THE GOOGLE STREET VIEW WI-FI SCANDAL AND ITS REPERCUSSIONS FOR PRIVACY REGULATION

MARK BURDON* AND ALISSA McKILLOP**

Between 2008 and 2010, Google secretly collected Wi-Fi header data from residential and business Wi-Fi access points throughout the world. The collection also included details of personal communications commonly known as 'payload data'. A number of regulatory investigations ensued from this global privacy scandal. Some privacy authorities, including the Australian Privacy Commissioner, sanctioned Google for the collection of payload data. However, the header data collection was largely overlooked. Those authorities that investigated the collection of Wi-Fi header data concluded that Google breached relevant privacy laws. As a result, some jurisdictions now classify Wi-Fi header data as personal information whereas others do not. The collection of Wi-Fi header data gives rise to complex policy and privacy considerations as this data is an important asset of new Location-Based Services. Consequently, it is important to revisit the Google scandal to investigate whether Google's collection of Australian Wi-Fi header data breached the Privacy Act 1988 *(Cth). Our analysis reveals that Google is likely to have breached the Act, which raises important questions about the regulatory actions conducted in Australia and the efficacy of the Act's application in the face of continuing and rapid technological development.*

I INTRODUCTION

Locational ineptitude is fast becoming a thing of the past thanks to the simple act of pulling out a smart phone and consulting the in-built mapping software. However, behind this simple act there lies a new, vast and complex technological network: the industry of Location-Based Services.[1] Location-Based Services rely on header data broadcast from Wi-Fi access points, such as residential wireless modems or routers, to provide individuals with interactive location and mapping

* Lecturer, T C Beirne School of Law, University of Queensland.

** Research Assistant, T C Beirne School of Law, University of Queensland; Trainee Solicitor, Dundas Lawyers. The authors would like to thank the anonymous reviewers for their helpful and considered feedback on previous drafts. The editors also deserve special praise for their input.

1 See generally Roba Abbas et al, 'Sketching and Validating the Location-Based Services (LBS) Regulatory Framework in Australia' (2013) 29 *Computer Law & Security Review* 576. For the purpose of this article, we adopt the definition of Location-Based Services as provided by Abbas et al: 'those applications that combine the location of a mobile device associated with a given entity (individual or object) together with contextual information to offer a value-added service': at 576.

applications.[2] Wi-Fi access points are a good source of geolocation information[3] as they continually broadcast data that can be used to verify location.[4] Previously, Location-Based Services used satellite vehicle based positioning systems manned by cellular communication network operators, such as Global Satellite Positioning (GPS).[5] GPS is extremely accurate, but Wi-Fi mapping is more beneficial because it is energy efficient and reliable indoors where satellite accessibility is restricted.[6] The global market for mapping Wi-Fi access points has expanded as the availability of Wi-Fi access points has exploded. Existing mapping services, such as Skyhook,[7] paved the way for new location-based technologies by developing a massive global mapping network covering 700 million Wi-Fi access points.[8] Skyhook partially depends on user-generated data as does another purely crowd-sourced map, WiGLE — Wireless Geographic Logging Engine.[9]

The mapping of Wi-Fi access points has also given rise to a lucrative industry of individualised location-based advertising,[10] which was the spur for Google to develop its own location map of Wi-Fi access points.[11] The map would enable Google to enhance its product line and help to maintain its dominance as the self-ordained cataloguer of global information.[12] Moreover, Google already had the ready ability to collect Wi-Fi header data on a global scale courtesy of the photographic requirements needed for its Street View service. The scene was

2 Katina Michael and Roger Clarke, 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' (2013) 29 *Computer Law & Security Review* 216, 217–19.

3 For a definition of geo-information, see Sjaak Nouwt, 'Reasonable Expectations of Geo-Privacy?' (2008) 5 *SCRIPTed* 375, 377, which provides the example of 'the location of buildings, roads, and parcels in a landscape, combined with information about these objects, like the function of the building, the type of road, and the use of the parcel' (citations omitted).

4 See Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation Services on Smart Mobile Devices' (Document No 881/11/EN WP 185, European Commission, 16 May 2011) 6 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf> ('*Working Party Opinion*'): 'geolocation based on WiFi access points provides a quick and, based on continuous measurements, increasingly accurate position'.

5 Alexander Zipf and Matthias M Jöst, 'Location-Based Services' in Wolfgang Kresse and David M Danko (eds), *Springer Handbook of Geographic Information* (Springer, 2012) 711, 713.

6 Ann Cavoukian and Kim Cameron, 'Wi-Fi Positioning Systems: Beware of Unintended Consequences: Issues Involving the Unforeseen Uses of Pre-Existing Architecture' (Report, Information and Privacy Commissioner, Ontario, Canada, June 2011) 3 <http://www.ipc.on.ca/images/Resources/wi-fi.pdf>.

7 Skyhook Wireless Inc, *Skyhook* (2014) <http://www.skyhookwireless.com/>.

8 Skyhook Wireless Inc, *Coverage Area* (2014) <http://www.skyhookwireless.com/location-technology/coverage.php>.

9 WiGLE — Wireless Geographic Lopping Engine, *Browsable Map o' the World* <http://wigle.net/gps/gps/Map/onlinemap2/>.

10 Marguerite Reardon, 'Location Information to Make Mobile Ads More Valuable', *Cnet News* (online), 15 April 2013 <http://news.cnet.com/8301-1035_3-57579746-94/location-information-to-make-mobile-ads-more-valuable/>.

11 See P Michele Ellison, Federal Communications Commission, 'In the Matter of Google, Inc: Notice of Apparent Liability for Forfeiture' (Notice No DA 12-592, 13 April 2012) 1 [1] <http://info.publicintelligence.net/FCC-GoogleWiFiSpy.pdf> ('*FCC Liability Notice*'). Google's purpose for collection 'was to capture information about Wi-Fi networks that the Company could use to help establish users' locations and provide location-based services'. For a discussion of Wi-Fi mapping, see Raymond Chow, 'Why-Spy? An Analysis of Privacy and Geolocation in the Wake of the 2010 Google "Wi-Spy" Controversy' (2013) 39 *Rutgers Computer & Technology Law Journal* 56, 66.

12 See Google Inc, *About Google* <http://www.google.com/about/>. Google's Mission Statement is 'to organize the world's information and make it universally accessible and useful'.

therefore set for one of the most significant, secret and global collections of personal information ever conducted by a government or a corporation.

