiable information: FTC, above n 67: iii.

¹⁸⁷ The OAIC allow ‘information asset’ release of de-identified data, provided that indirect identification risks are assessed and managed via a ‘motivated intruder’ test, an assessment is done ‘in the round’ and factors such as the cost, practicality, difficulty and likelihood of re-identification occurring are considered. ‘De-identification’ may occur through many methods which must be assessed in context: the OAIC list examples such as removing quasi-identifiers (eg, profession, income), combing identifying information into categories (e.g. ages into 25–35); using ‘tolerable errors’; swapping information between data subjects to retain the same overall outcomes; using synthetic data and data suppression: OAIC, above n 174:3–4. ‘Motivated intruder’ test means whether a reasonably competent non-specialist but motivated person would be able to identify the data via resources such as the Internet, public documents and reasonable enquiries. ‘In the round’ means an assessment of whether any entity or member of the public could identify an individual from the data, including in combination with other available information/data.

¹⁸⁸ Mark Andrejevic, University of Qld Centre for Critical and Cultural studies quoted in Saadati, above n 29.

¹⁸⁹ This is the scheme under the Privacy Act 1988 (Cth) for personal information which is not ‘sensitive’ as defined.

¹⁹⁰ This is the Facebook (and usual social media) model – subject only to the impacts of regulator or consumer pressure which has in the past, caused Facebook to modify new policies. To sign up, consumers must ‘accept’ a myriad of policies and rules, many of which are designed to enable data collection and its use.

¹⁹¹ For example, the OBA ‘opt out’ system at www.youronlinechoices.com.au. Note that this does not work with Internet Explorer.

¹⁹² Directive 95/46/EC specifies that ‘Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website’. <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>>. Note that in Australia, a pre-checked box is not effective consent under the Spam Act according to the regulator, the Australian Communications and Media Authority (ACMA): Justin Cudmore and James True, ‘Before you hit send: Complying with the Spam Act – the unsubscribe and identification requirements’, *Marque Lawyers* (9 November 2014, accessed 25 Mar 2015) <http://www.marquelawyers.com.au/assets/marque-update_before-you-hit-send-complying-with-the-spam-act-has-the-recipient-consented-161014.pdf?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link>.

through further site use.¹⁹³ This part puts the view that OBA 'consent' online is largely a legal fiction, which is a serious consumer deficiency given it underpins the targeting of advertising to consumers using personal and potentially, sensitive information.

3.3.1. Consent

In Australia, the *Privacy Act 1988* (Cth) prescribes that 'consent' means 'express'¹⁹⁴ or 'implied' consent.¹⁹⁵ It also mandates that the collection of 'personal information' (PI) (which includes¹⁹⁶ information reasonably capable of being re-identified) requires provision of a mandatory notice at or before the time of PI collection. If any defined 'sensitive information'¹⁹⁷ is collected or if PI is to be used for a purpose other than for the primary purpose disclosed at the time of its collection, then unless impracticable to obtain, prior express consent is required.

For OBA Guideline signatories, the consent requirements as to non-personal information collection depend upon the signatory's role: ISPs as 'Service Providers'¹⁹⁸ have different obligations to 'Third Party' OBA providers (such as ad

networks) and website publishers. The former must obtain Explicit Consent which is 'an active step demonstrating consent in response to a specific query' (e.g. click 'accept') and provide a withdrawal mechanism (e.g. an opt out) [Principle III].¹⁹⁹ Third Parties must provide for website notice plus either 'Explicit Consent' or 'Enhanced Consent'. This latter consent requires a linked notice (either in-ad or by the webpage on which the ad appears) or notice on an industry-developed website [Principle II], plus consumer 'choice' through an 'opt out' system accessible from its privacy notice.²⁰⁰ Website Operators (publishers) allowing third party OBA are required to provide "adequate disclosure", presumably in their privacy statement [Principle II B].

OAIC guidelines provide that consent²⁰¹ has four elements: the individual must be adequately informed²⁰² prior to giving consent, it must be voluntary,²⁰³ current and specific²⁰⁴ and provided by an individual with the capacity²⁰⁵ to understand and to communicate that consent. In order to effectively 'inform' consumers, *privacy policies* or notices must be honest, accurate and specific, easy to understand, prominently positioned, accessible for consumers with a disability and updated when necessary.²⁰⁶

Consent to OBA is generally obtained through either express consent (via an online registration form with an accept box for example) or by implied consent via a combination of privacy statement and in-ad linked notices. Industry assertions that consent may be implied by consumer failure to opt out online or to set a browser to exclude cookies have not gained traction with regulators. But what is apparent is that prior express consent, especially for the use of sensitive information, is rarely obtainable online absent a registration form or other mechanisms enabling consumer interaction. What is not apparent is how much sensitive information a consumer's browsing data may yield, without explicit consent being provided. Likewise, what is not apparent is that cookies

¹⁹³ An example is the Experia website which states: "We use cookies on this site to enhance user experience. By continuing on this website, you are agreeing to use of these cookies. For more information, please read our [hyper-linked] cookie policy." <<https://www.experianplc.com/news/company-news/2014/04-04-2014.aspx>>.

¹⁹⁴ The non-legally binding OAIC Guidelines indicate this is 'given explicitly, either orally or in writing'. Examples in an online context might include clicking 'agree': OAIC, 'Australian Privacy Principles Guidelines' (1 April 2015, accessed 5 April 2015) [9 para B. 36] <http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/appguidelines/APP_guidelines_complete_version_1_April_2015.pdf>.

¹⁹⁵ Section 6(1) contains this definition. The non-binding Guidelines suggest that this means consent may be reasonably inferable in the circumstances from conduct of the parties: Ibid [para B.37].

¹⁹⁶ The Privacy Commissioner states that personal information may include ". . . photographs, Internet Protocol (IP) addresses, Unique Device Identifiers (UDIDs) and other unique identifiers, contact lists, which reveal details about a user's social connections and the contacts themselves, voice print and facial recognition biometrics, because they identify and collect unique characteristics of an individual's voice or face, location information, because it can reveal user activity patterns and habits and, as a consequence, identity." Devices often hold personal information which can potentially be linked to the identity of their users: Timothy Pilgrim, 'App purchases by Australian consumers on mobile and handheld devices', *Submission to the Commonwealth Consumer Affairs Advisory Council* (2013, accessed 20 Apr 2015) <http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/app-purchases-by-australian-consumers-on-mobile-and-handheld-devices#_Toc352143563>.

¹⁹⁷ This is defined to include an individual's racial or ethnic origin; health information; political opinions; membership of a political association, professional or trade association or trade union; religious beliefs or affiliations; philosophical beliefs; sexual orientation or practices; criminal record; genetic information; biometric information that is to be used for certain purposes; biometric templates.

¹⁹⁸ An entity is a 'Service Provider' to the extent that it provides any of: an internet access service, toolbar, Internet browser, desktop application and client software.

¹⁹⁹ ADAA, above n 64.

²⁰⁰ Guideline Principle III is satisfied in practice through links to the OBA opt-out system at youonlinechoices.com.au.

²⁰¹ OAIC, above n 194.

²⁰² The non-binding OAIC Guidelines indicate that this means properly and clearly informed in plain English and without jargon; that is, aware of the implications of withholding consent such as that access to a website may be denied: OAIC, above n 194: 11 para B.47.

²⁰³ The OAIC Guidelines provide that this arises if the individual has a 'genuine opportunity' to provide or withhold consent and excludes duress, coercion or pressure such as to overpower the individual's will: OAIC, above n 194: 10, para B 43.

²⁰⁴ The OAIC Guidelines provide that this should be sought upon collection or at the time of use/disclosure, does not last indefinitely, should be no broader than required for uses and may be withdrawn at any time: OAIC, above n 194: 11 para B.48-51.

²⁰⁵ The OAIC Guidelines provide that capacity means that the individual is capable of understanding the consent decision and may be presumed to have capacity unless there is anything to alert the recipient otherwise. Note, however, that the guidelines make no mention of capacity online; yet it is clearly a circumstance where persons without the requisite capacity could attempt to provide consent and the recipient is unlikely to be alerted otherwise: OAIC, above n 194: 11 [para B. 52-55].

²⁰⁶ Pilgrim, above n 196.

and other tracking devices are being installed based upon implied consents in website privacy statements which few will ever read.

3.3.2. Online contracting for consent: privacy statements and the like

Consumers either do not read or do not understand most privacy statement or online terms pertaining to OBA, which are invariably a standard form document. This is problematic both from a consent perspective, but also under consumer law. Unfair terms regimes have now been in place in Australia for a number of years – but privacy policies and website terms and conditions which justify OBA activities remain controversial. It seems that many OBA industry members are failing to voluntarily regulate their own contracting behaviour, even under the shadow of the law. From the perspective of the legitimacy of online consent, and potentials for unfairness and unconscionability, it is useful to consider why this is the case.

Research evidences that consumers do not read online terms and conditions, do not understand them fully and that many of the terms are unfair and potentially unconscionable.²⁰⁷ A 2009 US study showed only one or two of every 1000 consumers accessed online terms and conditions and those that did only read a small proportion of the text.²⁰⁸ In 2012, researchers estimated that reading every privacy policy encountered on the Internet would take consumers 76 work days per year.²⁰⁹ IDG report that the median terms and conditions word count²¹⁰ for

the top 75 US websites is 2514,²¹¹ with Facebook at 11,195, LinkedIn at 7294, twitter at 3486 and Google+ at 1691.²¹² Length itself is inherently off-putting to consumers, and may even constitute a factor in finding a contract term to be unfair according to recent UK authority.²¹³ One online gaming store facetiously proved the point by inserting an “immortal soul clause” in their website terms and conditions. In one day, 7500 consumers granted Gamestation an eternal option to claim their “immortal soul”²¹⁴ without liability for loss or damage thereby caused²¹⁵ and upon notice served “in 6 (six) foot high letters of fire.” Only 12% of consumers selected “click here to nullify your soul transfer”;²¹⁶ the rest (presumably) did not read the terms and conditions. IDG also report that 93% of users do not read website terms and conditions,²¹⁷ with 43% complaining that they are too “boring” and cannot be understood.²¹⁸ The gist

²¹¹ A 2012 privacy policy study of the 75 top US websites suggests that the median length of their privacy statement is 2514 words and would take a consumer ten minutes to read. Given terms and conditions are usually equivalent to or longer than the privacy statements, this extrapolates to at least twenty minutes to read the contractual terms and conditions: Aleecia M. McDonald & Lorrie Faith Cranor ‘The Cost of Reading Privacy Policies’, *I/S: A Journal of Law and Policy for the Information Society* (2008, accessed 29 July 2014) <<http://www.is-journal.org/>> <<http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>>. The authors calculated the average privacy policy read time using the 75 most popular websites and an assumed 250 word per minute average reading rate. Using the 10 minute average reading time per policy, then known numbers of Americans online and average website use (using Nielsen/Net Ratings and Pew data) plus time valued at double wages for work and 25% average hourly salary for leisure, the survey found that the national opportunity cost in time to read policies was \$781 billion. They conclude that adding in comparison time to allow informed decision-making plus individual privacy “value” to the individual, meant that “targeted online advertising may have negative social utility”. See also Madrigal, above n 209.

²¹² Swinhoe, above n 210. Others include Reddit on 5706 and MySpace on 5486.

²¹³ *Spreadex v Cochrane* [2012] EWHC 1290.

²¹⁴ Fox News, ‘7500 Online Shoppers Unknowingly Sold Their Souls’ (15 April 2010, accessed 24 June 2014) <<http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/>>.

²¹⁵ “By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non-transferable option to claim, for now and forever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamestation.co.uk or one of its duly authorized minions.” See Catharine Smith ‘7500 Online Shoppers Accidentally Sold Their Souls to Gamestation’, *Huffington Post* (25 May 2011, accessed 21 June 2014) <http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html>.

²¹⁶ These consumers received a £5 coupon for noticing the link. The clause went on: “we reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction.”

²¹⁷ Swinhoe: above n 210.

²¹⁸ 58% said that they would rather read their utility bill: Swinhoe above n 210.

²⁰⁷ Consumer Affairs Victoria, ‘Unfair Contract terms in Victoria: Research into their extent, Nature, Cost and Implications’, *Research Paper No. 12* (October 2007, accessed 5 Aug 2014) [15] <<http://www.consumer.vic.gov.au/resources-and-education/research>>. The Privacy Commissioner cites the following 2001 study: “. . .only 3% of respondents carefully read website privacy policies ‘most of the time’, with the remainder of respondents split evenly between the following answers: ‘I have spent little or no time looking at websites’ privacy policies”, ‘I have glanced through websites’ privacy policies, but I have rarely read them in depth’ and ‘It has depended on the circumstances. Sometimes, I have reviewed websites’ privacy policies carefully. Other times, I have reviewed the privacy policies little, if at all.’

²⁰⁸ *Consumer Affairs Victoria* research shows a quarter of consumers fail to read contracts, and another 21% only gave them “ cursory consideration”: Ibid: 15.

²⁰⁹ Alexis C. Madrigal, ‘Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days’, *The Atlantic* (1 Mar 2012, accessed 28 Jul 2014) <<http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>>. Nationally, this would equate to 53.8 billion hours in the USA.

²¹⁰ Apple iTunes terms and conditions are 19,972 words long, almost 2000 words longer than Shakespeare’s *Macbeth*: Dan Swinhoe, ‘Infoshot: Happy Reading with Terms and Conditions’, *IDG Connect* (3 Jul 2014, accessed 28 Jul 2014) <<http://www.idgconnect.com/abstract/8491/infoshot-happy-reading-with-terms-conditions>>. *Macbeth* is 18,110 words in length.

is that consumers find that online terms and conditions are too long, contain legalese or wordings which consumers cannot understand, and are therefore not accessible to the average person. Add an explanation of OBA into the mix and technical complexity and personal information consequences create significant consumer difficulties.

These factors are precisely the sort of factors which might nullify 'consent' or form the basis for an action under the unfair contracts provisions in section 23 of the ACL and possibly, in unconscionability (as discussed below). Aside from these serious fairness issues, one survey suggests that consumers are suffering adverse outcomes as a result: one in five (21%) have ticked a consent box without realising all relevant contract terms or their implications.²¹⁹ In the case of OBA, consumers suffer detriment by handing over more information than they either want or realise – to a wider range of recipients than they might possibly imagine – and by viewing personally targeted advertising which they may not want to receive.

3.3.3. Enforceability/validity: online contracts

It is now well established that electronic contracts – such as those pertaining to the 'free' use social media or the consensual collection and use of data for online tracking purposes – are (usually) legally enforceable in Australia²²⁰ and many other countries around the world.²²¹ The legal issue is again, consent. If a consumer does not really read the contents of a contract but clicks 'agree' – such as one required to use social media platforms or a website – are they bound by its terms? The general contractual answer is yes – provided that either the terms are so physically obvious that a consumer should have noticed them pre-contract formation or reasonable steps are taken to ensure a person's attention is drawn to the terms and conditions, and they have clicked 'accept'. In this situation, assuming that there is nothing to alert the platform/website provider/OBA collector as to incapacity, then consent is presumed to be valid.²²²

Of course, this applies unless ACL issues of unfair terms, unconscionability or misleading or deceptive conduct arise or if privacy laws are breached, which are considered in the next section.

²¹⁹ Swinhoe, above n 210. For example, 10% were locked into a longer term contract than expected and 5% lost money due to non-cancellation clauses.

²²⁰ The *Electronic Transactions Act 1999* (Cth) paved the way for uniform state legislation across Australia. Other relevant legislation is the *Electronic Transactions (Queensland) Act 2001* (Qld), *Electronic Transactions (Victoria) Act 2000* (Vic), *Electronic Transactions Act 2000* (NSW), *Electronic Transactions Act 2000* (SA), *Electronic Transactions Act 2000* (Tas), *Electronic Transactions Act 2001* (ACT) and *Electronic Transactions (Northern Territory) Act 2000* (NT) and *Electronic Transactions Act 2003* (WA).