In this article, we examine the Google Street View scandal to investigate whether Google's collection of Australian Wi-Fi header data breached the *Privacy Act 1988* (Cth) ('*Privacy Act*'). Part II provides an overview of the Google Street View Wi-Fi scandal and regulatory responses of different jurisdictions. Part III investigates whether and to what extent Google breached relevant requirements of the *Privacy Act* regarding the collection of Wi-Fi header data in Australia. Two key issues are examined: (1) whether the Wi-Fi header data was personal information; and (2) whether the collection of Wi-Fi header data was in breach of the Act. Part IV then examines the immediate actions of the then Australian Privacy Commissioner and subsequent legal responses in the EU and in Australia. Our analysis questions the coherence of the immediate Australian regulatory response and subsequent decision-making, which provides a crucial insight into the application of the *Privacy Act* to contemporary technological developments.

II THE GOOGLE STREET VIEW WI-FI SCANDAL

Google launched Street View in May 2007. Google's specially modified vehicles obtained panoramic street-level photographs of residential roads and surrounding structures which were then used to enhance pre-existing mapping applications such as Google Maps and Google Earth.[13] Google's Street View photographic exercise attracted international media and regulatory attention.[14] However, unbeknownst to anyone outside of Google, the corporation was also attempting to develop a global map of Wi-Fi access points.

To create a map of Wi-Fi access points it is necessary to collect data contained within the packets of individual Wi-Fi networks that contain header and payload data. Header data is similar to a postal address written on an envelope: it communicates the destination of information and guides a packet from one device to another.[15] Header data includes identifying information about Wi-Fi devices and access points including the Service Set Identifier (SSID), Media Address Control (MAC) address and signal strength details. The MAC address and SSID ensure the compatibility of different manufactured devices within the same Wi-Fi

13 Google Inc, *Behind the Scenes: Street View* (2014) Google Maps <http://maps.google.com.au/maps/about/behind-the-scenes/streetview/>; Google Inc, *Views* (2014) Google Maps <https://www.google.com/maps/views/home?gl=us>.

14 Lauren H Rakower, 'Blurred Line: Zooming in on Google Street View and the Global Right to Privacy' (2011) 37 *Brooklyn Journal of International Law* 317, 326–7.

15 See Geoff Huston, 'A Rough Guide to Address Exhaustion' (2011) 14(1) *Internet Protocol Journal* 2, 2, 5 <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-1/ipj_14-1.pdf>, which refers to the concept of an 'address' and 'packet switching'. For a detailed overview of the technical architecture and software employed by Google, see generally Stroz Friedberg, 'Source Code Analysis of gstumbler' (Report, Google and Perkins Coie, 3 June 2010) <http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf>. This is a third party report produced on behalf of Google in response to regulatory questioning.

network.[16] Payload data is the content of user-generated communications and can include emails, details of websites visited, passwords of protected websites and other forms of messaging.

A MAC address is a unique 48-bit binary numerical identifier that the manufacturer assigns to a Wi-Fi enabled device.[17] A MAC address is visible in the communicated data frames irrespective of whether the wireless connection is encrypted.[18] A message communicated to another Wi-Fi enabled device will contain the MAC address of sender and receiver in the header or address section of the message. An SSID is a 'network name' and is used as a description to identify and to distinguish between different Wi-Fi access points. The default SSID usually incorporates the product type or manufacturer name.[19] There are some significant differences between a MAC address and an SSID. Unlike a MAC address, an SSID is not a unique identifier and is not device specific, which means that one SSID can be repeated several times within a limited geographical area.[20] Also, unlike a MAC address, an SSID can be personalised within a 32-character limitation.[21] A user can also prevent an SSID from being publicly displayed, but the signal will still be broadcast and appear in some of the management packets transmitted over the wireless network.[22]

Google originally fitted its Street View photography vehicles with Wi-Fi antennae and sophisticated software to capture, parse and store Wi-Fi data.[23] By 2008, Street View vehicles were deployed in Australia and collected Wi-Fi data from residential and business networks. In 2010, German data protection authorities started questioning Google about the prospective implementation of Street View in Germany.[24] These discussions revealed that Google Street View vehicles had collected Wi-Fi header data as part of the photographic collection.[25] The collected data was transferred to Google servers in the United States with the intention of

16 *Working Party Opinion*, above n 4, 5.

17 See Chow, above n 11, 63. The format is as follows: 48-2C-6A-1E-59-3D.

18 Cavoukian and Cameron, above n 6, 4.

19 Mark Watts, James Brunger and Kate Shires, 'Do European Data Protection Laws Apply to the Collection of WiFi Network Data for Use in Geolocation Look-Up Services?' (2011) 1 *International Data Privacy Law* 149, 151. For example, 'BigPond12B4' or 'Belkin11d'.

20 Ibid.

21 For example, by manually changing the default setting of 'BigPond12B4' to 'John's Home Network'.

22 Watts, Brunger and Shires, above n 19, 151.

23 See, eg, Peter Fleischer, 'Data Collected by Google Cars' on *Google: Europe Blog: Our Views on the Internet and Society* (27 April 2010) <http://googlepolicyeurope.blogspot.com.au/2010/04/data-collected-by-google-cars.html>.

24 See 'Navigating Controversy: Google Launches Street View Germany', *Spiegel Online: International* (online), 18 November 2010 <http://www.spiegel.de/international/business/navigating-controversy-google-launches-street-view-germany-a-729793.html>. See also Bart van der Sloot and Frederik Zuiderveen Borgesius, 'Google and Personal Data Protection' in Aurelio Lopez-Tarruella (ed), *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models* (Springer, 2012) 75, 85–7, regarding the privacy issues that arise in relation to Google Street View photography.