²²¹ Jay Forder & Dan Svantesson, *Internet & Ecommerce Law* (Oxford University Press, 2010):34–35. Note the United Nations Commission on Electronic Trade Law (UNICTRAL) *Model Law on Electronic Commerce*.

²²² See the discussion in Forder, above n 221: chapter 4.

4. Privacy and consumer law considered and some OBA cases

*Global legislative programmes dealing with data are playing catch-up with technology. . .*²²³

Part 4 considers regulatory responses to address the many OBA issues identified in this paper. There are no Australian cases or privacy complaints or investigations²²⁴ dealing with OBA, nor has there been close regulatory scrutiny of the industry guidelines or other 'soft' regulatory formats. There is no evidence of OBA complaints management or resolution publicly, nor anecdotally, are code signatories borne down with complaints.²²⁵ Despite significant international consumer concern, regulatory activities and case law, it is as if OBA issues rarely occur in Australia – or Australians are either too lackadaisical – or ill-informed to care. As previously indicated, the author is interested in a consumer law approach to OBA regulation and consumer protection. It seems possible, given privacy law inactivity to date, that the ACCC may yield greater consumer outcomes in terms of improved industry compliance, appropriate investigation and prosecution together with the fostering of innovation and deterrence – if it took at least, an initial lead on this issue.

The following discussion reveals that extant Australian privacy laws and regulatory practices are not addressing or resolving the consumer issues raised by the OBA industry. As such, the privacy law discussion is brief and provided only to illustrate its potential legal application which, in practice, has been inadequate in managing consumer data breach and OBA issues.

4.1. Australian privacy law: a (brief) overview

*Privacy isn't dead, it's just going through an identity crisis. . .*²²⁶

²²³ Cahill, above n 124.

²²⁴ In 2015, the Australian Privacy Commissioner (APC) announced a privacy audit of 21 online privacy policies against the requirements of APP 1. This is a very cost effective and useful form of regulator activity, especially where industry is lagging in its compliance activities: Timothy Pilgrim, 'Privacy Governance' Presentation to iappANZ (11 Feb 2015, accessed 20 Apr 2015) <<http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-governance>>. "We are just getting ready to conduct an assessment of the online privacy policies of 21 entities against the requirements of Australian Privacy Principle 1. These assessments will look at whether the policies are clearly expressed and up-to-date, cover the content and contact requirements and are available in an appropriate form".

²²⁵ The IAB corporate lawyer Daad Soufi was unaware of signatories facing (m)any complaints: Telephone interview, 20 April 2015. Fairfax Media legal department could not recall any complaints other than a small number which were all immediately resolved by informing consumers of the OBA 'opt out' mechanism: Telephone Call to Fairfax Legal Department, 15 April 2015.

²²⁶ Colin Wood 'Rethinking Privacy: Though Technology has Outpaced Policy, That's No Reason to Give Up', *Government Technology* (2 June 2014, accessed 30 Mar 2015) <<http://www.govtech.com/data/Rethinking-Privacy-Though-Technology-has-Outpaced-Policy-Thats-No-Reason-to-Give-Up.html>>.

There is no statutory or common law²²⁷ right of privacy in Australia.²²⁸ Nor are there mandatory data breach laws (as yet)²²⁹ and arguably,²³⁰ online privacy has recently been reduced by new mandatory data retention laws.²³¹ It is in this context that the *Privacy Act 1988 (Cth)* operates – as a set of regulatory principles designed for the offline world, which at times, have an awkward application to the novel and latent challenges of OBA.

The *Privacy Act 1988 (Cth) (PA)* consists of 13 Australian Privacy Principles (*APP*)²³² which are designed to, inter alia,²³³

regulate²³⁴ the collection, use, storage and disclosure (collectively *handling*) of defined ‘personal information’, and to provide a consumer right to access and correct that information.²³⁵ Since 2014, “personal information” was expanded to mean:

... information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not or whether recorded in material form or not.²³⁶

It clearly applies to the *handling* of information of or about an identified consumer obtained through the use of cookies or other tracking devices, as well as any other ‘personal’ or ‘sensitive’ information as to that person regardless of its source. This has implications for the OBA industry. The 2015 *OAIC Guideline* indicates that an IP address is regarded as ‘personal information’²³⁷ and that access to a database enabling identification by combining information may render an individual ‘reasonably identifiable’.²³⁸ So it is now arguable that OBA browsing-based interest categories may, objectively

²²⁷ The High Court left the possibility open in *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, but subsequent cases have not taken the law further.

²²⁸ c/f the USA, UK, Canada and New Zealand. See a discussion of these actions in Australian Law Reform Commission (ALRC), ‘Serious Invasions of Privacy in the Digital Era’, *Final Report* (June 2014, accessed 3 Apr 2015) 22 [1.24–1.31] <<https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>>.

²²⁹ In 2014, the Privacy Commissioner commented that “. . . a number of high profile breaches were not reported to us. . .” Note that the federal government has foreshadowed enacting such legislation at 2015 end, but as this article suggests, the decision was driven more by the desire to push mandatory data retention laws through a hung Senate (upper house), than any government commitment to data breach privacy: Gavin Smith and Valeska Bloch, ‘Data deal – mandatory data breach notification laws introduced as trade-off for controversial metadata retention regime’, *Allens* (5 March 2015, accessed 31 Mar 2015) <<http://www.lexology.com/library/detail.aspx?g=ed5495b5-1a8a-407e-a94e-6a587893063e>>.

²³⁰ It should be noted that the Communications Minister stated that the bill “. . . does not expand the range of telecommunications metadata which is currently being accessed by law enforcement agencies. It simply ensures that metadata is retained for two years. . .”: Minister for Communications Malcolm Turnbull, *House of Representatives Hansard*, 30 October 2014, p.12560.

²³¹ The Minister stated that the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth)* was designed to prevent the “. . . further degradation of the investigative capabilities of Australia’s law enforcement and national security agencies”: *Ibid*:12562. When passed, it amended the *Telecommunications (Interception and Access) Act 1979 (Cth)* s187AA to specify that telecommunications companies are now obliged to store (inter alia) phone and computer metadata including subscriber/account holder details, and the following as to a communication – source and destination; date, time, duration and location, service type used (e.g. email, SMS, social media or voice) and delivery services type (e.g. cable, Wi-Fi, ADSL, VoIP). The Act excludes storage of the content of phone calls or emails, or web browsing history, all of which are specifically excluded in the legislation for ‘privacy reasons’: Dean Carrigan, John Gallagher and Yvonne Lam, ‘Controversial mandatory data retention laws passed’, *Clyde & Co LLP* (30 March 2015, accessed 31 Mar 2015) <<http://www.lexology.com/library/detail.aspx?g=ef4d20da-0bd0-4045-ae8d-07b14992d6d5>>.

²³² These replaced previous principles via the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, in Schedule 1 of the *Privacy Act 1988 (Cth)*.

²³³ Part III credit reporting provisions apply to the handling of credit-related personal information disclosed by credit providers to credit reporting bodies for inclusion on individuals’ credit reports.

²³⁴ Other largely sector-specific legislation imposing obligations upon the Australian Information Commissioner (*OAIC*) are the *ACT public sector Information Privacy Act 2014 (ACT)*, the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979* under which the APC has consultative, monitoring and compliance functions, information and complaints management obligations under the *National Health Act 1953* as to Medicare and the NHS, tax file numbers and government agency data matching under the *Data-matching Program (Assistance and Tax) Act 1990*, spent conviction breaches and complaints under the *Crimes Act (Cth)*, consultative privacy-related issues assistance to AUSTRAC under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, oversight, complaints and compliance as to health identifiers under the *Healthcare Identifiers Act 2010*, information handling under the eHealth records system: *Personally Controlled Electronic Health Records Act 2012* and personal information contained within the *PPSR: Personal Property Securities Act 2009*.

²³⁵ It also regulates individual tax file numbers under the *Data-matching Program (Assistance and Tax) Act 1990 (Cth)* and sensitive health information for health and medical research purposes.

²³⁶ PA section 6(1). Note that “sensitive information” means: (a) information or an opinion about an individual’s: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

²³⁷ So, too, does the EU Working Party 29 (2008) Opinion and the English Court of Appeal in *Google Inc. v Judith Vidal-Hall and others* [2015] EWCA Civ 311, 27 March 2015. The Court of Appeal held there is a serious case to answer that behavioural data collected by third party cookies is personal data, even when not connected to other information directly identifying an individual.– see part 4.3 following. Note the UK definition of ‘personal information’ is slightly different (but arguably, narrower).

²³⁸ *OAIC*, above n 194: 20 [paras B.92].

considered,²³⁹ be 'personal information' which may be 'disclosed' when seen by third parties online.²⁴⁰ It is likely that in the OBA context, the meaning of 'personal information' will be assessed on a case-by-case basis, as indicated in the Guidelines,²⁴¹ and may be influenced by international cases. Controversially, the OBA industry does not see that information as 'personal information',²⁴² a fact which the OAIC noted in 2011²⁴³ and which is also reflected in the OBA Guideline definition discussed above.

The PA does not apply to most small businesses²⁴⁴ with an annual turnover of \$3 million or less.²⁴⁵ It does apply if these entities (inter alia)²⁴⁶ trade in personal information; that is, either disclose or collect an individual's personal information by (respectively) receiving or providing a "benefit, service or advantage. . ." without the individual's consent.²⁴⁷ So while some data brokers and active data collectors/disclosers may be caught, it is questionable if all smaller entities engaging in OBA will be subject to the PA – for example, a small website operator engaging in first party OBA or allowing third party cookie installation on its site, through for example, use of free Google software that incor-

porates that entitlement.²⁴⁸ As there are no OBA-related privacy cases in Australia, there is no judicial or other guidance on this question. In terms of remedies for breach, the APC's enforcement regime has recently greatly improved: it is now able to conduct audits, make a determination,²⁴⁹ accept court-enforceable written undertakings²⁵⁰ and apply for civil penalty orders.²⁵¹ These range from \$340,000 for individuals to \$1.7 million for companies.

4.1.1. Potential OBA privacy issues?

It seems probable that if the 'personal information' threshold is reached, then certain OBA industry practices would infringe the APP regime,²⁵² if a complaint or APC-initiated investigation were to arise. The more likely potential privacy issues are as follows:

- **APP1** imposes the obligation for an entity to implement PA compliance "practices, procedures and systems" and to have a ". . . clearly expressed and up-to-date" privacy policy available [1.3]; for example, on a website.²⁵³ Many entities have inadequate privacy policies²⁵⁴ which fail to transparently and openly explain OBA collection practices (such as for example, by way of cookies, list purchases, competition data and website registrations) and fail to transparently reveal OBA use purposes and potential data flows. Absent this, then any consent obtained as to use becomes questionable. It is also quite likely that upon audit, many OBA entities would fail to demonstrate the compliance requirements implicit within APP 1.²⁵⁵ The Privacy Commissioner (APC) has recently announced an audit of the privacy policies of 21 online

²³⁹ This is an objective test with 'practical regard to the context within which an issue arises'. Considerations include the nature and amount of information, the circumstances of its receipt, who will access it; other information held by or available to the APP entity holding the information, whether it is possible for that entity to identify the individual having regard to available resources, practicability (including time and cost): OAIC, above n 194: 20–21 [paras B91–B94].

²⁴⁰ Vidal-Hall, above n 170: para 3.

²⁴¹ OAIC, above n 194 'Australian Privacy Principles Guidelines'.

²⁴² Interview with Daad Soufi, IAB corporate lawyer on 20 Apr 2015. She commented as to industry perception but made no legal comment as to this position.

²⁴³ A 2011 OAIC Fact Sheet states that information collected by online advertisers may not be sufficient to identify a person; "it may just be general information about your interests and sites you have visited. So companies using OBA may not need to comply with . . . the Privacy Act about how personal information is handled" (author emphasis). It then states that online information can be combined to provide "a much clearer picture of who you are". This suggests that combined data may constitute 'personal information', which after 2014, may suggest that the prior version may now be captured too – as it relates to "an individual who is reasonably identifiable" in combination with other available data: OAIC, 'Privacy fact sheet 4: Online behavioural advertising – know your choices' (Dec 2011, accessed 15 Mar 2015) <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-4-online-behavioural-advertising-know-your-options>> <<http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/Privacy-fact-sheet-04-online-behavioural-advertising.pdf>>. Note that this pre-dated the expanded definition of 'personal information'.

²⁴⁴ Or not for profits.

²⁴⁵ PA section 6EA provides that they may 'opt-in'. If this link is accurate, there appears to be no entity which has decided to 'opt in' to date: <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-12-2001-coverage-of-and-exemptions-from-the-private-sector-provisions>>.

²⁴⁶ It also includes a (defined) health service provider.

²⁴⁷ Or if mandated by law.

²⁴⁸ Some third party OBA collection occurs in this way – that is, the third party ad network's right to install cookies on site visitor's browsers is bundled within free software which website owners use containing terms and conditions of which they may not even be aware.

²⁴⁹ PA Part VI.

²⁵⁰ PA sections 33E and 33F. See the 2015 Optus case discussed in Part 4.

²⁵¹ PA Part VIB.

²⁵² The APPs are: 1. Open and transparent management of personal information (PI); 2. Anonymity and pseudonymity; 3. Collection of unsolicited PI; 4. Dealing with unsolicited PI; 5. Notification of the collection of PI; 6. Use or disclosure of PI; 7. Direct marketing; 8. Cross-border disclosure of PI; 9. Adoption, use or disclosure of government-related identifiers; 10. Quality of PI; 11. Security of PI; 12. Access to PI; 13. Correction of PI.

²⁵³ This must cover the kinds of PI collected/held, how this occurs; the purposes for which it is collected, held, used and disclosed; access and correction processes; complaints process and management; and location of any overseas disclosure.

²⁵⁴ APP 1.4 details the policy must contain (a) the kinds of PI collected and held; (b) how the entity does this; and (c) for what purpose(s); as well as individual rights such as (d) access and correction; (e) how complaints are made and dealt with; (f) if disclosure occurs to overseas recipients; and (g) the likely overseas countries.

²⁵⁵ The author telephoned one large media organisation which is an OBA Guideline signatory, and found that the privacy statement telephone contact details for the privacy officer were defunct and no-one knew who that officer actually was.

companies under APP 1, which is potentially, a positive development for compliance and potential regulatory action.²⁵⁶

- **APP3** provides that an entity must not solicit²⁵⁷ and collect PI unless it is “reasonably necessary²⁵⁸ for one or more of the entity’s [lawful]²⁵⁹ functions or activities” [3.2] and then, only by “lawful and fair means” [3.5] and from the individual [3.6] – unless it is unreasonable or impractical to do so. “Sensitive information” (SI)²⁶⁰ is only collectable if the individual also “consents.”²⁶¹ While most entities justify obtaining PI for advertising reasons and cookie use for a functionality reason (e.g. a shopping basket), the ‘lawful and fair’ criteria may be contentious in some third party OBA situations, where the purpose or effect of collection is misrepresented²⁶² and/or absent express or implied ‘consent’ (as many be required).
- **APP 5** contains the requirements generally included within privacy statements²⁶³ and stipulates these must be dis-

closed at or before collection where practicable, and clearly and prominently displayed by (e.g.) link or where the PI is collected from a third party, that third party is contractually bound to notify or make the individual aware. Individuals must be informed of the method of collection; for example, through the use of cookies.²⁶⁴ Clearly this is better satisfied by links or ‘accept’ boxes contained within instant pop-ups, rather than through a long, unheralded privacy statement or subsequent in-ad link.

- **APP 6:** PI held²⁶⁵ for a “primary purpose” must not be used for a “secondary purpose” without consent unless the secondary purpose is (if the PI is ‘sensitive’) “directly related” or where not sensitive, “related” to the primary purpose.²⁶⁶ Again subject to ‘consent’ being satisfied, this is simply a drafting exercise which can readily be met through broad purpose categories such as for “online behavioural advertising and for data sale to third parties. . .”. However, big data analysis of disparate datasets from multiple sources seeks to locate correlations and relationships for marketing insights; as such, Leonard asserts that “overcollecting. . . (to sift for possible correlations) is the norm. . .”²⁶⁷ It is also difficult to discern how the integrity of collection purposes can be maintained as data is on-sold to and from brokers and combined in contexts which may lead to re-identification or expose new correlations and uses, perhaps unanticipated upon original collection purposes.
- **APP7**²⁶⁸ prohibits *direct marketing* (DM) using SI without consent, but allows PI use in limited circumstances. DM means the use or disclosure of PI to communicate directly with an individual to promote goods and services and includes “online advertising”.²⁶⁹ An example is OBA on a social media site using PI which includes browsing data or purchase history obtained through the use of cookies²⁷⁰ from identified or identifiable (e.g. logged-in) users. APP 7.2 allows DM use where the information is collected from the individual who would reasonably expect the use for that purpose and a simple opt-out mechanism (such as *youronlinechoices*) is provided. Where there is no such reasonable expectation or where information is collected by a third party (such as a data vendor), where practicable the individual must have consented to use, and an opt-out (reminder) statement must be provided in every piece of DM. Finally, an individual may also notify a DM entity to disclose its source of PI where

²⁵⁶ Pilgrim, above n 224. “We are just getting ready to conduct an assessment of the online privacy policies of 21 entities against the requirements of Australian Privacy Principle 1. These assessments will look at whether the policies are clearly expressed and up-to-date, cover the content and contact requirements and are available in an appropriate form”.

²⁵⁷ ‘Solicited’ PI includes “personal information about an individual provided by another entity in response to a request, direction, order or arrangement for sharing or transferring information between both entities. . .” (i.e. third party OBA or other sharing) as well as forms/competitions completed: OAIC *Guideline* above n 194: 4 [para 3.7]. Note that “unsolicited” PI must be destroyed or de-identified soon as practicable if it is lawful and reasonable to do so: APP 4.

²⁵⁸ This is an objective test as to whether a reasonable person, properly informed would agree collection is necessary: OAIC *Guidelines*, above n 194:6. Note that PI collection may not be reasonably necessary where more information than is required for a function is collected or where it is being collected for entry into a database for future use: *Guideline*, above n 194: 7 [para 2.32].

²⁵⁹ ‘Lawful’ means not unlawful, that is not illegal, criminal, prohibited or proscribed by law and includes collection via hacking for example, but excludes a breach of contract: OAIC *Guidelines*, above n 194:14 [para 3.6–3.61].

²⁶⁰ “Sensitive information” means (a) information or an opinion about an individual’s:(i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

²⁶¹ “Consent” means “express consent or implied consent”: PA section 6.

²⁶² OAIC *Guideline* above n 194: 14 [para 3.63].

²⁶³ APP 5 provides that at or before (or asap after) collection of PI, the entity must take reasonable steps to ensure that the individual is informed of: its identity and contact details; if PI is not collected from the individual or that individual may not be aware of the collection, the fact and circumstances of the collection; if PI was collected mandatorily by law; the purposes of collection; consequences if all or any PI is not collected; any disclosures or type thereof; that its privacy policy contains access/correction/complaints and complaints management information; and finally, details of the location of any overseas disclosure intended.

²⁶⁴ OAIC *Guideline*, above n 194: 6 [para 5.11].

²⁶⁵ The word ‘hold’ refers to information in the possession and control of the entity either physically or by right or power to deal with it: OAIC *Guideline*, above n 194: 4 [para 6.7].

²⁶⁶ APP 6.2 (b)–(e) and 6.3 contain exclusions related to for example, court and enforcement mandated situations.

²⁶⁷ Leonard, Peter “Customer data analytics: privacy settings for ‘Big data’ ” *Business International Data Privacy Law* 4(1) (2014, accessed 10 Apr 2015) 53–68 <<http://idpl.oxfordjournals.org/>>.

²⁶⁸ This is subject to the application of the *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth). Note these do not relate to online advertising.

²⁶⁹ OAIC *Guideline*, above n 194: 3 [para 7.9].

²⁷⁰ OAIC *Guideline*, above n 194: 3 [para 7.11]. Note that to be captured, this must still involve use of ‘personal information’ to select which ads are displayed.

reasonably practicable to do so or to not use such PI to facilitate DM by any other organisation.²⁷¹

- APP 10 and 11 require such steps to be taken as are reasonable in the circumstances to ensure that personal information collected is “accurate up to date and complete” and protected against loss, misuse or interference and “. . . unauthorised use, modification or disclosure”. Both of these areas are fraught for the OBA industry; data may evolve through many hands, constrained by a range of contractual or legal obligations which weaken as the chain becomes more diffuse while re-identification becomes more likely – and of course, consumers end up not knowing where their data is or who may hold or analyse it.

Other APP provisions relate to PI access (APP 12) and correction (APP 13) but are not discussed in detail here.²⁷² The obvious issue is whether a consumer can locate an OBA entity, much less seek access and data correction rights. The application of the APPs by the Australian Privacy Commissioner (APC) is discussed below.

4.1.2. *Privacy enforcement performance – little by little, so far*
The APC has been criticised as a “toothless tiger”²⁷³ for many years,²⁷⁴ and despite recently enhanced enforcement

powers, there is as yet little evidence of a change in policy or approach.²⁷⁵

The APC has options in terms of OBA: it could publicly criticise the OBA *Guidelines* or encourage the industry to register a privacy code,²⁷⁶ and it could investigate an OBA privacy breach complaint or seek to penalise personal data loss due to insufficient hacking protection²⁷⁷ or undertake a self-initiated enquiry under Part V.²⁷⁸ The IAB says it has informed the APC out of courtesy as to a current (minor) OBA Guideline review, but has had little to do with him on this issue practically.²⁷⁹ This seems a common phenomenon: in 2014, there were only 71²⁸⁰ voluntary data breach notifications to the APC under the non-mandatory notification regime,²⁸¹ and albeit those numbers

²⁷¹ This APP does not apply to the *Do Not Call Register Act 2006* or the *Spam Act 2003*.

²⁷² APP 8 Prior to cross border disclosure, an entity, the organisation, must take reasonable steps to ensure that the recipient does not breach the APPs, unless laws apply which impose “substantially similar” obligations which the individual can access. APP 9 prohibits the use of “government related identifiers” subject to certain exclusions. APP 10 provides that an entity must take such reasonable steps (if any) in the circumstances to ensure that PI collected is complete, accurate and “up-to-date” and that PI used or disclosed is accurate, relevant and complete, having regard to the purpose of such use/disclosure. APP11 requires an entity holding PI to take all reasonable steps to protect it from interference, misuse or loss, and from unauthorised access, modification or disclosure. If any PI is no longer needed for any use/disclosure purpose under the APPs, then the entity “. . . must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified”. Finally, APP 12 deals with correction rights.

²⁷³ “The ALRC often heard concerns that the *Privacy Act* is a ‘toothless tiger’, lacking adequate enforcement mechanisms and sufficient sanctions to ensure compliance. . .”: ALRC, ‘Executive Summary’ ALRC Report 108 (2008, accessed 20 Apr 2015) <<http://www.alrc.gov.au/publications/Executive%20Summary/extended-public-engagement#>>; Matt Goodwin, ‘Toothless Tiger. . . Now With Teeth’ Pigott Stinson (3 Sept 2013, accessed 20 Apr 2015) <<http://pigott.com.au/publications/toothless-tigernow-with-teeth/>>.

²⁷⁴ The Department of Immigration cases cited above are cases on point. No proceedings were initiated in either case despite findings of data security and disclosure breaches. In the asylum seeker case, the APC accepted remedial policy, staff education, data retrieval and audit activities. As to the G20 breach, due to its non-systemic nature, it seems that the APC countenanced the decision elected not to notify world leaders: Farrell, above n 143.

²⁷⁵ The first large scale breach case post the amendments involved *Singtel Optus Pty Ltd* which voluntarily notified three privacy breaches caused by their own systems’ security flaws, each affecting over 100,000 customers: Michael Pattinson, ‘First enforceable undertaking under new privacy laws’, *Allens Linklaters* (31 Mar 2015, accessed 20 Apr 2015) <<http://www.allens.com.au/pubs/priv/fopriv31mar15.htm>>. The APC decided not to pursue civil penalties and accepted a section 33E enforceable undertaking from Optus, partly due to its cooperation and the (expensive) systems, audit and related corporate reviews included as a part of the settlement: see the text here: <<http://www.oaic.gov.au/privacy/applying-privacy-law/enforceable-undertakings/singtel-optus-enforceable-undertaking>>. It is surprising though that the APC did not take action under APP 11 as to a failure to take reasonable steps to protect information – in one case, 122,000 customers had personal information published in the White Pages and online – without their consent. This seems an egregious breach with significant potential consumer harm, worthy of civil penalties. In contrast, the ACCC has prosecuted Optus for advertising misrepresentations which resulted in \$3.61M in penalties: the Full Federal Court found that Optus was not a ‘first offender’ and had lax compliance systems: Gilbert & Tobin, ‘Singtel Optus Pty ltd v ACCC’ (27 Apr 2012, accessed 20 Apr 2015) <<http://www.lexology.com/library/detail.aspx?g=46cac7c5-c732-4001-b553-98f620b75935>>.

²⁷⁶ PA Part IIIB.

²⁷⁷ The APC will not take action in circumstances of hacking as there has been no “disclosure” as required under APP 6 unless AP 11 is breached. That is little consolation to consumers affected nor perhaps most importantly, incentive for the hacked organisation to better protect itself – to “take such steps as are reasonable in the circumstances” [APP 11] to protect its data from unwanted intrusion. ‘Hacking’ or unauthorised data access is of course an issue for the police and criminal law enforcement – but again, this does not redress the privacy harm.

²⁷⁸ PA section 33C. See the reports here: <<http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>>.

²⁷⁹ Interview with Daad Soufi, IAB corporate lawyer on 20 April 2015. The Commissioner indicated publicly that he had been involved with the 2011 *Guideline* ‘review’, a remark which seems at odds with Ms Soufi’s comment that this review ‘never really happened’.

²⁸⁰ This is a 16.4% increase on 2012–2013, which is a significant improvement.

²⁸¹ OAIC, ‘Community Attitudes to Privacy Research Report’ (2013, accessed 30 Mar 2015) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/Final_report_for_WEB.pdf>.

increased this past year, they remain small. The Privacy Commissioner asserts that “. . . a number of high profile data breaches. . . were not reported to us. . .” which presumably reflects both the weakness of a non-mandatory reporting scheme and corporate attitudes to the APC. Criticised for its ‘soft’ regulatory approach – even with enhanced powers²⁸² – the APC’s effectiveness is under question. On the positive, it has released many significant and well written advisory documents recently, which may lay the framework for a tougher future approach, and by September 2015, it is claiming a 50% increase in voluntary privacy breach notifications. But overall, the Privacy Regulation Enforcement Policy²⁸³ and corporate priorities emphasise a ‘culture of privacy’ approach rather than enforcement activity²⁸⁴ – despite clear evidence that privacy and data breach is a serious and growing problem in Australia.

Albeit compliance is a laudable aim with potential long term benefits, this type of ‘soft’ enforcement alone rarely initiates the momentum required for aggressive corporate investment in any area of legal compliance. Absent some significant

court cases,²⁸⁵ financial penalties or widespread instances of consumer backlash, it is unlikely to be effective against the significant consumer and privacy issues implicit within online behavioural advertising at this time.

For that reason, we now turn to consumer law and the ACCC.

4.2. Consumer laws: an overview²⁸⁶

Some companies think they have a lot to gain from breaching our competition and consumer law; they should have much to lose as well. . . – ACCC Chair, Rod Sims, 15 Feb 2015²⁸⁷

The Australian Competition and Consumer Commission (ACCC) claims to be closely “watching” the online advertising industry, but has done no public work on consumer issues arising from OBA, including the online contracts and forms of consumer consent which justify its existence.²⁸⁸ The Australian Consumer Law provisions potentially relevant to consumer OBA issues are prohibitions upon misleading and deceptive conduct, unconscionable conduct and unfair contract terms. Remedies available to both the regulator²⁸⁹ and successful plaintiffs²⁹⁰ are extensive.

Given recent EU and US regulatory successes in this area, it is desirable – absent greater privacy law enforcement – that the ACCC turn its attention to OBA industry activities in the near future.

²⁸² See for example, the outcome of the first case of privacy breach when the new powers applied: OAIC, ‘Optus Enforceable undertaking’ (26 March 2015) <<http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/enforceable-undertakings/enforceable-undertaking-optus.pdf>>.

²⁸³ OAIC, ‘Privacy Regulatory Action Policy’ (2014, accessed 9 Apr 2015) <http://www.oaic.gov.au/images/documents/about-us/corporate-information/privacy-operational/OAIC_Privacy_regulatory_action_policy.pdf>.

²⁸⁴ “For the next twelve months our focus will be on governance, assisting organisations and agencies to build a culture of privacy, and ensuring that organisations and agencies are proactive in meeting their compliance requirements. . .”: OAIC, ‘Privacy law reform report card’ (12 Mar 2015, accessed 9 Apr 2015) <<http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-law-reform-report-card>>. Note that six months later, the Privacy Commissioner seemed concerned to emphasise overall systemic improvement across the OAIC, including 117 privacy breach notifications for the preceding year. Whether this “50% increase” in voluntary reporting over 2014 reflects a bulge Sept 2014–Aug 2015 is a possibility, so, too, is the potential for breaches to be increasing significantly or corporations deciding that notification is better practice, or a combination of all these factors – and more. Whatever the cause, the OAIC’s overall performance (despite budget cuts) seems to have improved. This workload improvement may have been assisted by referral of various functions to other agencies: Timothy Pilgrim, ‘Office of the Australian Information Commissioner – Update’, Presentation to The Law Society of New South Wales Government Solicitors Conference, Sydney (1 September 2015, accessed 1 September 2015) <<http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/office-of-the-australian-information-commissioner-update>>. It should be noted that the OAIC is no doubt keen to highlight its achievements; its budget was cut then part reinstated, and it (arguably) survives under the Sword of Damocles; the present Australian Government has announced its intention to disband the Office (to a reduced Privacy Commissioner role) and hive off its FOI functions.

²⁸⁵ The *Optus Case* (see footnote 275 above) is a clear example where the APC opted for an enforceable undertaking rather than seeking the publicity and educative benefits of a court case and potential civil penalty. It sends a signal that organisations which voluntarily notify breaches, cooperate with the APC’s investigation and are prepared to undertake significance compliance obligations and auditing, will not necessarily face enforcement action. The APC’s approach may also be resource-related but it is difficult to imagine a case more likely to succeed than Optus’ admitted breaches.

²⁸⁶ This section considers a basic overview (rather than summary) of the potentially relevant ACL provisions; it does not purport to summarise the law but rather seeks to highlight its possible application to potential OBA issues, especially by reference to the next section – which deals with some international case law.

²⁸⁷ Speech by Rod Sims, ACCC Chairman, ‘ACCC’s Complaint and Enforcement Policy’ Committee for Economic Development of Australia, Sydney (19 February 2015).

²⁸⁸ See for example, the 2014 *Advertising and Selling Guide*, which only mentions online advertising in the context of misleading and deceptive conduct. It makes no mention of OBA and consumer law in its regard: ACCC, ‘Advertising & Selling Guide’ (accessed 3 Oct 2014) <http://www.accc.gov.au/system/files/Advertising%20and%20selling_0.pdf>.