25 Chow, above n 11, 70, citing Matt McGee, *Google Maps Privacy: The Street View & Wifi Scorecard* (11 November 2010) Search Engine Land <http://searchengineland.com/google-street-view-scorecard-55487>.

creating a Wi-Fi mapping database.[26] Google claimed there was nothing illegal about the collection of data as it was simply doing what Skyhook and WiGLE had done previously.[27] The collected data was publically accessible and it could not be used to identify an individual, so information privacy laws did not apply.[28] Further investigations by European data protection authorities revealed that Google also collected payload data from unencrypted Wi-Fi networks.[29] Google then made a series of admissions stating that it had inadvertently collected payload data and that the collection was conducted by a rogue engineer without Google's knowledge.[30]

Google's collection of Wi-Fi data sparked a number of regulatory investigations around the world and the inevitable US class actions.[31] Most of the investigations focused on the collection of payload data and the collection of Wi-Fi header data was generally overlooked. For example, the UK Information Commissioner's Office concluded that Google's collection of payload data significantly breached the *Data Protection Act 1998* (UK), c 29.[32] Similarly, the Canadian Privacy Commissioner confirmed that Google was in breach of *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.[33] However, the Hong Kong Privacy Commissioner concluded that the collected payload data did not contain 'any meaningful details that [could] directly identify any one individual'.[34] Google therefore had not breached Hong Kong privacy law. The US Federal Communications Commission (FCC) investigated whether Google was in breach of relevant US federal communications law, particularly the *Federal*

26 Ibid. See also *FCC Liability Notice*, above n 11, 9–10 [20]–[21]. Google's purpose for collection 'was to capture information about Wi-Fi networks that the Company could use to help establish users' locations and provide location-based services': at 1 [1].

27 See Fleischer, 'Data Collected by Google Cars', above n 23.

28 Ibid.

29 *Commission Nationale de l'Informatique et des Libertes* [National Commission on Informatics and Liberty], decision n° 2011-035, 17 March 2011 <http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>. This decision imposed a financial penalty on Google.

30 See, eg, Alan Eustace, 'WiFi Data Collection: An Update' on *Google: Official Blog* (14 May 2010) <http://googleblog.blogspot.com.au/2010/05/wifi-data-collection-update.html>.

31 Electronic Privacy Information Center, *Investigations of Google Street View* (2012) <http://epic.org/privacy/streetview/>.

32 Information Commissioner's Office, 'Information Commissioner Announces Outcome of Google Street View Investigation' (Press Release, 3 November 2010) 1; 'Google Guilty of "Significant Breach" of Data Protection Act: ICO', *New Statesman* (online), 4 November 2010 <http://www.newstatesman.com/technology/2010/11/data-google-ico-commissioner>; Loek Essers, 'Google "Surprised" by Revived ICO Street View Investigation', *Computer World UK* (online), 20 June 2012 <http://www.computerworlduk.com/news/security/3365254/google-surprised-by-revived-ico-street-view-investigation/?intcmp=rel_articles;scrty;link_2>.

33 Office of the Privacy Commissioner of Canada, 'Archived — Preliminary Letter of Findings: Complaints under the *Personal Protection and Electronic Documents Act* (the *Act*)' (Investigation Document, 19 October 2010) <http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.asp> ('*Canadian Investigation Letter*').

34 Office of the Privacy Commissioner for Personal Data, Hong Kong, 'Personal Data (Privacy) Ordinance: Google Street View Cars Collecting Wi-Fi Payload Data in Hong Kong: Decision by the Privacy Commissioner for Personal Data' (Case No 201006847, 30 July 2010) 5 [12] <http://www.pcpd.org.hk/english/publications/files/Google_result_e.pdf>.

Wiretap Act,[35] which prohibits electronic eavesdropping.[36] The FCC fined Google US$25 000 because Google impeded the FCC's investigation by delaying the provision of information and the verification of required submissions.[37] The FCC report was critical of Google's actions and demonstrated that Google's 'rogue engineer' defence was a fabrication, as the engineer in question had informed Google managers about the intention to collect payload data.[38]

A small number of jurisdictions did investigate whether the collection of Wi-Fi header data, in conjunction with payload data, breached relevant legislation. The Dutch Data Protection Authority (Dutch DPA) concluded that Wi-Fi header data was 'personal data' under the *Data Protection Directive* because it was possible to identify an individual from both SSID and MAC address data.[39] The Dutch DPA found examples from the data collected by Google of a number of customised SSIDs that gave rise to the identification of an individual. Non-customised SSIDs could also be used to identify an individual when collected with MAC addresses, calculated geographical locations and Wi-Fi signal frequency rates.[40] Google could combine the data to match an SSID and a MAC address with a specific address which made it possible to reveal the identity of an individual. The Dutch DPA concluded that Google had a legitimate purpose for the collection of Wi-Fi header data (in order to improve its products),[41] but Google had nonetheless failed to notify individuals about the collection.[42] Several administrative orders were issued against Google and it was required to develop of an opt-out mechanism for future collections of Wi-Fi header data.[43] Google was also threatened with

35 18 USC §§2510–2522 (2000). See Letter from David C Vladeck, Bureau of Consumer Protection, to Albert Gidari, Perkins Coie LPP, 27 October 2010 <http://www.ftc.gov/os/closings/101027googleletter.pdf>.

36 Amy Schatz and Amir Efrati, 'FCC Investigating Google Data Collection', *The Wall Street Journal* (online), 11 November 2010 <http://online.wsj.com/article/SB10001424052748704804504575606831614327598.html?mod=WSJ_hp_LEFTWhatsNewsCollection>.

37 *FCC Liability Notice*, above n 11, 23–4.

38 Ibid 15. The 'rogue' engineer who specifically developed Google's Wi-Fi scanning software for the Street View collection had highlighted to his managers potential privacy concerns relevant to the collection of Wi-Fi data. However, the privacy implications were not considered serious because 'the Street View cars would not be "in proximity to any given user for an extended period of time" and "[n]one of the data gathered ... [would] be presented to end users of [Google's] services in raw form"': at 11 [22]. The issue was marked as a factor to address with the Product Counsel, but this never occurred.

39 *Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31, art 2(a) ('*Data Protection Directive*'). Article 2(a) defines personal data as

> any information relating to an identified or identifiable natural person ('data subject"'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

40 Dutch DPA, 'Final Findings: Dutch Data Protection Authority Investigation into the Collection of WiFi Data by Google Using Street View Cars' (Report, 7 December 2010) 30 <http://www.dutchdpa.nl/downloads_overig/en_pb_20110811_google_final_findings.pdf> ('*Dutch DPA Final Findings*').