²⁸⁹ ACL Part 5-1 contains non-court imposed enforcement powers including powers to accept undertakings, substantiation notices and the power to issue public warning notices. Section 134A CCA enables the ACCC to issue infringement notices in lieu of civil penalty proceedings as well.

²⁹⁰ ACL Part 5 powers include injunctive relief, pecuniary penalties and compensation orders.

4.2.1. Part 2-1 misleading and deceptive conduct

Online behavioural advertising is a product fuelled by the use of consumer information which is collected through standard form contractual online agreements, often made between large corporations and individuals. Section 18 of the ACL²⁹¹ provides that a ‘person²⁹² shall not in trade or commerce²⁹³ engage in conduct which is misleading or deceptive or which is likely to mislead or deceive’.

The ordinary meaning of these words is that the conduct (which includes statements) involves a real or not remote chance of leading a consumer into error. The ACCC has instituted one case under a section 18 equivalent against Google as to its *Adwords* program, which concerned ‘search’-related advertising, for which the High Court ultimately concluded that Google was not legally responsible.²⁹⁴ As such it was not an OBA-related case under present industry definitions. It is possible, however, that subject to resolvable

issues as to jurisdiction and governing law,²⁹⁵ misleading or deceptive OBA terms and conditions or conduct by an entity acting in breach of OBA terms may be actionable under section 18. It is certainly analogous to US provisions upon which the FTC has recently instituted a number of OBA-related proceedings discussed below.

Given the likelihood that large corporations are involved, many consumers are affected and the potentials for significant remedies²⁹⁶ and industry educative benefits, the ACCC might well consider taking action.

4.2.2. ‘Other’ ACL provisions – goods, services and other complications. . .

Other potentially applicable ACL provisions have higher thresholds, which raise several contentious issues: firstly, whether a purportedly ‘free’ product such as *Facebook* or website access provided upon registration is subject to other ACL provisions at all; and secondly, whether there is a defined “consumer”²⁹⁷ and “supply [or acquisition] of goods or services”, which is required to activate ACL provisions governing unconscionable conduct or unfair terms.²⁹⁸ For the purposes of this paper, it

²⁹¹ The ACL is found in the *Competition and Consumer Act 2010* (Cth) (CCA) Schedule 2. Note that it is a national law such that state fair trading and related legislation mirror the national provisions. As such, they are not dealt with separately here.

²⁹² OBA websites/advertisers including social media platforms are usually corporations which are ‘persons’ under the ACL and are usually regarded as ‘carrying on business within Australia’, either through doing business with an Australian consumer online or through physical presence (for example, by representative offices or data centres) and therefore their conduct is captured under these provisions. Note that as a Commonwealth law, the ACL applies to any trading or financial corporation formed within Australia or incorporated within a territory of Australia, or a foreign corporation (or a holding company of any of these): *Competition and Consumer Act 2010* (Cth) sections 4 and 13(1).

²⁹³ ‘In trade or commerce’ means within Australia or between Australia and any place(s) outside, and includes ‘any business or professional activity (whether or not carried on for profit)’: ACL section 2.

²⁹⁴ *Google Inc. v Australian Competition and Consumer Commission* [2013] HCA 1. The case was watched internationally by regulators, especially after the Full Federal Court found for the ACCC. The High Court overturned that decision, finding that Google was not responsible for misleading and deceptive ad content in sponsored links, albeit its systems ‘arranged’ the content provided by the advertiser and Google staff were shown by emails to have known that some of the ads included competitor’s names. It concerned the content of ‘sponsored links’ containing competitor’s names or trademarks, for which it found the advertisers responsible, not Google. The Court cited *Adwords* terms and conditions and Google’s advertising policies, which precluded deceptive use of business names to imply an affiliation, partnership or any special business relationship. The advertisers included competitor’s names in their sponsored link advertisements but inserted their own website, and Google functionality enabled consumers to click on a competitor’s name and be taken to the advertiser’s site. This was found to be misleading and deceptive. The Full Federal Court took a more technical approach by analysing Google algorithms and concluded that Google’s technology created the sponsored ads and as such they were legally liable for their content: *ACCC v Google* (2012) 201 FCR 503 [522]. The advertisers were found legally liable for breaching the then equivalent of section 18 ACL by the trial judge and did not appeal: *ACCC v Trading Post* (2011) 197 FCR 498.

²⁹⁵ Cases such as *ACCC v Chen* [2002] FCA 1248 and *ACCC v Hughes* [2002] FCA 270 confirm that the overseas websites dealing with Australian consumers are subject to the ACL. There is room for legal argument disputing jurisdiction where the provider is overseas-based and the contractual terms of use prescribe an overseas choice of law to suit the provider, as is commonly the case. For example, Facebook’s terms prescribe the laws of Ireland as the governing law and only allow the laws of a consumer’s usual place of residence to apply where mandated, such as in the EU. Section 67 of the ACL provides that if the ‘proper law’ is Australian, it shall apply regardless of any contrary contractual term; in turn, this requires a court to consider the facts of the case, including the parties’ location, where the services are provided, where the contract was formed, the location of the equipment, as well as the contractual terms. As such, there is no certainty that proceedings can be commenced under Australian law in Australia which is obviously the better forum for an Australian consumer for cost, convenience and enforcement reasons.

²⁹⁶ The remedies for breach are extensive, including injunctions, damages and ancillary orders under Chapter V of the ACL. The ACCC may also seek fines of up to \$1.1 million for corporations and \$220,000 for individuals. Note that the CCA uses the term ‘pecuniary penalties’ to avoid the criminal standard of proof.

²⁹⁷ ACL Section 3 defines a ‘consumer’ by reference to acquiring (1) goods, which in this case would include by “exchange” (section 2); or (2) services by way of acceptance (section 2). Consumer in terms of acquiring ‘goods’ means (in summary) if and only if the amount paid does not exceed \$40,000 or the goods were of a kind ordinarily acquired for personal, domestic or household use or consumption. As indicated, the services offered online (unless possibly a software download alone) would seem to exhibit the character of services, but the question is open.

²⁹⁸ Note that false representations (section 29) and statutory guarantees (Part 3-2) would also apply in the event of the thresholds being satisfied, but it is not proposed to discuss these as they would not readily apply to OBA and related consumer information collection practices.

is not proposed to dissect these issues beyond the suggestion that the discussion as to 'free' in part 4.3 below supports the view that there is an exchange of value (information-for-service) and it seems clear that a website publisher, social media and ad networks are all operating "in trade or commerce" with respect to web users, who are also 'consumers' in the sense that the acquisition (as defined) is valued at less than \$40,000 or is (objectively) for personal, domestic or household use or consumption.²⁹⁹ Therefore, the open question is the 'goods' or 'services' requirement. It is likely that this might be found as a matter of degree on a case-by-case basis, and that albeit software is sometimes provided in these transactions (which is defined as a 'good'), the inherent nature of social media and website registration interactions and experience is indicative of a 'service'. The question is before the Federal Court in 2016, in a case involving international online gaming subscription.³⁰⁰ The defendant argues that subscribed online access to video games is a "service" within ACL section 2(1), so that the ACCC case pleading a consumer 'goods' *acceptable quality* guarantee does not apply. The question will generate much interest if resolved.

Hence for the purposes of this **part 4**, it is assumed that at least websites and social media with which consumers exchange personal information and which require registration 'subject to terms' are (goods or) services and thereby, caught by the ACL provisions. This is relevant both to regulating their conduct in an OBA context and to the terms and conditions under which OBA practices occur.

4.2.3. Part 2-2 unconscionable conduct

Unconscionable conduct is prohibited under ACL section 21 in relation to (goods or) services, or alternatively, by equitable unconscionability under section 20. This latter form applies where

for example, thresholds as to 'goods' or 'services' are not met, but is restrictive in the sense that it requires the web user to exhibit a 'special disability', which is unlikely in an online context.³⁰¹ In contrast, providing its threshold criteria are met, section 21 unconscionability might apply.³⁰² Section 22 sets out a range of non-exclusive criteria to elucidate section 21³⁰³: the most relevant to OBA issues might include the relative bargaining strengths of the parties³⁰⁴; whether the OBA entity required the web user to comply with conditions not reasonably necessary to protect its legitimate interests;³⁰⁵ whether the web user was able to understand the documents³⁰⁶; any undue influence or pressure or unfair tactics exerted upon the web user,³⁰⁷ the extent to which the OBA entity fails to disclose any intended conduct which might affect the web user's interests or any foreseeable risks not apparent to the web user³⁰⁸; and the extent to which the OBA entity acted in good faith.³⁰⁹ In addition, section 22(1)(j) includes the extent to which the OBA entity was prepared to negotiate the contract, the contract terms and conditions, including any unilateral right of variation³¹⁰ the party's conduct in complying with its terms and any post-contractual conduct of either party; all of which may be relevant in an OBA context.

²⁹⁹ 'Consumer' is defined in ACL s. 3 as to both 'goods' and 'services'. In the latter case, the definition provides a person is a 'consumer' if the services do not exceed \$40,000 or are of a kind ordinarily acquired for personal, domestic or household use or consumption. There seems little doubt that the former would apply to an arguably 'free' contract, or even one where information is exchanged for access; but even if not, a service such as joining Facebook would fall within the latter part of the definition as it is of a kind ordinarily acquired for 'personal, domestic or household use or consumption', which is assessed objectively: *Carpet Call v Chan* (1987) 55 ASC 55-553.

³⁰⁰ While *ACCC v Valve Corporation* NSD 886/2014 filed 28 Aug 2014 (NSW Registry, Federal Court of Australia) principally concerns alleged breaches of the consumer guarantee provisions by Valve in its online sale terms, the case must also establish whether in its subscription games provisioning which includes access to software to play online games, Valve is supplying a 'good' or a 'service'. The ACL defines 'computer software' as a 'good' in section 2. This question is relevant as different ACL consumer guarantees apply to goods or services, and the ACCC pleaded its case as to the guarantees pertaining to 'goods' only. Prior to this ACL definition, under state legislation, the NSW Supreme Court held that a digital download was not "goods": *Gammasonics Institute for Medical Research v Comrad Medical Systems* [2010] NSWSC 267.

³⁰¹ ACL section 20 prohibits unconscionable conduct "within the meaning of the unwritten law from time to time" and applies if section 21 does not. It applies to conduct which does not involve the supply or acquisition of goods or services. Note that equitable unconscionability is interpreted by the courts to mean where an innocent party acts under a 'special disadvantage', the other party has actual or constructive knowledge of that disadvantage and unfairly or unconscientiously exploits that disadvantage. In these circumstances, the courts have traditionally placed the onus upon the stronger party to show that the transaction was fair, just and reasonable. 'Special disadvantage' means a serious disadvantage beyond just an inferior bargaining position or commercial vulnerability and extends beyond mere inequality of bargaining power (such as that which exists between a consumer and an entity such as Google). See *Blomley v Ryan* (1956) 99 CLR 362 & *Commercial Bank of Australia v Amadio* (1983) 151 CLR 447.

³⁰² Section 20(2) provides that equitable unconscionability does not apply to situations under which section 21 as to unconscionable conduct in connection with the supply or acquisition of goods and services, applies.

³⁰³ The ACL provides that the court *may* consider the contract terms, the manner in which and extent to which it was carried out and is "not limited" to considering the contract formation circumstances.

³⁰⁴ ACL s 22(1) (a). Note that The High Court has stated that inequality of bargaining power alone cannot constitute equitable unconscionability – which may be persuasive as to s. 21 statutory unconscionability: *ACCC v Berbatis* (2003) 214 CLR 51. See also the recent *ACCC v Coles Supermarkets Australia Pty Limited* [2014] FCA 1405 in which s. 21 was applied against Coles in its business dealings and contracts with its commercial (manufacturer) suppliers, resulting in \$10 million in penalties.

³⁰⁵ ACL s 22(1) (b).

³⁰⁶ ACL s 22(1) (c).

³⁰⁷ ACL s 22(1) (d).

³⁰⁸ ACL s 22(1) (i).

³⁰⁹ ACL s 22(1) (l).

³¹⁰ ACL s 22(1) (k).

There is no authority in Australia applying unconscionability to an online contracting context,³¹¹ much less an OBA scenario. But an argument might well be constructed whereby multiple contractual factors might be pleaded together in order to establish that (for example) a social media provider has acted unconscionably towards a consumer. This might be especially the case in circumstances where terms evince exploiting consumer technical ignorance as to OBA or fail to explain OBA risks not foreseeable to an average consumer³¹² or where the consumer is exploited as a result of a personal vulnerability of which the other party is (somehow) aware.³¹³ The section applies to conduct both before and after contract formation, such that unconscionable sign-up processes entailing long and legalistic online terms and conditions enabling OBA³¹⁴ (especially where access to legal advice is not readily available or recommended) might also be actionable either alone or in conjunction with unconscionable marketing, contractual terms or conduct, in the right circumstances.

ACL remedies for unconscionability are extensive.³¹⁵ It is probable that any such action would be pleaded in conjunction with a claim under the EU-style unfair terms regime. These provisions are briefly considered next.

4.2.4. Part 2-3 unfair contract terms

The unfair contract term provisions render void unfair terms in a ‘standard form’³¹⁶ ‘consumer contract’³¹⁷ made, renewed or varied after 1 July 2010.³¹⁸ Given social media and website terms are in many cases, provider-biased standard form contracts, and consumers are generally unable to negotiate those terms,³¹⁹ these provisions have become particularly relevant in both Australia and the EU.³²⁰ A term is unfair if three criteria apply: firstly, it would cause a significant imbalance in the parties’ rights and obligations arising under the contract; secondly, it is (presumed)³²¹ not to be reasonably necessary to protect the legitimate interests of the advantaged party; and thirdly, it would cause detriment (financial or other) to a party were it applicable or relied upon. The court may take account of factors it thinks relevant and must take into account both transparency³²² and the whole contract.³²³ Albeit a term entitling the collection of personal or other information for OBA purposes is not exemplified in section 25, it might still be found to infringe the three main criteria for unfairness and to lack transparency under section 25(3). In that situation, the term may be severed from the contract if it is capable of operating

³¹¹ There is authority pertaining to online advertising: *ACCC v Zanok Technologies Pty Ltd* [2009] FCA 1124; *Caspi v Microsoft Network LLC* 323 N.J. Super 118 (NJ Super App Div 1999).

³¹² An analogous circumstance might be *ACCC v Keshow* [2005] FCA 558 involving sales of educational materials to indigenous Australians who it seems, did not understand what was being sold to them or how it would be billed.

³¹³ Note that most social media platforms allow children aged over 12 to join up and the OBA *Guideline* allows OBA to children 13 and over. This does not mean, however, that age could not be used to justify an action in unconscionability, as it is arguable that a 13 year old may be unable to understand (e.g.) Facebook terms and conditions – and if signed up with an accurate birth date, Facebook is in a position to know their age.

³¹⁴ Note, however, authority under a previous incarnation of the ACL held that unconscionability requires some circumstances beyond mere contractual terms that would render reliance upon them unreasonable, unfair, wrong or immoral: *Hurley v McDonald’s Australia Ltd* (2000) ATPR 41–741 [31] as discussed in Dan Jerker Svantesson, ‘Unconscionability: Consumer Ecommerce’, *Commercial Law Quarterly: The Journal of the Commercial Law Association of Australia* 25:1 (Mar/May 2011, accessed 23 May 2014) [11] <<http://search.informit.com.au.ezproxy.bond.edu.au/documentSummary;dn=043279687656685;res=IELHSS>> ISSN:0819-4262>. It is possible that this case would be distinguished given the franchise context – the earlier case of *George T Collings (Aust) Pty Ltd v H F Stevenson (Aust) Pty Ltd* (1991) ATPR 41–104 [52,622–3] found that an onerous standard form contract term could not be relied upon as it was unconscionable.

³¹⁵ Depending upon who institutes the action (a ‘customer’ or the ACCC), remedies include undertakings (s. 218); substantiation notices (s. 219); public warning notices (s. 223); pecuniary penalties (s. 224); injunctions (s. 232); damages (s. 236 subject to CCA s. 137B); compensation or other orders (s. 237); non-punitive orders (s. 246); adverse publicity orders (s. 247); disqualification orders (s. 248) and infringement notices (s. 134A CCA).

³¹⁶ ACL s. 27 imposes a presumption that the contract is standard form, unless another party in the proceeding proves otherwise – by reference to ss (2) which lists (a) whether one party has most of the bargaining power; (b) whether the contract was prepared by one party; (c) whether one party was required to “accept or reject” those terms; (d) whether there was effective opportunity to negotiate the terms; whether the terms take into account the specific characteristics of another party; and (f) any other matter prescribed in the regulations. Clearly, this would apply to most consumer ‘sign-up’ situations.

³¹⁷ A consumer contract, as discussed above in part 2, means a contract for the supply of goods or services to an individual who subjectively acquires them for personal, domestic or household use or consumption. Part 2–3 does not apply to a contract to supply goods or services for business use between businesses.

³¹⁸ Note these provisions came in six months earlier than other ACL provisions. With respect to the Cth, contracts entered into or varied after 1 Jul 2012 are covered, those varied or renewed apply only to the extent of the renewal or variation: *Trade Practices Amendment (Australian Consumer Law) Act (No 2) Schedule 7, section 8(2)*.

³¹⁹ Most OBA notice terms are presented on a take-it-or-leave-it basis which reflects administrative convenience as well as (inequality of) bargaining power. The consumer who wants Facebook is not in a position to call Facebook Inc. to amend terms. They are however, in a position to select another social network – but arguably none are substitutable in terms of market – at least not in terms of Facebook’s reach, services or popularity.

³²⁰ Council Directive (EC) 93/13 on Unfair Terms in Consumer Contracts [1993] O.J. 24 April 1993, L 95/29 <<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?url=CELEX:31993L0013&from=EN>>.

³²¹ ACL section 24(4) imposes a presumption against the party advantaged by the term.

³²² ACL section 24(3) defines transparency as a term expressed in reasonably plain language, legible and presented clearly readily available to any party affected by the term.

³²³ ACL section 24(2). Note that section 23 does not apply to any term which defines the subject matter of the contract (that is, consideration payable disclosed when the contract is entered into but excludes any consideration contingent upon the happening or non-happening of any particular event: ACL section 26(2)). Or sets the upfront price payable under it; or is a term expressly required by law: ACL section 26.

in its absence³²⁴ which in the case of OBA clauses, would usually be the case.

In March 2015, a Belgian Report into Facebook concluded that “. . . Facebook. . . violates the EU Unfair Contract Terms Directive” which it asserts, covers all consumer contracts for the supply of goods and services, including ‘free’ services.³²⁵ Those violations relate to (inter alia) major contractual terms³²⁶ but do not preclude lesser terms such as those pertaining to OBA which equally, ought not to infringe unfair terms laws. In May, the Belgian Commission for the Protection of Privacy issued a detailed and strongly argued Recommendation 04/2015 urging Facebook to desist from its secret “tracking and tracing” of users, and finding that Facebook was in violation of privacy laws. Finally, when Facebook stonewalled this regulatory “hint” by re-asserting a jurisdictional barr, the Commission issued legal proceedings.³²⁷ The original BPC Report found that Facebook “. . . leverages its dominant position on the OSN³²⁸ market to legitimise the tracking of individual’s behaviour across services and devices”.³²⁹ It found that tracking is both “horizontal and vertical” which means that Facebook combines data from acquired companies, partnering platforms and websites or ‘partnered’ mobile apps as well as ‘vertical expansion’ through WhatsApp and Instagram acquisitions and new (tracking-

enabling) functionalities.³³⁰ On 10 November 2015, the Court gave Facebook 48 hours to cease tracking users who did not have a Facebook account via cookies and plug-ins, or face daily fines of 250,000 EUR. The judgment confirmed that cookies track and collect “personal data” and that an IP address constitutes “personal data”; in both cases, express consent to data collection is required under Belgian privacy laws. Further the data collection was neither lawful or fair, as personal data is processed by Facebook before individuals are informed as to its collection and even where they do not join (and thereby ‘accept’ Facebook service terms and conditions). Facebook is to appeal the decision.

As consumer consciousness matures in Australia, consumers and regulators may avail themselves of ACL provisions to either avoid unfair terms or indeed, entire online contracts if they are rendered inoperable by severance. This is in addition to any complementary action pleaded under misleading or deceptive conduct or (less likely) unconscionability, as briefly outlined above. It is useful to examine some international cases, to better envisage consumer law possibilities.

4.3. OBA cases and case scenarios

As there are no consumer or privacy law cases concerning OBA³³¹ in Australia, this section selects a miscellany of examples from various jurisdictions to show the type of litigation which regulators and consumers are starting to institute. It is not suggested that these cases constitute a coherent body of law, or that the matters would be decided the same way in Australia; rather that these cases are interesting, illustrative and possibly, predictive of potential Australian OBA cases in the future.

In 2012, the US Federal Trade Commission (FTC) took action against Facebook³³² which resulted in an order which prohibits misrepresentation as to the extent to which the privacy and security of user information is maintained.³³³ The settlement imposed onerous privacy compliance obligations to prevent third party access to information once deleted³³⁴ and to clearly and prominently disclose (outside its policies) the categories of non-public user information it would disclose to third parties

³²⁴ ACL section 23(2).

³²⁵ EMSOC & SPION, ‘From social media service to advertising network’, *Draft Report on Facebook* (31 March 2015, accessed 13 Apr 2015) <<https://www.law.kuleuven.be/icri/en/news/item/facebook-revised-policies-and-terms-v1-2.pdf>>.:25 [fn 63]. The Report also concludes Facebook breaches Article 5(3) of the *e-Privacy Directive* as to obtaining free, specific, informed and unambiguous/explicit prior consent for users (despite high-level disclosure) and tracks non-users improperly: page12. Facebook has acknowledged that it had the capacity (in error) to track ‘non-users’ but denies it was actually doing so: EC, “Cookies” (undated, accessed 10 Apr 2015) <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm>. Article 5(3) requires prior informed, specific, freely given consent for storage of or access to information stored on a user’s terminal equipment as follows – “Art 5(3): Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”

³²⁶ Others cited include liability limitations, indemnities, unilateral variation, forum, choice of law and termination. The report read as if this list was not exhaustive. Note the discussion as to the German unfair terms case in part 4.3 below.

³²⁷ As to the recommendations, see Commission for the Protection of Privacy, Recommendation No. 04/2015 dated 13 May 2015 (13 May 2015, accessed 4 Sept 2015) <http://www.privacycommission.be/sites/privacycommission/files/documents/recommendation_04_2015_0.pdf>. A second recommendation was foreshadowed later in 2015 but may be forestalled given the legal issues yet to be determined.

³²⁸ ‘OSN’ means online social network: EMSOC, above n 325: 6.

³²⁹ MSOC, above n 325.

³³⁰ EMSOC, above n 325: 9–10. The decision is available here: *Belgian Commission for the Protection of Privacy v Facebook Inc., Facebook Belgium SPRL, Facebook Ireland Limited*, Divisional Court 222 (9 Nov 2015 accessed 4 Jan 2016) <<https://www.privacycommission.be/en/news/judgment-facebook-case>>.

³³¹ See *Google Inc. v Australian Competition and Consumer Commission* [2013] HCA 1 discussed above n 294.

³³² The complaint alleges deceptive privacy settings, deceptive privacy changes; deceptive app access, deceptive sharing with advertisers, deception as to verified app security; deception as to photo and video deletion and deceptive representations as to Safe Harbour compliance.

³³³ This is defined as ‘covered information’ which refers to that from or about an individual consumer including, but not limited to: (a) first name and last name; (b) a home or other physical address including street name of city or town; (c) an email address or other online contact information; (e) photos and videos; (f) Internet protocol (“IP” address), User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above: *In the Matter of Facebook Inc.*, Docket No. C-4365 Decision and Order.

³³⁴ Or the user account is terminated.

(i.e. apps), the identity or category of such third parties, and state if such sharing exceeds the restrictions imposed by the privacy settings in effect for the user and if so, to obtain the user's express consent.³³⁵ The complaint raised OBA issues insofar as Facebook allegedly enabled targeted advertising by sharing users who met targeted 'traits' contrary to its numerous statements and policies such as ". . . we do not give your information to advertisers".³³⁶ Clearly, on these facts, the case could have been pleaded in Australia in misleading and deceptive conduct.

The US FTC has been active using consumer and privacy law in a wide range of interesting OBA-related situations: in 2014, social network *Path* deceived consumers by accessing mobile phone address book data in breach of its privacy policy³³⁷; and *Goldenshores Technologies* were sued for data misuse and deceiving consumers when its popular flashlight app secretly shared user location and unique device identifiers to third parties including ad networks, and deceived consumers by providing a fake option not to share their data.³³⁸ Ad companies are also in the FTC sights: video advertising network³³⁹ *ScanScout* was investigated and orders agreed³⁴⁰ for representing to consumers that it allowed a cookie 'opt out' when it actually continued tracking using flash cookies³⁴¹; and online advertising network, *Epic Marketplace*, allegedly used "history sniffing" tracking technology to track millions of consumers browsing the web for OBA purposes. The technology used could "sniff" website browsing history across a range of sensitive subjects such as fertility, menopause, impotence, incontinence, bankruptcy and so on – to enable targeted advertising based upon those visits. This illustrates how, contrary to Australian industry representations, sensitive

health information is inferable from website browsing³⁴² and is tracked and used in an OBA context. The case settled with consent orders including a prohibition upon *Epic* continuing to use the technology and its agreement to destroy all data collected, as well as a bar upon any further misrepresentations as to their data privacy, confidentiality and data storage practices, or as to the technical aspects of tracking. Interestingly, the FTC's objection to the activity stemmed more from the breach of *Epic's* online privacy policy which disclosed that it engaged in information collection across its own 45,000 strong ad network – but the history sniffing technology went beyond that to include thousands of other non-network sites. Data brokers are also in the FTC sights: in May 2014, an extensive self-initiated investigation into the industry was handed down³⁴³ and in late 2014, the FTC alleged that *Leaplab*³⁴⁴ bought payday loan application documentation containing extensive personal information, which it then (without consumer consent and in breach of the loan documentation terms) on-sold to marketers, data broking entities who aggregated and on-sold the data³⁴⁵ and an alleged scam finance company. It is alleged this breached section 5(a) of the FTC Act³⁴⁶ which prohibits unfair³⁴⁷ or deceptive acts in or affecting commerce. The litigation continues, and if successful, illustrates that data brokers and other information-gatherers may supply private information illegally into the marketplace, which expand existing databases and filter into use by the OBA industry and others.

³³⁵ Above n 333: sections II and III.

³³⁶ Above n 333: Count 5 page 11. The 'traits' included location, age, sex, birthday, interested in (whichever sex); relationship status; likes and interests, education and employer name. It is alleged that if a user clicked on a platform ad, his/her User ID was shared with the advertiser, which enabled the advertiser to access the user's profile page, combine the user's real name with targeted traits and information as to the user's visit to the advertiser's website.

³³⁷ *United States of America v Path, Inc.* FTC Matter/File No. 122 3158 (1 Feb 2013) <<https://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc>>.

³³⁸ *In the Matter of Goldenshores Technologies, LLC, and Erik M. Geidl* FTC Matter/File No 132 3087 (9 Apr 2014) <<https://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter>>. The settlement order contained substantial compliance, disclosure, express consent and technical requirements to overcome the deceptive misrepresentations.

³³⁹ As an ad network provider, *ScanScout* is an intermediary between web publishers, from whom it buys advertising space, and advertisers, with whom it contracts to fill that space with video ads.

³⁴⁰ The orders prohibit any misrepresentations as to their data collection practices or consumer' control over them, and required a prominent website notice with hyperlink connected to a one-click user opt out mechanism, which link also appears in its video advertising and any OBA it may conduct. There are also provisions as to complaint management and embedding corporate compliance and record keeping.

³⁴¹ *In the Matter of ScanScout Inc., No. C-4344 F.T.C. Matter/File No. 102 3185* (21 Dec 2011) <<https://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter>>.

³⁴² Brian Merchant, 'Looking up symptoms online? These companies are tracking you' (23 Feb 2015, accessed 13 Apr 2015) <<http://motherboard.vice.com/read/looking-up-symptoms-online-these-companies-are-collecting-your-data>>. See also his article on an unrelated but equally controversial area of tracking: Merchant, Brian, 'Your porn is watching you', *Motherboard* (6 April 2015, accessed 13 Apr 2015) <<http://motherboard.vice.com/read/your-porn-is-watching-you>>.

³⁴³ FTC, 'Data Brokers: A Call for Transparency & Accountability' (May 2014, accessed 4 Apr 2015) <<https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>>.

³⁴⁴ *FTC v Sitesearch Corporation, doing business as LeapLab, formerly LeapLab Corporation, a Nevada corporation; LeapLab, LLC, formerly DirectROI, LLC, an Arizona limited liability company; Leads Company, LLC, a Nevada limited liability company; and John Ayers, an individual* (United States District Court for the District of Arizona, Phoenix Division) FTC Matter/File No: 142 3192 (23 Dec 2014) <<https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf>>.

³⁴⁵ Only 5% were sold to online lenders; the rest were sold at 50 cents each for marketing purposes. These applications contained name, address, phone number, bank account and social security numbers and employer.

³⁴⁶ 15 USC §45A which entitles the FTC to seek injunctions, rescission, reformation of contract, refunds and disgorgement of "ill-gotten monies". See also the related case of *FTC v Sequoia One LLC & Ors*, Case No. 2:15-cv-01512, US District Court of Nevada, filed 7 August 2015, where proposed settlement orders as at August 2015 against three defendants included a prohibition upon them from selling or benefitting from personal information obtained, plus judgments of \$7.1 million against two defendants and \$3.7 million against the third.

³⁴⁷ Acts or practices are "unfair" if they cause substantial injury to consumers that they cannot reasonably avoid themselves and that is not outweighed by countervailing benefits or competition: *Leaplab*, above n 344: para 43.

Unfair terms cases have also arisen in Europe. In 2014, the Berlin District Court held that 25 terms in Google's online *Terms of Use* and its *Privacy Statement* are unenforceable.³⁴⁸ *In re Google, Inc.*³⁴⁹ is significant in several respects; firstly, the court found that the consent to terms upon registration creates a legally enforceable contract – whereas Google had (ironically) argued that as its services are 'free', there is no valid contract. The court very practically found that the requirement to consent to terms upon registration meant that there is an exchange for value, as Google obtains the registrant's commercially-valuable personal data for marketing purposes.³⁵⁰ Secondly, the court found that Google contract terms were unfair³⁵¹ and thirdly, held that ticking a consent box was not valid consent³⁵² for privacy purposes. Google's argument raises an important issue in the online consent/OBA debate. Consumers are repeatedly told by the industry and others that online advertising supports free Internet services, but some academics are starting to dispute this characterisation. Hoofnagle for example, contends that 'free' online web or social media services are not really 'free' at all because personal information is valuable³⁵³ and tradeable.³⁵⁴ Economically, personal information is a unique consumer asset in a transactional cost sense, which in registering on a website or in signing up for Facebook, is exchanged in a bilateral, dependent trading relationship online. Economists argue that consumers bear transaction costs: they are subject to profound information asymmetry³⁵⁵ and bounded

rationality³⁵⁶ in online contracting, and bear burdens such as targeted marketing and identity theft, and transferred costs such as time, effort or money to reduce OBA impacts.³⁵⁷ Risks are also transferred in cases of data breach and misuse, or where personal data is disclosed to or traded with entities with little interest or obligation to observe consumer information use and privacy preferences.³⁵⁸ It is the author's view that the same approach should be taken in Australia with respect to online contract validity and whether or not online 'free' website or social media services are provided "in trade or commerce" under the ACL.³⁵⁹ Clearly, the collection and use of consumer data for OBA and other purposes is a dominant trading activity of entities such as Google and Facebook.³⁶⁰ There seems little doubt that online contractual dealings with consumers bear a commercial character³⁶¹ where selling paid services, and based upon the German case, the same applies given the 'business activity' of obtaining consumer information for OBA use or with the intention of advertising or creating saleable data sets as to such people³⁶² via so-called 'free' service offerings.³⁶³ Had Google succeeded in its argument, a very difficult precedent would have been set in terms of the validity of online consent and terms generally; indeed, it is difficult to see why Google would want such an argument to succeed (save for success in the instant) given its potential overall implications for their business.