41 See also van der Sloot and Borgesius, above n 24, 96–8, regarding the breadth of Google's purpose for Street View collection and the application of the *Data Protection Directive.*

42 Ibid.

43 Dutch DPA, 'Dutch DPA Issues Several Administrative Orders against Google' (Informal Translation Press Release, 19 April 2011) <http://www.dutchdpa.nl/Pages/en_pb_20110419_google.aspx>. The opt-out solution entailed the inclusion of 'no map' at the end of an SSID.

fines for non-compliance but these were not imposed as Google complied with the orders.[44]

The French Data Protection Authority, *Commission Nationale de l'Informatique et des Libertés* (CNIL), also concluded that Wi-Fi header data was personal data.[45] Like their Dutch counterparts, CNIL decided that it was possible to identify an individual through a customised SSID and it was possible to aggregate the different data elements together to identify an individual. CNIL also revealed that Google could search for an SSID or a MAC address and then match that data to a specific geographic location.[46] In rural areas it was therefore possible to identify an individual by combining this information with address data and, even in more populated urban areas, it was still possible to match an individual to a specific address by the combination of location data, SSID, MAC address and wireless strength data.[47] Google argued that it would be practically difficult for it to aggregate collected data this way, but CNIL rejected Google's arguments given its aggregation capabilities.

The New Zealand Privacy Commissioner reached the same conclusion as the Dutch and French, but did not examine the data collected by Google in New Zealand. Wi-Fi header data could be classified as personal information[48] because SSIDs could be customised by name and, if one was to 'walk down any street in a New Zealand suburb with a wireless device', one would be able see individually named Wi-Fi networks.[49] Furthermore, it did not matter whether the Wi-Fi header data was publically available or not because Google still required a legitimate reason for collection.[50] In considering that point, the Commissioner decided that Google had a lawful purpose for collection because the improvement of products or services was a legitimate business function. However, Google breached the *Privacy Act 1993* (NZ) due to its lack of notification to individuals in conjunction with an unfair collection practice that was systematic and covert.[51]

In Australia, s 36 of the *Privacy Act* generally allows a complaint to be made to the Privacy Commissioner and, once a complaint is investigated, there are a limited

44 Dutch DPA, 'Google Has Complied with Dutch DPA Requirements' (Press Release, 5 April 2012) <http://www.dutchdpa.nl/Pages/en_pb_20120405_google-complies-with-Dutch-DPA-requirements.aspx>.

45 *Commission Nationale de l'Informatique et des Libertes* [National Commission on Informatics and Liberty], decision n° 2011-035, 17 March 2011 <http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>.

46 Ibid.

47 Ibid.

48 *Privacy Act 1993* (NZ) s 2 (definition of 'personal information'). Under this Act, 'personal information means information about an identifiable individual'. For a discussion about the construction of personal information under the Act, see generally Paul Roth, 'What is "Personal Information"?' (2002) 20 *New Zealand Universities Law Review* 40.

49 Privacy Commissioner (New Zealand), *Google's Collection of WiFi Information during Street View Filming* (13 December 2010) <http://privacy.org.nz/news-and-publications/commissioner-inquiries/google-s-collection-of-wifi-information-during-street-view-filming/>.

50 Ibid.

51 Ibid.

range of powers available to the Commissioner to enforce a determination.[52] Under s 40(2), the Commissioner may 'investigate an act or practice if: (a) the act or practice may be an interference with the privacy of an individual; and (b) the Commissioner thinks it is desirable that the act or practice be investigated'. These investigations are known as Own Motion Investigations (OMIs) and the then Privacy Commissioner, Karen Curtis, conducted such an investigation into Google's collection of Wi-Fi data.[53] The Commissioner concluded that Google had breached relevant provisions of the *Privacy Act* regarding the collection of payload data.[54] It should be noted that, unlike complaints made under s 36, the Commissioner had no powers to enforce remedies against an organisation investigated under an OMI. Nevertheless, Google agreed to make certain undertakings.[55]

The Commissioner decided not to examine Google's collection of Wi-Fi header data, as indicated by statements to the media.[56] We contend that the then Commissioner's reluctance to examine Google's Australian Wi-Fi header data collection was a major oversight as some jurisdictions concluded that Wi-Fi header data was personal information and the collection was thus subject to information privacy law. The question therefore arises whether such data should be classified as personal information in Australia, and if so, whether Google's collection of Wi-Fi header data breached the *Privacy Act*. We examine these complex issues in the next section.

III DID GOOGLE'S COLLECTION OF WI-FI HEADER DATA BREACH THE *PRIVACY ACT*?

At its point of inception, the *Privacy Act* regulated the conduct of Australian government agencies and Australian Capital Territory (ACT) agencies. Certain private sector organisations were then covered by the Act 12 years later.[57] The Act adopts a principled approach to information privacy protection that provides a

52 See *Privacy Act* s 27(1).

53 Louisa Hearn, 'Privacy Watchdog Probes Google's Wi-Fi Data Harvest', *The Sydney Morning Herald* (online), 19 May 2010 <http://www.smh.com.au/technology/technology-news/privacy-watchdog-probes-googles-wifi-data-harvest-20100519-vckv.html>.

54 Office of the Australian Information Commisioner, *Australian Privacy Commissioner Obtains Privacy Undertakings from Google* (9 July 2010) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/google-street-view-wi-fi-collection/australian-privacy-commissioner-obtains-privacy-undertakings-from-google>.

55 These included making a public apology and a privacy impact assessment in relation to future Google Street View activities involving personal information, and to regularly consult with the Commissioner about significant product launches involving personal information collection.

56 Louisa Hearn, 'Please Explain: Why Google Wants Your Wi-Fi Data', *The Age* (online), 13 May 2010 <http://www.theage.com.au/technology/technology-news/please-explain-why-google-wants-your-wifi-data-20100513-uyyh.html>; Meredith Griffiths, 'Privacy Concerns as Google's Street View Captures WiFi Data', *ABC News* (online), 13 May 2010 <http://www.abc.net.au/pm/content/2010/s2898832.htm>. These statements are examined in greater detail in Part IV.