³⁴⁸ Note that the German unfair contract terms legislation specifies that terms which conflict with the "main elements of German law and unfairly disadvantage consumers" are invalid. Google will appeal the application of this clause, arguing that the legislation cited is limited to organisations established in Germany or which use equipment in Germany.

³⁴⁹ *In re Google, Inc.*, LG Berlin, No. 15 O 402/12, 11/19/13. There is no English translation of this case available on the Internet. As such, this discussion is reliant upon secondary sources.

³⁵⁰ Karin Retzer 'German Court Finds 25 Provisions in Google's Online Terms of Use and Privacy Policy to Be Unenforceable'. *Morrison & Foerster LLP* (20 Dec 2013, accessed 10 Aug 2014) <<https://www.jdsupra.com/legalnews/german-court-finds-25-provisions-in-goog-45359/>>.

³⁵¹ These were the unilateral termination, the monitoring of content for policy compliance, unilateral alteration of service; variation to terms of use without consent and the (mutual) limitation for liability as to statutory product liabilities. Note that on 13 May 2014, the Norwegian Consumer Council filed a complaint against Apple with their consumer ombudsman alleging a violation of European consumer unfair terms law as to a clause permitting unilateral variation without notice in the *Apple iCloud terms and conditions*. Commentators suggest that this case will succeed, as it would be likely to do were it brought in Australia under the unfair terms regime.

³⁵² Spain and Germany are threatening financial sanctions because the privacy terms fail to comply with their privacy laws: Loeb Essers, 'Berlin court rules Google privacy policy violates data protection law' (20 Nov 2013, accessed 10 Aug 2014) <<http://www.cio.com/article/2380759/legal/berlin-court-rules-google-privacy-policy-violates-data-protection-law.html>>.

³⁵³ Chris Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price', 61 *UCLA Law Rev* 606 (2013–2014, accessed 10 Apr 2015) [633] <<http://www.uclalawreview.org/pdf/61-3-2.pdf>>.

³⁵⁴ *Ibid.*

³⁵⁵ Above n 27.

³⁵⁶ This proposes that all decision-makers work within three constraints: (1) limited and often unreliable information as to possible alternatives and their consequences; (2) the limited capacity of the human mind to evaluate and process the available information; and (3) the limited time available to make a decision. "... Therefore even individuals who intend to make rational choices are bound to make satisficing (rather than maximizing or optimizing) choices in complex situations. These limits (bounds) on rationality also make it nearly impossible to draw up contracts that cover every contingency": Business *Dictionary.com*, 'Bounded Rationality' (undated, accessed 10 Apr 2015) <<http://www.businessdictionary.com/definition/bounded-rationality.html>>.

³⁵⁷ Hoofnagle above n 353: 625.

³⁵⁸ Hoofnagle above n 353.

³⁵⁹ The ACL definition includes "any business or professional activity whether or not carried on for profit": ACL s 2.

³⁶⁰ See the detailed discussion as to how information is monetised by Facebook in Hoofnagle, above n 353: 630–634.

³⁶¹ *Hearn v Rourke* [2003] FCAFC 78 per Dowsett J, the focus must be on the conduct in question – which on the facts of *In re Google* included the terms enabling the commercial use of the consumer information.

³⁶² A similar though not analogous fact situation is solicitation by mail for subscribers for UK books etc, which conduct was held to be "in trade or commerce": *Swan v Downes* (1978) 34 FLR 36 c/f *E v Australia Red Cross Society* (1991) 27 FCR 310 where the provision of free blood was held not to be "in trade or commerce".

³⁶³ An extension of the argument might be to suggest that promoting such services as "free" breaches ACL section 18 insofar as while there is no apparent cost, the consumer is supplying data which has commercial value to other party. This would be an unlikely extension to the law (which tends to focus directly upon the representation with respect to whether a consumer must pay or lose money directly in some way) but would more realistically reflect the exchange between the parties – and seems open on the reasoning of the German case.

Google is also central to US and UK OBA cases concerning the infamous Safari 'workaround'.³⁶⁴ In 2012, Google paid a civil penalty of US \$22.5 million to settle FTC proceedings alleging that it had misrepresented to Apple Safari users in its Privacy Policy that it would not place tracking cookies on their browser or serve targeted advertising to them. In 2013, Google settled 37 US state-initiated³⁶⁵ consumer-based actions for US\$17 million. The plaintiffs alleged "...secret and blanket tracking and collation of information, often of an extremely private nature³⁶⁶ ... about and associated with the claimant's internet use."³⁶⁷ The court found that Google was tracking their private information (as to their internet usage) without their knowledge or consent and provided that information to advertisers via its 'doubleclick' service. The advertisers then targeted ads to the plaintiff's deduced interests, which were displayed on their devices and revealed private information about them, which may have been seen by third parties. The claim succeeded at first instance and before the Court of Appeal, based upon the tort of misuse of private information,³⁶⁸ breach of confidence³⁶⁹ and breach of the UK *Data Protection Act*.³⁷⁰ Interestingly for the interpretation of the Australian privacy legislation, the court also found that there is a serious case to answer as to whether non-personal behavioural data information could become 'personal' if Google (as 'data controller') had other information which it could use to identify the claimant from browser-generated information in its possession – *whether or not it actually did so*. Arguably, the Australian definition of 'personal information' is broader than that in the UK legislation, focussing on whether the individual is 'reasonably identifiable' (regardless of method).

³⁶⁴ Google placed cookies on Safari browsers to collect what the court calls 'browser-generated information' (BG) which it then aggregated and used in its commercial 'DoubleClick' advertising service to enable OBA. It is alleged that this revealed private information about the claimants which others may have seen: *Google Inc. v Judith Vidal-Hall and others* (2015) EWCA Civ 311, 27 March 2015 [para. 3].

³⁶⁵ 37 State Attorneys and the District of Columbia undertook a representative proceeding.

³⁶⁶ The claimants submitted confidential documentation to the court in this regard, but their statement of claim also alleges that as a result of Google placing a *DoubleClick* cookie on their browser (after an *Intermediary* cookie was first installed via a completed form) which worked around Safari's default privacy settings, Google was able to and did obtain information as to user interests, hobbies, pastimes, news reading and shopping habits, social class, racial or ethnic origin, political affiliation or opinion, religious or similar beliefs, trade union membership, physical and mental health, sexuality and interests, age, gender, financial situation and geographic location: above n 364: *General Particulars of Claim* para 7.5.

³⁶⁷ Above n 364 [para 137].

³⁶⁸ This issue was relevant to determining if the plaintiffs could serve Google out of the jurisdiction in California.

³⁶⁹ The confidence arose as Google allegedly acquired information by unlawful or surreptitious means, which it should have known it ought not to breach through use.

³⁷⁰ The claimants sought damages for anxiety and distress due to damage to their personal dignity, autonomy and integrity, but did not seek pecuniary loss. In August 2015, the Supreme Court granted Google leave to appeal.

Since 2012, Facebook has paid out over US\$30 million to settle privacy-related law suits,³⁷¹ and faces a current class action³⁷² alleging that it systematically intercepts 'private' Facebook message content and metadata to mine user data³⁷³ and profits from it by sharing it with "advertisers, marketers and other data aggregators".³⁷⁴ The claim alleges that the Facebook *Statement of Rights and Responsibilities and Privacy Policy* (which hyperlink to the *Data Use Policy*) do not disclose its practices as to private message mining and violate Californian privacy and competition laws.³⁷⁵ These allegations could as readily apply in Australia under section 18.

These cases illustrate that inappropriate OBA data gathering and disclosure practices are often misleading and deceptive and may be actioned as such by regulators, which generates a beneficial outcome to consumers both as to future privacy protection, and increased informational accuracy and fairness. They also serve an important industry educative function. Given significant US and European interest in this area and the tendency of the ACCC to follow suit,³⁷⁶ it is quite possible that the ACCC may consider action within the OBA sphere in the near future.³⁷⁷

³⁷¹ Pat McGrath, 'Facebook alleged to have sold information in user's private messages' *ABC News* (3 Jan 2014, accessed 15 Apr 2015) <<http://www.abc.net.au/news/2014-01-03/facebook-sued-for-selling-information-in-users-private-messages/5183904>>.

³⁷² *Campbell & Hurley et al. v Facebook Inc.* Case No 5:2013cv05996 (filed 30 Dec 2013) <<http://dockets.justia.com/docket/california/candce/5:2013cv05996/273216>>.

³⁷³ The allegation is that Facebook scans private messages for third party links, follows those and uses the information from that link to add to user profiles for OBA purposes. The 'motive' might be that private messages are believed to be just that, and users may include more intimate information which they would not otherwise post publicly.

³⁷⁴ *Ibid.*

³⁷⁵ *Electronics Communications Privacy Act* 18 U.S.C. §§2510 et seq; *Invasion of Privacy Act* Cal. Penal Code §§ 630, et seq; *Unfair Competition Law Business and Professions Code* § 17200 et seq.

³⁷⁶ The ACCC is watching the EU case against Google closely, but Chairman Rod Simms observed that they are happy to allow larger regulators to take the lead in such cases. The author notes, however, that the ACCC often sets its priorities based upon recent actions of the FTC in particular. The instance of fake online reviews is one such example.

³⁷⁷ The ACCC has recently conducted a limited audit of various industry terms and conditions, which resulted in many companies changing their documentation by consent: ACCC, 'Unfair Contract Terms – Industry Review' (2013, accessed 14 July 2014) <<http://www.accc.gov.au/publications/unfair-contract-terms>>. This is a far less expensive form of regulatory activity and potentially achieves useful results in terms of targeting the bigger players, protecting a greater number of consumers, improving industry standards and sending out a message across the industry.

5. Industry solutions: codes, guidelines and technology – not law

*Meaningful self-regulation requires the constant re-evaluation of new technologies, new business models, and new policy developments. . .*³⁷⁸

Part 4 reveals that while Australian consumer and privacy laws are aligned in intent as to OBA, regulatory activity is not so in practice. Further, this section reveals that the OBA industry is reluctant to highlight its activities or to engage more fully, to ensure that regulation, voluntary self-regulatory behaviours and industry practices are complementary. The continued consumer-unfriendly use of intimidating privacy or ‘tracking’ statements, one-sided terms and conditions, poor online ‘consent’ information and opt-out facilities – and a badly drafted self-regulatory guideline – all suggest an industry in hiding.

5.1. The OBA guideline

*The key to industry self-regulation is rigorous compliance efforts, tough enforcement and accountability. . .*³⁷⁹

There are over 35 regulated areas in Australia with direct application to online advertising content³⁸⁰; of these, only the ADAA’s³⁸¹ OBA Guideline impacts upon OBA practices directly. The OBA Guideline scope has already been criticised in part 2 as to its limited application. As this part reveals, it also has little practical implementation or compliance content.³⁸² This is a serious practical issue and is in contrast to the European

³⁷⁸ Network Advertising Initiative (NAI) ‘How Self-Regulation Works’ (undated, accessed 18 Mar 2015) <<https://www.networkadvertising.org/about-nai/about-nai>>. The NAI describes itself as ‘. . . the organization for third-party online advertising technology companies, including networks, exchanges, DMPs, SSPs, RTB platforms, analytics companies, and service providers.’

³⁷⁹ Ibid.

³⁸⁰ The author regards the regulation of advertising content in Australia to be best practice. The industry has consistently ‘kept up’ with legal and consumer attitudes and have established world class bodies and best practice disputes resolution.

³⁸¹ Founding members of the ADAA are: The Australian Association of National Advertisers (AANA), the Australian Direct Marketing Association (ADMA), the Australian Interactive Media Industry Association (AIMIA), The Communications Council (TCC), the Australian Interactive Advertising Bureau (IAB), The Media Federation of Australia (MFA), The Internet Industry Association (IIA), Google, Microsoft, NineMSN, Sensis Digital Media, Digital Ten and Yahoo!7: ADAA, Your Online Choices (undated, accessed 10 Apr 2015) <<http://www.youronlinechoices.com.au/about-adaa>>.

³⁸² These are: Adconian, Fairfax Digital, Google, Microsoft, News Digital Media, NineMSN, realestate.com.au, Sensis Digital Media, Digital Ten and Yahoo!7: Ibid. Notable absences include social media companies such as Facebook, although it appears to be a signatory to the US and EU versions. After contacting IAB Australia (as the Guideline administrator) with queries, the website was updated to indicate there were 16 members: Radium One, Amobee, Fairfax Digital, Google, Microsoft, News Corp Australia, NineMSN, Mi9, REA, Telstra Advertising Network, Network Ten Digital, Eyeota, Adobe, Xaxis, Carsales Network and Yahoo!7: ADAA, Your Online Choices (undated, accessed 16 Apr 2015) <<http://www.youronlinechoices.com.au/about-adaa>>.

equivalent, which has a clear implementation framework³⁸³ designed to build upon the guideline principles to compliance the “entire advertising ecosystem”.³⁸⁴ Their Recommendation commits national advertising self-regulatory bodies to “. . . applying self-regulatory standards for OBA, integrating the principles of the recommendation into their Codes, and handling complaints. . .”³⁸⁵ In 2011, upon the Australian Guideline introduction,³⁸⁶ an IAB forum indicated that an external privacy consultant would assist in the complaints handling framework development process, adoption of the international OBA ‘icon’ would be reviewed and consultation with consumer groups would occur in “Q3 2011” – but none of these processes occurred or remain on the IAB/ADAA public agenda in 2015.³⁸⁷ The result is that Australia has no OBA compliance implementation processes or guidance for industry or consumers – which is where the OBA audit trail ends and where the OBA Guideline corporate compliance regime fails.

The Australian OBA Guideline is weak and poorly formulated – compared to other industry self-regulatory codes in Australia, particularly in the area of advertising content. It is evaluated by reference to the Australian Self-Regulation Best Practice model in Annexure 1.³⁸⁸ As the evaluation reveals, the Guideline establishes seven self-regulatory principles to which signatories voluntarily commit and is designed to enable the deployment of OBA in a way which “promotes and maintains consumer confidence”.³⁸⁹ That claim includes the fostering of “transparency, knowledge and choice for consumers” through the application of “consumer-friendly standards”.³⁹⁰ This objective is backed by minimal compliance, validation and consumer complaints management provisions under Principle VII Accountability. The Guideline prescribes ongoing reviews and reporting of complaints, but without structure, rules, time limits or transparency. If these occur, no information is publicly available. As such, the Guideline has serious transparency weaknesses. Nor does it prescribe consumer redress or

³⁸³ Under the EASA ‘Best Practice Recommendation on Online Behavioural Advertising’, implementation is prescribed through ‘The Technical Specifications for implementing the IAB Europe OBA Framework and EASA BPR in Europe’ and the compliance-based, Self-Certification Criteria for Participating Companies: IAB (Europe), ‘Technical Specifications for implementing the IAB Europe OBA framework’ (30 Jan 2012, accessed 10 Apr 2015) <http://www.iabeurope.eu/files/1113/6991/5494/technical_specifications_for_iab_eu_OBA_fw_v1.pdf>; EDAA, ‘Self-Certification Criteria for Participating Companies’ (16 Nov 2012, accessed 12 Apr 2015) <<http://www.edaa.eu/wp-content/uploads/2012/10/self-certification-criteria-final-v1.1.pdf>>.

³⁸⁴ <<http://www.edaa.eu/european-principles/>>.

³⁸⁵ Ibid.

³⁸⁶ “The Australian [OBA] Guideline . . . is an important first step on the road to implementing a comprehensive self-regulatory scheme. . .”: ADAA, ‘Youronlinechoices website’ (undated, accessed 12 Apr 2015) <<http://www.youronlinechoices.com.au/about-adaa>>.

³⁸⁷ IAB, Online Behavioral Advertising Forum (2011, accessed 15 Apr 2015) <https://www.iabaaustralia.com.au/uploads/uploads/2013-10/1382569200_c4744acad99817803505534365bd0139.pdf>.

³⁸⁸ Australian Government Taskforce on Industry Self-Regulation, ‘Industry Self-Regulation in Consumer markets – Final Report’ (1 Aug 2000, accessed 28 Feb 2015) <<http://archive.treasury.gov.au/documents/1131/PDF/2part1.pdf>>.

³⁸⁹ OBA Guideline above n 64:2.

³⁹⁰ OBA Guideline above n 64:3.

sanctions. It also succeeds in few respects in terms of a consumer communication: it is very difficult to read and understand, lacks transparency in places, lacks accountability to consumers, refers consumers to signatory complaints schemes without delineating a process or appeals options, contains no industry redress or sanction requirements and contains little reference to procedural or other fairness to consumers.

On the positive, it does establish certain specific circumstances within which signatories are obliged to provide website notices as to their OBA practices (Principle II.A.1.), and absent 'Explicit Consent' from web users as to information collection and use, are obliged to provide 'Enhanced Notice' (Principle II.A.2: for example, an AdChoice link with additional disclosure) plus the requirements to obtain prior Express Consent for sensitive information categories prior to the OBA use. As all of these instances relate to 'non-personal' information collection, they would not otherwise be covered by the *Privacy Act* provisions. It should however take a more prescriptive approach and implement compliance requirements beyond self-validation and undefined self-certification. Both are serious weaknesses in terms of independence, efficiency and effectiveness.

In addition to the matters identified above, the **part 2** discussion reveals the limited scope of defined OBA, which restricts the application of the *Guideline* and reduces consumer redress as to OBA generally. As a minimum, it would be desirable that first party OBA and other presently-excluded practices be included, if only to insert some form of self-regulatory regime over the compliance attributes required to prevent privacy laws being activated in those areas. There would also be value in the industry incorporating the *Privacy Act* compliance requirements within its *Guidelines* and using the section 35A system whereby the Commissioner can officially recognise an industry external dispute resolution scheme for *Privacy Act* purposes.³⁹¹ This would overcome the present division between *Guideline* and *Act* obligations, reduce signatory obligations and control over complaints resolution processes and simplify the regime to a "one-stop shop" for consumers.³⁹²

A new iteration of the *OBA Guideline* is pending, but after a non-independent and undisclosed industry review, no material changes are envisaged.³⁹³ Given the lack of consumer complaint or regulatory oversight, that outcome was perhaps predictable – from an industry perspective.

³⁹¹ To be recognised, under section 35A(2)(a)–(g) a scheme must demonstrate the DIST Benchmarks of accessibility, independence, fairness, accountability, efficiency and effectiveness, as well as additional *Privacy Act* accountability, reporting and regular reviews requirements: OAIC, 'Guidelines for recognising external dispute resolution schemes under section 35A of the *Privacy Act*' (Sept 2013, accessed 9 Apr 2015) [2] <http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/advisory-privacy-guidelines-and-rules/Guidelines_for_recognising_external_dispute_resolution_schemes.pdf>.

³⁹² Above n 388: 37. Page references are taken from Chapter 8.

³⁹³ Interview with Ms Daad Soufi.

5.2. Industry solutions: not selling hard enough

*Imagining a world where HTTP cookies were never invented. . .*³⁹⁴

There are five broad approaches currently deployed by the industry to improve consumer choice and awareness of OBA, none of which are particularly effective or usefully implemented in Australia.

5.2.1. Opt out website and tool

YourOnlineChoices.com.au contains an online 'opt out' tool enabling consumers to notify certain *OBA Guideline* signatories that they do not wish to be subject to their OBA activity.³⁹⁵ Overseas industry equivalents are superior in terms of appearance, functionality and offerings; they also include an assessment tool to identify which of the signatories tracks the user, which is transparent disclosure as to the extent of tracking³⁹⁶ and arguably, a strong incentive to opt out choices. The US *Network Advertising Initiative* (NAI) website is best practice in terms of appearance and ease of use.³⁹⁷ In contrast, the Australian website is best described as old fashioned and "clunky" in operation³⁹⁸; it presents only industry 'pro' OBA information and is arguably arranged to discourage consumers from opting out.³⁹⁹ It lacks an assessment tool to identify which of the signatories tracks the user, and its opt out tool technology is slow

³⁹⁴ The Future of the Cookie Working group seeks to "re-imagine" the technology in a way that "promotes greater persistence of both identity and consumer choice". Its starting point is this quote. IAB (US), above n 106.

³⁹⁵ Facebook advice on this is as follows: "People can opt out of seeing ads on Facebook that are based on the websites and apps they use off Facebook through the industry-standard Digital Advertising Alliance opt out, the European Interactive Digital Advertising Alliance opt out or the Digital Advertising Alliance of Canada opt out. Here, they can opt out of these ads from Facebook and from more than a hundred other companies. People can also opt out using their phone settings": Richard Allan, 'Setting the Record Straight on a Belgian Academic Report' (8 April 2015, accessed 12 A3 April 2015) <<http://newsroom.fb.com/news/h/setting-the-record-straight-on-a-belgian-academic-report/>>. Note that Facebook is not a signatory to the Australian OBA *Guideline* nor is it listed for opt-out.

³⁹⁶ The author's computer was being tracked by 52 ad network companies in the UK system: <<http://www.youronlinechoices.com/uk/your-ad-choices>>; and 72 of 94 US *Network Advertising Initiative* members had set cookies on my browser: <<http://www.networkadvertising.org/choices/#completed>>.

³⁹⁷ See <<http://www.networkadvertising.org/choices/>>. Note that each webpage has an icon which takes consumers straight to the opt out tool. This is far more consumer-friendly than other opt out websites. The tool also works with Internet Explorer and is fast and simple to use.

³⁹⁸ For example, some links go to pages which appear to have no text, until the user scrolls half a page down- and there it is.

³⁹⁹ For example, there is no main link to the opt-out tool; it is accessed via small hyperlinks on pages amidst text.

and incompatible with major browsers such as Internet Explorer – which is not disclosed to users.⁴⁰⁰

While an opt-out service is potentially positive in terms of enhanced user choice and control, there are five points of concern from a consumer perspective. Firstly, it is piecemeal; the system is limited to industry ‘signatories’ who commit to the process only – although many large players are included.⁴⁰¹ UK estimates are that 70% only are captured,⁴⁰² which, given the constantly expanding scope and scale of the industry, means that consumers will still be exposed to a significant amount of tracking if they do not take additional technical measures to prevent it – and that preventative action is an ongoing and updatable requirement. Secondly, the ‘opt out’ and additional remedial measures are required for every device which a consumer uses. Thirdly, the opt-out system is not without technical issues – and a user who opts out, then deletes all cookies later, may have to opt out again.⁴⁰³ Fourthly, most experts also recommend further self-initiated steps to effectively block OBA: browser control⁴⁰⁴ plus an add-on or extension⁴⁰⁵ should be installed.⁴⁰⁶ Finally, signatories can covertly rort the opt-out system itself: somewhat ironically, Facebook has been accused⁴⁰⁷ of setting a tracking cookie⁴⁰⁸ via

the European OBA opt-out site.⁴⁰⁹ In other words, Facebook was allegedly tracking the very people who were there expressly to opt-out.

5.2.2. Icons, audit and information

The EDAA and US/Canadian DAA also use an advertising option icon or trust mark (*Adchoices* or *Cookie Consent*) for industry participants who adhere to the *Self-Regulatory Program for Online Behavioral Advertising* to better inform consumers and to evidence compliance certification⁴¹⁰ through TRUSTe⁴¹¹ or Ghostery.⁴¹² The icon links to a privacy notice which reveals which companies are collecting and/or using OBA data on the website visited, and links to the opt-out option. The EU website notice provides an ‘opt-in’ tracking consent, as required under *ePrivacy Directive*. As previously indicated, the Australian industry has not adopted this system.⁴¹³

5.2.3. Do Not Track (DNT)⁴¹⁴

In recent years, browser providers such as *Safari* and *Firefox* implemented DNT as a default browser setting, which at that

⁴⁰⁰ The author uses Internet Explorer (as do around 22% of all Australians) and patiently waited over 20 minutes for the tool to load, which it appeared to be doing. The IAB have since informed me that it does not work with IE (or some other browsers), but there is no notice of this on the tool page nor on the ‘Help’ page – which directs users to external cookie browser control links. It does, however, work with Google Chrome which is used by around 49% of Australians: Clicky Web Analytics, ‘Web Browsers’ (20 Apr 2015, accessed 20 Apr 2015) <<https://clicky.com/marketshare/au/web-browsers/>>.

⁴⁰¹ Australian participants are: A-mo-bee, Adobe, Carsalesnetwork, eyeota, Fairfax Media, Google, Microsoft, M9, Newscorp, Nine msm, radium one, realestate.com, Telstra, Ten, Xaxis, Yahoo!?: <<http://www.youronlinechoices.com.au/>>.

⁴⁰² Nicole Kobie, ‘Why the cookies law wasn’t fully baked – and how to avoid being tracked online’, *The Guardian* (19 Mar 2015, accessed 10 Apr 2015) <<http://www.theguardian.com/technology/2015/mar/19/cookies-how-to-avoid-being-tracked-online>>.

⁴⁰³ IAB (UK), ‘Your Online Choices: What do I need to know and why?’ (undated, accessed 13 Apr 2015) <<http://www.globalmediapolicy.net/sites/default/files/Consumer-guide-to-online-behavioural-advertising.pdf>>.

⁴⁰⁴ This only works against 70% of cookies.

⁴⁰⁵ For example, *Ghostery*, *Disconnect* or *Adblock Plus*.

⁴⁰⁶ This shows users what trackers are on each page, what their ‘purpose’ is and to allow selective consumer blocking of tracking. For example, whether it has a useful functional purpose such as enabling a website twitter feed versus a tracking function.

⁴⁰⁷ EMSOC, above n 325. See also Güneş Acar, Brendan Van Elsenoy et al., ‘Facebook tracking through social plug-ins’, *Technical Report prepared for the Belgian Privacy Commission* (27 Mar 2015, accessed 10 Apr 2015) <https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf>.

⁴⁰⁸ Described as “a long-term, uniquely identifying cookie”: *Ibid.*

⁴⁰⁹ This means that “. . . all later visits to Facebook social plug-ins [for example, the ‘like’ button] can be linked by Facebook using this cookie. . .” Facebook disputes this constitutes ‘tracking’. However, the Report alleges this conduct breaches article 5(3) of the *ePrivacy Directive* as to a lack of free and informed prior consent and tracking. The Belgian Commissioner is to announce its actions (if any) on 29 April 2015.

⁴¹⁰ In Australia, the compliance standard is presently AS3806: 2006 which is due to be replaced by ISO19600 in the near future. The latter introduces compliance as ‘embedded’ in the organisation’s culture, that is, ‘integrated with the organisation’s quality, risk, financial, environmental and health and safety management processes and its operational procedures and requirements. It defines ‘compliance obligations’ as the requirement or commitments that an organisation has to or chooses to comply with: CompliSpace ‘Compliance Standards ISO 19600 and AS 3806 – differences explained’ (14 Apr 2015, accessed 14 April 2015) <<https://complispace.wordpress.com/2015/04/14/compliance-standards-iso-19600-and-as-3806-differences-explained/>>.

⁴¹¹ The program is called TRUSTed Ads: Audience Science, ‘TRUSTe Now Largest DAA Compliance Solution for Online Behavioral Advertising’ (5 May 2011, accessed 13 Apr 2015) <<http://www.audiencescience.com/truste-now-largest-daa-compliance-solution-for-online-behavioral-advertising/>>.

⁴¹² DAA, Advertising Option Icon (2010, accessed 13 Apr 2015) <<http://www.aboutads.info/participants/icon/>>.

⁴¹³ The interactive trust mark/icon system was a part of a dual pronged strategy: first, the 2010 self-regulatory code which required use of the icon to reveal an ad was served due to OBA targeting; secondly, the icon links to a website with both information and an opt-out option. The EU Article 29 Working Party has criticised the IAB Europe (IABE) and European Advertising Standards Alliance (EASA) codes as inadequate to evidence user consent, relying upon these features alone: *Out-Law.com*, ‘Privacy watchdogs deem advertising code non-compliant with EU cookies laws’ (4 Jan 2012, accessed 10 Apr 2015) <<http://www.out-law.com/en/articles/2012/january-/privacy-watchdogs-deem-advertising-code-non-compliant-with-eu-cookies-laws/>>.

⁴¹⁴ ‘Do Not Track’ uses simple technology to use an http header to signal user opt-out preference: Jonathan Mayer and Arvind Narayanan, ‘Do Not Track’ (undated, accessed 13 Apr 2015) <<http://donottrack.us/>>.

stage, covered 20%⁴¹⁵ of the browser market. The IAB (US) tweeted this was “. . .nothing less than a nuclear first strike against the ad industry. . .”⁴¹⁶ When Microsoft followed suit, the ad industry refused to comply,⁴¹⁷ arguing that consumer choice dictated a deliberate ‘opt out’, not a browser-led default setting to that effect. This argument prevailed,⁴¹⁸ albeit logically, no default is not a deliberate choice to ‘opt in’ either. The story reveals more about OBA industry power trumping consumer interests than anything else, but arguably, DNT as a voluntary system had limited effect anyway.⁴¹⁹

5.2.4. Direct consumer access to correct data

Data giant Acxiom allows consumers an online “access and correct” process. While this is a mutually positive compromise as it offers improved data accuracy for their ongoing use and may enhance consumer control, the process is time-consuming and difficult.⁴²⁰ Further, this option does not resolve the fact that yet again, consumers are joining the dots – finding out who holds their data, then having correct it website-by-website.⁴²¹

⁴¹⁵ Anthony Leather, ‘Google Chrome Browser Market Share Tops 20%: Leaves Firefox In Its Dust’, *Forbes* (4 Aug 2014, accessed 13 Apr 2015) <<http://www.forbes.com/sites/antonyleather/2014/08/04/google-chrome-browser-market-share-tops-20-leaves-firefox-in-its-dust/>>.

⁴¹⁶ Mike Zaneis is the IAB Senior Vice President and General Counsel, so it seems unlikely that this tweet was not a strategic exercise.

⁴¹⁷ Microsoft Internet Explorer and Google Chrome covered 78% of the market and then, allowed third party cookies by default. “The big question is whether Microsoft and Google, the big two companies that depend on online advertising, will follow suit”: Katy Bachman, ‘Ad networks beware: Firefox to block third party cookies’, *Adweek* (2013, accessed 10 Apr 2015) <<http://www.adweek.com/news/technology/ad-networks-beware-firefox-block-third-party-cookies-147513>>. Microsoft did, but met with significant ad industry criticism and indeed, refusal to accede to DNT which is essentially a ‘request’ only.