57 Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (LexisNexis Butterworths, 2005) 64 [2.66].

regulatory structure predicated on the application of general principles rather than governance through determinate rules.[58] At the time of the Street View scandal, government agencies and covered private sector organisations were regulated by different sets of privacy principles. The Information Privacy Principles (IPPs) applied to Commonwealth and ACT government agencies and the National Privacy Principles (NPPs) applied to private sector organisations. In March 2014, a new set of privacy principles — the Australian Privacy Principles — replaced the IPPs and the NPPs and apply to government agencies and private sector organisations.[59] For the purpose of this article, we examine how the *Privacy Act* applied in 2010 and how Google, as a private sector organisation, was covered by the NPPs.[60]

Judicial interpretation of the *Privacy Act*'s key components is scant and the interpretation of many of the Act's central provisions is still a matter of some speculation.[61] Accordingly, this article examines the limited Commonwealth cases, state cases, and guidance and case notes produced by the Office of the Australian Information Commissioner (OAIC) and its predecessor, the Office of the Privacy Commissioner (OPC).[62] There are sufficient similarities between both sets of privacy principles and the Commonwealth and state case law to apply these different resources concomitantly. Two key question need to be addressed:

1. Was the Wi-Fi header data collected by Google classifiable as personal information under the Act?

2. Was Google's collection of Wi-Fi header data in breach of *NPP* 1?[63]

58 See, eg, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 1, 233–8 [4.1]–[4.18] ('*For Your Information Report*').

59 See Normann Witzleb, 'Halfway or Half-Hearted? An Overview of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth)' (2013) 41 *Australian Business Law Review* 55, 55.

60 The authors work on the basis that Google, and its Australian subsidiary, Google Australia, would not be exempt from the Act on the basis that it is a small business.

61 See, eg, Graham Greenleaf, 'Privacy in Australia' in James B Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008) 141, 141, 148.

62 The new role of the Privacy Commissioner was established in the *Australian Information Commissioner Act 2010* (Cth).

63 There are also a number of organisational exemptions under the Act which exempt certain organisations from the Act's coverage: see, eg, Greenleaf, 'Privacy in Australia', above n 61, 168. The authors of this article are operating on the basis that none of these exemptions would have applied to Google in relation to the Street View scandal. It should also be noted that the *Privacy Act* also includes a sub-set of personal information called 'sensitive information' that may have higher degrees of sensitivity and which accords higher statutory obligations. 'Sensitive information' under s 6(1) of the Act can include racial origins, political beliefs, religious beliefs or sexual orientation. It is possible that Google collected sensitive information in the form of customised SSIDs. See, eg, 'The Politics of WiFi Names' on *OpenSignal* (31 May 2012) <http://opensignal.com/blog/2012/05/31/the-politics-of-wi-fi-names/>; Michael J Feeney, 'WiFi Signal with Racist, Anti-Semitic Slur in Teaneck, NJ Sparks Police Probe; Signal Came from Rec Center Router', *New York Daily News* (online), 18 January 2012 <http://www.nydailynews.com/news/national/wifi-signal-racist-anti-semitic-slur-teaneck-nj-sparks-police-probe-signal-rec-center-router-article-1.1008135>; Answerit, *Can You Suggest a Nice Gay Name for My Wireless Network?* (2011) <http://answerit.news24.com/Question/Can%20you%20suggest%20a%20nice%20Gay%20name%20for%20my%20wireless%20network?/83807>. See also Dutch DPA, 'Dutch DPA Issues Several Administrative Orders against Google', above n 43: the examination of Google's collection in Holland confirmed the collection of sensitive information. However, we do not examine this particular issue here.

A *Was the Wi-Fi Header Data Collected by Google Personal Information?*

The classification of information as 'personal information'[64] is a threshold issue as the *Privacy Act* only covers an act or practice involving personal information.[65] What is or is not personal information is consequently vital to the operation of information privacy law, and different definitions reflect differing political perspectives about the appropriate role of information privacy protections in different jurisdictions.[66] It is therefore necessary to briefly overview the different definitions of 'personal information' currently in operation in Australia and in other jurisdictions. The text of the *Privacy Act* stems from the Organisation for Economic Co-operation and Development's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, developed in 1981 and amended in July 2013.[67] The term 'personal data' is defined under the *OECD Guidelines* as information 'relating to an identified or an identifiable individual' and refers to information that has the capacity to identify an individual by direct or indirect linkages.[68] The EU *Data Protection Directive* adopts essentially the same definition of 'personal data' and provides that the ability to identify through indirect linkages is to be construed broadly in light of the Directive's purpose to protect fundamental rights and freedoms in relation to personal data processing.[69] The requirement for broad construction has been further extended in the recently

64 'Personal data' and 'personal information' are used interchangeably in this article.

65 *Privacy Act* s 6A(1). Indeed, the definition of 'personal information' is crucial to the application of information privacy laws in general. See, eg, Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Review* 1814, 1816. The term 'Personally Identifiable Information' is used in the US to describe 'personal information'. See also Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) *UCLA Law Review* 1701, 1742–3, which criticises personally identifiable information as an inappropriate way to measure privacy protections.

66 See, eg, Paul M Schwartz, 'The EU–US Privacy Collision: A Turn to Institutions and Procedures' (2012) 126 *Harvard Law Review* 1966, 1975.

67 Organisation for Economic Co-operation and Development, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (23 September 1980) <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> ('*OECD Guidelines*'). For a discussion about the implementation of the *OECD Guidelines* in Australia and New Zealand, see generally Justice Michael Kirby, 'Twenty-Five Years of Evolving Information Privacy Law — Where Have We Come from and Where Are We Going?'(2003) 21 *Prometheus: Critical Studies in Innovation* 467.

68 *OECD Guidelines*, above n 67, cl 1(b): '"personal data" means any information relating to an identified or identifiable individual (data subject)'. The amendments to the *OECD Guidelines* in 2013 did not change the definition of 'personal data'. For a critique of the expansive effect of direct and indirect linking in light of re-identification contexts, see Ohm, above n 65, 1741. See also Teresa Scassa, 'Geographical Information as Personal Information' (2010) 10 *Oxford University Commonwealth Law Journal* 185, 189–90, 198–9, regarding the complexities of indirect linking in a geographical context.

69 See Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (Document No 01248/07/EN WP 136, European Commission, 20 June 2007) 4 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>.

proposed *General Data Protection Regulation*, which now provides an updated definition of 'personal data' as any information relating to a data subject.[70]

The *OECD Guidelines* deliberately provided member states with a substantial amount of interpretative leeway given the differing political considerations accorded to information privacy protection. This interpretive leeway was used significantly by the Commonwealth regarding the *Privacy Act*'s definition of 'personal information' as stated in s 6(1):

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

There is a significant difference between the definition of 'personal data' in the *OECD Guidelines* and the definition of 'personal information' under s 6(1). The former regards personal data as relating to 'identified or identifiable individuals', whereas the latter relates to information 'about' an individual.[71] The *Privacy Act*'s definition of personal information is therefore more constricted in its application because the removal of 'relates to' narrows the situations in which information can identify an individual.[72] A MAC address is a good case in point as it is a device identifier rather than an individual identifier.[73] In that sense, it is not information 'about' an individual, but it can clearly be information that 'relates' to an individual. This point is addressed further below in Part IV.