⁴¹⁸ Microsoft (then with a 58% market share) reversed its decision in April 2015: Microsoft claim their reversal follows the latest World Wide Web consortium (W3C) draft standard which states that tracking preference must reflect deliberate user choice and absent that, “there is no tracking preference expressed”: Brendon Lynch, ‘An update on Microsoft’s approach to Do Not Track’ (3 Apr 2015, accessed 13 Apr 2015) <<http://blogs.microsoft.com/on-the-issues/2015/04/03/an-update-on-microsofts-approach-to-do-not-track/>>. Google Chrome has never offered DNT and now has around 50% of the browser market.

⁴¹⁹ Note that only 21 suppliers are listed in *donotrack.us* website (including Twitter and Pinterest but no other social media site) which if accurate, is a very low participation rate. Lardinois, Frederic, ‘Microsoft Will Remove “Do Not Track” As The Default Setting In Its New Browsers’, *Tech Crunch* (3 Apr 2015, accessed 13 Apr 2015) <<http://techcrunch.com/2015/04/03/microsoft-disables-do-not-track-as-the-default-setting-in-internet-explorer/#.a97fwa:MCnG>>.

⁴²⁰ It requires a sign in process including name, address and social security number and is subject to somewhat draconian (and circular) terms which include their right to market to you, unless you click elsewhere and opt out. The process is very slow and potentially circular in places. See Acxiom, ‘AbouttheData Terms of Use’ (undated, accessed 14 Apr 2015) <<https://www.aboutthedata.com/portal/terms-of-use>> and Acxiom, ‘Privacy Policies’ (undated, accessed 14 Apr 2015) <<http://www.acxiom.com/about-acxiom/privacy/us-consumer-choices/>>.

⁴²¹ <<https://www.aboutthedata.com/>>.

5.2.5. Other consumer browser and software options

Other technological approaches to blocking OBA are essentially browser and software based. In 2012, the US Electronic Frontier Foundation (EFF) recommended four steps to protect against online tracking: firstly, install ad blocking software⁴²²; secondly, go to Security settings and set cookies to automatically expire upon exiting the browser and disallow third party cookies;⁴²³ thirdly, turn off ‘referer’ (sic); and fourthly, install a browser add-on like ‘HTTPS Everywhere’ which maximises ‘secure’ browsing. By 2015, EFF also developed *Privacy Badger* which blocks trackers by default.

5.3. Emerging industry concerns

*Businesses must have a viable way to protect their customers. . . Innovations that have improved the quality of life on a scale not seen since the industrial revolution will be stymied if the digital advertising supply chain is not fixed. . .*⁴²⁴

Recent industry literature suggests that the online advertising industry is starting to question the continued viability of OBA – for reasons such as failing “state management”,⁴²⁵ loss of consumer trust,⁴²⁶ questionable advertising

⁴²² For example, *Adblock Plus*.

⁴²³ In Internet Explorer, for example, users must click the ‘gear’ symbol in the top right hand of the screen, then select Internet Options, then go to the Privacy tab and click ‘Advanced’. Check the box saying ‘Override automatic cookie handling’ and then set the “Third Party Cookies” to “Block”. Similar operation is required in Google Chrome, although Safari and Firefox have third party cookies ‘off’ by default.

⁴²⁴ Randall Rothenberg, “IAB Head: ‘The Digital Advertising Industry Must Stop Having Unprotected Sex’”, *Business Insider* (6 Feb 2014, accessed 9 Apr 2015) <<http://www.businessinsider.com.au/iab-randall-rothenberg-supply-chain-2014-2>>.

⁴²⁵ IAB (US), ‘Privacy and Tracking in a Post Cookie World’, *White Paper* (Jan 2014, accessed 9 Apr 2015) <http://www.iabaustralia.com.au/uploads/uploads/2014-11/1415289600_3ee3de01b67c04945704bce1e7964095.pdf>.

⁴²⁶ A 2014 study of social media advertising effectiveness concluded that consumers were “not responsive” to social media advertising and “. . .most are annoyed by online advertisements in general. . .” Bohdan Pikas & Gabi Sorrentino, ‘The effectiveness of Online Advertising: Consumer’s Perceptions of Ads on Facebook, Twitter and YouTube’, *Journal of Applied Business and Economics* 16(4) (2014, accessed 7 Apr 2015) [80] <<http://search.proquest.com.ezproxy.bond.edu.au/docview/1566175341/fulltextPDF/7D991CB57AD54DBFPQ?accountid=26503>>. That view is supported by Nielsen findings: online advertising is significantly less trusted than personal recommendation and offline media sources. For example, Nielsen’s Global survey (2013) shows trust in TV ads (62%), newspapers (62%), magazines (60%) outdoor ads/radio (57%) have consistently out-ranked online advertising – search (48%), video (58%), social network ads (48%), mobile display ads (45%), online banner ads (42%), and mobile text ads (37%): Nielsen ‘Global survey of trust in advertising’, *The Nielsen Company* (Sept 2013, accessed 4 April 2015) [6] <<http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2013%20reports/nielsen-global-trust-in-advertising-report-september-2013.pdf>>.

efficacy,⁴²⁷ adverse supply chain impacts and damage to brand “trust capital”.⁴²⁸ It seems that after many years of apparent exponential increase in online advertising ‘value’, the long-term metrics may be starting to unravel, as tangible costs in both trust and consumer response to OBA are emerging and connections of brand value to ethics and trustworthy customer data protection are clear.⁴²⁹ Recent OBA research challenges the view that targeting ads to consumers based upon past purchasing behaviors and existing interests actually creates a sale which would not have occurred anyway,⁴³⁰ and asserts that attaching ads to consumer interests just re-ploughs new spend into the same old ground. In essence, OBA may not be working as well as Google and Facebook represent. Some commentators now go so far as to assert that the ever-noisy Internet has weakened brand control and “diluted the power of advertising”.

Taking a long term view, it is not impossible that these issues may become predictive of future OBA industry policy and self-regulatory practices. If so, the significant consumer-focused structural and legal changes posited in part 6 might have a greater potential to become reality.

6. Where to for online behavioural advertising?

As policymakers consider different approaches . . . it is critical to understand how interventions such as negative press attention,

⁴²⁷ Recent studies are starting to question the metrics of advertising online – concluding that Internet ads are relatively “ineffective” and metrics such as ‘search clicks’, meaningless: Tom Blake, Steven Tadelis and Chris Nosko, ‘Consumer Heterogeneity and Paid Search Effectiveness: A Large Scale Field Experiment’, *NBER Working Paper No. 20171* (May 2014, accessed 10 Apr 2015) <<http://www.nber.org/papers/w20171.pdf>>. The 2012 Facebook/Datalogix study and the eBay study concluded respectively, that “people who are being influenced aren’t actually clicking ads” and “people who click most ads aren’t being influenced”: Thompson, above n 120. Even the IAB (US) has started questioning industry value, in asserting for example, that almost half of all paid online advertisements are never seen by consumers: Rothenberg, above n 139: 4. Nielsen have also shown metrics based upon consumers ‘taking action’ after viewing advertising, which consistently show a lower response rate from all online forms: Nielsen, above n 426: 7. One 2014 eBay study concluded that paid OBA search ad spending was simply targeting consumers who would buy anyway (*endogeneity*) and as such resulted in “negative returns” for the advertiser: Blake, above: 155–174. It concluded that less frequent purchasers may be influenced, but that was not sufficient to overcome the negative cost effect of the more frequent purchasers not being influenced c/f Derek Willis, ‘Facebook Says Experiments Prove Ads on Its Site Can Spur Donations’, *The New York Times* (22 Dec 2014, accessed 15 Mar 2015) <<http://www.nytimes.com/2014/12/23/upshot/facebook-says-experiments-prove-ads-on-its-site-can-spur-donations.html?abt=0002&abg=0>>.

⁴²⁸ ‘Trust capital’ is described as the consumer’s ‘emotional bond’ borne from product satisfaction, but also from the ethical collation, storage and use of their personal data. Blake Cahill argues that brand future integrity is inextricably linked to ethical data management: Cahill, above n 124.

⁴²⁹ Cahill, above n 124.

⁴³⁰ Blake et al., above n 427.

*self-regulation. . . enforcement actions, and direct regulation affect tracking. . .*⁴³¹

*Make no mistake: this means an industry behavior change, at an unprecedented scale. . .*⁴³²

*My constant refrain is that the ACCC must be an active enforcer, and be seen to be. . .*⁴³³

The Australian digital advertising industry is uniquely placed to resolve the many issues surrounding online behavioural advertising, but has failed to undertake self-regulation responsibly. This part proposes a reframing of that regulation through an alliance regulatory approach,⁴³⁴ which proposes a range of complementary mechanisms using industry, regulator and consumer inputs. These might include:

- Legislation and/or best practice self-regulation: a new Code which meets best practice standards as to plain English and content; comprehensive coverage of OBA across all devices and across the OBA industry; a trust mark compliance system to evidence compliance and audit standards;⁴³⁵ an independent complaints process with a range of resolution options and potential sanctions which might be approved by the privacy or consumer regulator; improved legal compliance through audited systems and reporting practices; improved disclosure and transparency through public complaints resolution disclosure; and appropriate appeals, sanctions and consumer remedies for Code breach. The government might also consider regulating ad networks and data brokers.⁴³⁶
- Technical improvements: rebuild youonlinechoices.com.au to improve its consumer accessibility, to offer the cookie assessment tool and to improve the opt-out process.⁴³⁷

⁴³¹ Hoofnagle, above n 21.

⁴³² Rothenberg above n 139.

⁴³³ Sims, Rod ‘Empowering consumers in the digital age’, *National Consumer Congress* (13 March 2014, accessed 16 Mar 2015).

⁴³⁴ Malbon, above n 27: 151. He coins this phrase to refer to the use of power to attain policy goals in a cooperative policy-aligned exercise between a regulator and parties with localised power sources.

⁴³⁵ Note that ADMA does have a Data Pass program which is essentially data management compliance training and designed to differentiate their members in the marketplace. It covers the data lifecycle from collection, use, analysis and disclosure uses in advertising. See <<http://www.adma.com.au/connect/articles/how-can-you-show-that-you-are-a-trusted-marketer-the-answer-is-adma-data-pass/>>.

⁴³⁶ See as to Federal Government agencies, the voluntary OAIC guidelines devised to ensure data matching is conducted in a manner consistent with the APPs and “good privacy practice”: OAIC, ‘Guidelines on Data Matching in Australian Government Administration’ (June 2014, accessed 9 Apr 2015) <<http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/advisory-privacy-guidelines-and-rules/guidelines-data-matching-australian-gov-admin.pdf>>. There seems no reason why similar guidelines could not be devised for the data broking industry.

⁴³⁷ The US NAI website is an industry best practice model in this regard.

- Industry Participation: government needs to mandate or incentivise OAB industry participation in the opt-out system such that consumer preferences reach all relevant participants.
- Consumer education: evidence suggests that consumers neither understand online tracking technologies, how OBA works or how to protect their privacy online. *Youronlinechoices* should better fulfil this function and be promoted to consumers online and off, as well as on OBA websites, privacy statements and in-ads.
- Industry standardisation: creation of model OBA consumer/privacy notices to enable improved consumer understanding; creation of standardised on-time express consent facilities online or an opt-in system; creation of a standards-setting body to better regulate and set audit standards for the digital advertising industry supply chain.⁴³⁸
- Regulatory enforcement: the ACCC could readily audit online practices across the OBA industry as to misleading or deceptive or unfair contractual terms, and the APC could likewise audit privacy policies⁴³⁹ and either could take enforcement action where necessary in the interests of industry education and consumer protection.

Finally, the ACCC could also institute proceedings to pursue an Australian precedent as to the application of the unfair terms to consumers using supposedly 'free' website or social media services, as well as the APC conducting more online compliance audits or instituting self-initiated investigations to establish that privacy laws are being observed by entities such as ad networks and data brokers – especially as to the new definition of 'personal information'. The APC should, with an eye to moving beyond its compliance phase, lobby government to increase its budget, given the enforcement potentials of its new powers and the ever-growing big data privacy challenge.

It is suggested that this type of multi-faceted alliance approach – with an eye on future technological and industry workarounds and developments – is the best possible approach to OBA regulation in Australia at this time.

7. Conclusion

*With consumer concerns comes the very real prospect of regulatory intervention. . .*⁴⁴⁰

⁴³⁸ The US IAB Head has called for this in 2014: “*The big difference between the digital advertising supply chain and that of other industries is openness: anyone can participate. There are no overarching checks to control for quality, and no one company can see all of the entities involved in its transactions . . . the digital advertising industry must stop having unprotected sex. We need a standard-setting body, a trust monitor, to guarantee the sanctity and probity of the digital advertising supply chain.*” Rothenberg, above n 139.

⁴³⁹ Pilgrim, above n 224.

⁴⁴⁰ IAB (US), above n 106: 7.

The consumer law and privacy implications of online behavioural advertising and big data breach are only just starting to be felt in Australia. While the EU has opted for a regulatory position to try to stem the perceived haemorrhaging of online personal privacy rights and to mandate data breach disclosure, the US has taken a voluntary code approach, augmented by significant FTC enforcement activity. Regrettably, Australia has taken the lesser of two options: a weak self-regulatory code and little if any, enforcement action. This paper exposes this weakness in Australia's otherwise laudable but largely compliance-based privacy regime and questions the policy basis for under-resourcing or under-prioritising the enforcement of both privacy and consumer-related laws in this area.⁴⁴¹ This paper has endeavoured to show that the dark side of online behavioural advertising is as much an issue for consumer law as for the privacy regime, and indeed, that effective enforcement, punitive consequences and industry deterrence are at least in the short term, more likely outcomes under the auspices of the ACCC. The FTC has clearly demonstrated that misleading and deceptive conduct in the collection, management and use of personal information, as well as non-disclosure and deceptive terms and conditions, are the real concerns in OBA – and privacy breach is but one of a range of injuries to society and the economy caused by illegal OBA behaviours.

Given the rapid technological rate of change, the lag in Australian regulatory response and the runaway train potentials of big data and online behavioural advertising in all its evolving forms, it is time that Australian regulators took decisive action.

Appendix: Supplementary material

Supplementary data to this article (Annexure 1 and References) can be found online at [doi:10.1016/j.clsr.2015.12.006](https://doi.org/10.1016/j.clsr.2015.12.006).

⁴⁴¹ The ACCC's responsibilities are increased regularly by the Australian government. In 2014, it received an additional \$20 million in funding but suffered a 12.5% staff reduction. Clearly, resources allocation and corporate priorities affect the issues upon which the ACCC can focus, but it quite fairly asserted that it did not “miss a beat”. In some ways, 2014 was a watershed year for the ACCC in terms of consumer-based regulatory action and it is notable that its Chair is calling for increased penalties in the light of some significant victories against large corporations, where penalties imposed would clearly not ‘hurt’ the bottom line sufficiently: Sims, above n 433.

Appendix: Acronyms

ACCC	Australian Competition and Consumer Commission
AAMIA	Australian Interactive Media Industry Association
AANA	Australian Association of National Advertisers
ADAA	Australian Digital Advertising Alliance
ADMA	Australian Direct Marketing Association
ADAA	Australian Digital Advertising Alliance
APC or 'PC'	Australian Privacy Commissioner
FTC	US Federal Trade Commission
IAB	Interactive Advertising Board
IAB (UK)	Interactive Advertising Board (UK)
IAB (US)	Interactive Advertising Board (US)
IIA	Internet Industry Association
MFA	Media Federation of Australia
OBA	online behavioural advertising
OAIC	Office of the Australian Information Commissioner
PA	Privacy Act 1988 (Cth)
TCC	The Communications Council