The *Privacy Act*'s definition of personal information was also considered by the Australian Law Reform Commission (ALRC) in 2008 as part of its *For Your Information Report*. The ALRC concluded that personal information should still be information about an individual rather than information that relates to an individual.[74] Nevertheless, an update to the definition of personal information was required so Australia would be in line with other jurisdictions and international

70 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (Document No 0011, 25 January 2012) ('*General Data Protection Regulation*'). A 'data subject' is defined in art 4(1) as

> an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

71 For the normative dimensions of defining personal information in relation to control theories of privacy, see Raymond Wacks, *Personal Information: Privacy and the Law* (Clarendon Press, 1989) 22–4. See also Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002) 42, regarding the properties of personal information and their role in protecting privacy under information privacy law. See also David Lindsay, 'Misunderstanding "Personal Information": *Durant v Financial Services Authority*' (2004) 10 *Privacy Law and Policy Reporter* 13.

72 For a description of the requirement for information to identify a specific individual as 'reductionist', see Schwartz and Solove, above n 65, 1871. The converse approach is the 'expansionist' tendency of the EU to broaden definitions of personal information: at 1875.

73 See Chow, above n 11, 64.

74 *For Your Information Report*, above n 58, 306 [6.51]. The principle reason for the use of 'about' as opposed to 'relates' appears to be consistent with the APEC Privacy Framework.

instruments.[75] Personal information should therefore be information about an individual who is 'identified or reasonably identifiable'.[76] The ALRC also recommended that practical ongoing guidance about how information could reasonably identify an individual was required to indicate how the definition of personal information would apply in specific contexts.[77]

The ALRC's new definition of personal information was adopted by the Commonwealth and commenced in March 2014. Section 36 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) provides for a new definition of personal information that substitutes s 6(1) of the current *Privacy Act*. The new definition in s 6(1) of the *Privacy Act* states that personal information is 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not'.

The Explanatory Memorandum to the amendment bill makes clear that the new definition is not intended to change the scope of the existing meaning and thus considerations of what amounts to personal information are still 'to be based on factors which are relevant to the context and circumstances in which the information is collected and held'.[78] The OAIC was also encouraged by the Australian government to develop and publish 'appropriate guidance … about the meaning of "identified and reasonably identifiable"'.[79]

Taking on board the above, it is important to outline two factors. First, personal information does not need to be information of a 'private, intimate or sensitive character'.[80] Second, and as highlighted in the above discussion, the definition of personal information is predicated on the ability of collecting organisations to identify an individual from information collected about them. Identification can be achieved in two ways under the *Privacy Act*:

1. *Apparent* — where an individual can be identified from a record or information without recourse to extraneous information.[81]

75 Ibid 307 [6.53].

76 Ibid. For a discussion of the identifiable/identified distinction, see Schwartz and Solove, above n 65, 1875–8.

77 *For Your Information Report*, above n 58, 309 [6.63].

78 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53.

79 Ibid.

80 *NW v New South Wales Fire Brigades* [2005] NSWADT 73 (1 April 2005) [11]. See also *Seven Network (Operations) Ltd v Media Entertainment & Arts Alliance* (2004) 148 FCR 145, 166 [45] (Gyles J) ('*Seven Network*'); *Re Callejo and Department of Immigration and Citizenship* (2010) 51 AAR 308, 333–5 [64]–[67], cited in *Re Lobo and Department of Immigration and Citizenship* (2011) 56 AAR 1, 93 [288]. For the proposition that '"personal information" … is not confined to information that concerns the "personal affairs" of a person', see *WL v Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [20]. See also Nouwt, above n 3, 383, for the proposition that the processing of geo-information does not have to amount to 'an interference with … privacy or personal life' to establish an action under information privacy laws.

81 *Re WL and LA Trobe University* (2005) 24 VAR 23, 28 [17]–[18].

2. *Reasonably Ascertainable* — where there is not enough information in the record to identify an individual from that record but it can be used to cross-reference other information that identifies an individual.

The concept of personal information consequently features both context dependent and context independent approaches,[82] and is capable of broad application.[83] A *context independent* approach enables the categorisation of personal information without recourse to the social context within which the information is used. As in the 'apparent' element of the Act's definition, the information itself enables identification. The minimal application of social context simplifies the categorisation of personal information because it is possible to make a definitive prediction of what information is always likely to be classified as personal information.[84] For example, an individual's name usually has the capacity to identify an individual, so therefore a name will most likely be classed as personal information. Alternatively, a *context dependent* approach, as defined by the 'reasonably ascertainable' element, deems that an individual can also be identified by information that does not directly identify but nevertheless can give rise to identification because of the social context in which that information can be used.[85] Definitional prediction becomes virtually impossible because all information could be classed as personal information in the right circumstances. For example, if it is possible to aggregate different pieces of data around a specific point of information, such as a residential address, then an agency or an organisation is able to uncover the identity of an individual 'by linking data in an address database with particular names in the same or another database, that information is "personal information"'.[86]

A record of information therefore does not have to identify a person directly for it to be classed as personal information under the Act. Identity may be apparent from other sources of information such as a driver license number, student number, description or a pseudonym, provided the identity is 'easy to see or understand' or 'obvious'.[87] However, information that simply allows an individual to be contacted, such as a telephone number or address, would not itself be classed as personal information because the *Privacy Act* was not intended to provide 'an

82 Mark Burdon and Paul Telford, 'The Conceptual Basis of Personal Information in Australian Privacy Law' (2010) 17(1) *Murdoch University Electronic Journal of Law* 1, 12. See generally Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books, 2010), regarding the importance of social context in relation to the construction and application of information privacy law.

83 *WL v Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [20]–[22], cited in *OS v Mudgee Shire Council* [2009] NSWADT 315 (17 December 2009) [19]. Since the Act 'is beneficial legislation, s 4(1) should be interpreted broadly and the exclusions from the definition of personal information should be construed narrowly': *EG v Commissioner of Police, Police Service (NSW)* [2003] NSWADT 150 (24 June 2003) [24]. See also *Department of Education and Training v PN* [2006] NSWADTAP 66 (6 December 2006) [78].

84 See Sharon Booth et al, 'What Are "Personal Data"? A Study Conducted for the UK Information Commissioner' (Report, University of Sheffield, 2004) 99–100.

85 Ibid.

86 *For Your Information Report*, above n 58, 309 [6.61].

87 *Re Lobo and Department of Immigration and Citizenship* (2011) 56 AAR 1, 93 [290], quoting *Chambers 21st Century Dictionary* (Chambers, 1999).

unqualified "right to be left alone"".[88] Nevertheless, once an individual's name is associated with their address, the address is about an identified individual and therefore constitutes personal information.[89] As such, whether Wi-Fi header data is personal information under the Act must be determined in reference to the context in which Google collected and stored the Wi-Fi header data.[90]

Google collected MAC addresses, SSID, transmission rate data and location data during the Street View collection exercise.[91] Google contended that the data was not personal information and therefore information privacy law did not apply.[92] Thus, in the Australian context, Google implicitly contended that an individual's identity was not 'apparent' or 'reasonably ascertainable' from the SSID, MAC address and transmission rates collected from Wi-Fi access points. To a certain extent, Google's assertion is correct. Both default SSIDs and MAC addresses are unique device identifiers rather than personal identifiers and are unlikely to be classed as personal information in an apparent sense.[93]

While a MAC address could not be classed as apparent personal information on its own, there is scope for a customised SSID to do so under specific circumstances. For example, this may occur when the Wi-Fi access point holder customises their SSID with their name and their name is so rare that the SSID becomes a unique identifier,[94] such as when a Wi-Fi access point holder customises their SSID with their name and address.[95] The Dutch DPA concluded that SSID data could be classed as directly identifying in such circumstances.[96] The New Zealand Privacy Commissioner also seems to have reached a similar conclusion. However, it is unclear whether the Commissioner's conclusion is founded on the basis that a customised SSID can be personal information on its own or whether identification is dependent on a combination of SSID and geographical location data. Google argued that the customisation of an SSID may not itself automatically determine the identity of an individual. For example, it is possible that one customised SSID could still be used by a number of individuals.[97] Student accommodation is a good example where the occupants of the household are likely to change quite frequently, thus making it more difficult to link an SSID to a given individual.

88 *For Your Information Report*, above n 58, 309 [6.61].

89 *WL v Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [21]–[22].

90 *WL v Randwick City Council [No 2]* [2010] NSWADT 84 (6 April 2004) [25]. See also *WL v Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [15].

91 See *Dutch DPA Final Findings*, above n 40, 15–7.

92 Fleischer, 'Data Collected by Google Cars', above n 23.

93 See, eg, *OS v Mid-Western Regional Council [No 3]* [2011] NSWADT 230 (29 September 2011) [20], where aerial photographs with lot numbers marking houses were insufficient to determine identity.

94 For example, the former Acting Queensland Privacy Commissioner was Lemm Ex. There is only one person named Lemm Ex in Australia.

95 For example, 'markburdon7smithstreet4001'.

96 *Dutch DPA Final Findings*, above n 40, 30: 'with respect to network names, that equipment can have a name chosen by its owner, that can be directly identifying (first and last name in combination with the calculated location)'.

97 *Commission Nationale de l'Informatique et des Libertes* [National Commission on Informatics and Liberty], decision n° 2011-035, 17 March 2011, 16 <http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>.

When applying the Australian law to this situation, it is important to consider the ability of a name or an address to identify an individual. Apparent identity therefore relies heavily on the factual scenario in question and generally requires a person to be 'singled' out.[98] For example, in *NW v Fire Brigades (NSW)*, even 'short-form' naming consisting of a surname and an initial sufficiently identified the complainant.[99] However, the pool of potential candidates was limited to employees at a local fire brigade station.[100] Unusual names can give rise to identity in large populations but also common names, such as 'John Smith', can identify an individual within a smaller community or organisation.[101] This seems to have been a basis for the New Zealand Privacy Commissioner's observation that in a systematic and large-scale collection of data, such as the one undertaken by Google, it becomes reasonably certain that at least some of the data collected is likely to identify an individual and should be treated as personal information.[102] It is therefore possible that customised SSID data could be classed as apparent personal information but only in limited circumstances.

However, all non-customised and customised SSIDs, and indeed MAC addresses, have the potential to be classified as information that will enable identity in a reasonably ascertainable sense when collected with location data.[103] The Dutch DPA contended that MAC addresses collected with calculated location data[104] were personal data because a unique identifier of a device which is linked to a location is also inextricably linked to an individual who resides at that location.[105] The Dutch DPA examined Google's geolocation server for 75 MAC addresses obtained in the Wi-Fi payload collection and then matched those MAC addresses to 45 separate locations within a radius of 36 metres. Each location contained an average of 8 houses and the Dutch DPA was able to further refine the search to one particular residence based on an analysis of signal strength data broadcast from the Wi-Fi access point.[106] CNIL also reached a similar conclusion.[107]

The Dutch and French investigations also demonstrated that Google would have been able to aggregate the Wi-Fi header data with other extraneous data and even

98 *NW v Fire Brigades (NSW)* [2005] NSWADT 73 (1 April 2005) [11]–[12]; *WL v Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [21], cited in *OS v Mudgee Shire Council* [2009] NSWADT 315 (17 December 2009) [20].

99 [2005] NSWADT 73 (1 April 2005) [12].

100 Ibid [12].

101 *Bailey v Hinch* [1989] VR 78, 93 (Gobbo J).

102 Privacy Commissioner (New Zealand), above n 49.

103 See *Dutch DPA Final Findings*, above n 40, 29; *Commission Nationale de l'Informatique et des Libertes* [National Commission on Informatics and Liberty], decision n° 2011-035, 17 March 2011, 17 <http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>.

104 It is important to note that Google was collecting GPS location data at the same time it was collecting Wi-Fi header data: see Stroz Friedberg, above n 15, 7 [35].

105 *Dutch DPA Final Findings*, above n 40, 29.

106 Ibid 18–20.

107 *Commission Nationale de l'Informatique et des Libertes* [National Commission on Informatics and Liberty], decision n° 2011-035, 17 March 2011, 16 <http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>.

with the Wi-Fi payload data collected by Google.[108] As highlighted above, the New Zealand Privacy Commissioner may have also reached a similar conclusion regarding the combination of an individualised SSID and location data. For example, if an SSID has been customised with an individual's name, it then becomes a simple matter to cross-reference that name with address information, such as public registers or telephone directories, to confirm the identity of an individual.

It is necessary to consider the construction of 'reasonably ascertainable' to determine whether MAC addresses and SSID data could be classified as personal information in Australia. The use of 'ascertainable' in s 6(1) anticipates the need to refer to extraneous material.[109] Similarly, the words 'from information or opinion' should not be read as limiting recourse to the information alone, unlike the 'apparent' form of personal information.[110] However, the ascertainment of identity is qualified through the word 'reasonably'.[111] Reasonableness is more than a mere possibility, conjecture or speculation that identity can be ascertained; it translates to a *likelihood of actual identification*.[112] Identification will not be reasonable where it requires accessing multiple databases and cross-matching information and further 'cross-matching with an external database'.[113] Reasonable identification in Australian law therefore requires 'moderate steps' to cross-reference material, such as the ability of a member of the public looking up title particulars of a property including the name of the owner.[114]

As highlighted above, judicial and regulatory examination of reasonableness also has to take into account the context in which the organisation collects information. A piece of information is less likely to be categorised as personal information if the collecting organisation has few information resources and would not be able to easily or quickly identify an individual by cross-referencing the information in

108 The Wi-Fi collection process developed by Google ensured that both payload and header data was collected. As a consequence, identification of individuals would be more likely through Google's collection of payload data, which includes emails, websites and passwords and potentially bank account details, which could easily be aggregated with header data to reveal identity. See, eg, *Dutch DPA Final Findings*, above n 40, 12:

> Another example from the payload data concerns the inbox of a client of a webmail provider. Based on the timing of the emails, the addresses of the senders and, in particular the subject line, it is possible to reconstruct an accurate picture of moments in the life of this data subject, his interests and his career development.

109 *Re WL and La Trobe University* (2005) 24 VAR 23, 33–4 [47], citing *Bailey v Hinch* [1989] VR 78.

110 *Re WL and La Trobe University* (2005) 24 VAR 23, 33 [44]–[45]; *Re Lobo and Department of Immigration and Citizenship* (2011) 56 AAR 1; Graham Greenleaf, 'Key Concepts Undermining the NPPs — A Second Opinion' [2001] *Privacy Law and Policy Reporter* 20. For an example of 'apparent' identification, see *Seven Network* (2004) 148 FCR 145, 166 [45].

111 *Re WL and La Trobe University* (2005) 24 VAR 23, 33 [42], [44]–[45].

112 *X v Transport Company* [2007] PrivCmrA 26 (December 2007); *Re Lobo and Department of Immigration and Citizenship* (2011) 56 AAR 1, 97–8 [302]; *OS v Mid-Western Regional Council [No 3]* [2011] NSWADT 2304 (29 September 2011) [20].

113 *Re WL and La Trobe University* (2005) 24 VAR 23, 34 [52]; *WL v Randwick City Council [No 2]* [2010] NSWADT 84 (6 April 2010) [30]; *Seven Network* (2004) 148 FCR 145, 166 [45].

114 *Re WL and Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [16]–[17], cited in *Marrickville Legal Centre v Chief Commissioner of State Revenue* [2012] NSWADT 98 (23 May 2012) [44].

question with other information held by it.[115] However, the converse also occurs. It is more likely that a piece of information will be categorised as personal information if the collecting organisation has significant information resources and the cross-referencing is not prohibitive in terms of cost or difficulty.[116]

Google insisted it did not collect information about individual householders and it could not identify an individual from the data collected.[117] However, the investigations by the Dutch DPA and CNIL indicate otherwise. According to the Dutch DPA, Google apparently failed to appreciate its own aggregation skills and resources:

> Google itself, pre-eminently, has the means to identify the individual owners of the Wifi routers. The effort Google would have to make to identify the homeowners with the aid of the data it already holds, and the continuous measurements, cannot be considered to be disproportionate, in particular in view of the fact that it is precisely Google itself that has access to an enormous potential of capable technicians and computer scientists. Google can perform this identification from its own offices on the basis of data the company already holds and receives on a daily basis.[118]

Google is a world-leader in data collection and aggregation processes and it should be viewed contextually as having significant resources to aggregate the Wi-Fi header data collected in the Street View exercise with other data held by Google or other data that is publically available. Google's own customisation of the Wi-Fi collection process used in the Street View scandal demonstrates its ability to collect information that is way beyond the reasonable expectations of normal data-collecting organisations.[119] As such, what are 'moderate steps' for Google in the context of identifying individuals from the Wi-Fi data collected would be giant leaps for most organisations. None of the aggregation activities required to identify an individual in a reasonably ascertainable sense would have been prohibitive for Google in terms of costs and resources.[120] Furthermore, because Google took no precautionary measures to prevent the identification of individuals, it could not rely on a potential defence that data aggregation processes would have been beyond 'moderate steps'.[121] Google could have held collected Wi-Fi data separately, sent data to different servers or employed security measures to prevent the cross-matching of data.[122] However, Google did not take

115 *Re WL and La Trobe University* (2005) 24 VAR 23, 33–4 [44]–[47]. Cf *WL v Randwick City Council [No 2]* [2010] NSWADT 84 (6 April 2010) [27]–[29].

116 Ibid.

117 Fleischer, 'Data Collected by Google Cars', above n 23, 1.

118 *Dutch DPA Final Findings*, above n 40, 29.

119 See, eg, *FCC Liability Notice*, above n 11, 15 [31], regarding the effort that Google put into this collection project. See also *Dutch DPA Final Findings*, above n 40, 23, regarding Google's considerable data processing powers.

120 See, eg, *Canadian Investigation Letter*, above n 33, [18]. See also Scassa, above n 68, 207–8, regarding the aggregation of information to identify an individual in Street View photographs.

121 See, eg, *Re WL and La Trobe University* (2005) 24 VAR 23, 33–4 [44]–[47]. Cf *WL v Randwick City Council [No 2]* [2010] NSWADT 84 (6 April 2010) [27]–[29].

122 See *Re WL and La Trobe University* (2005) 24 VAR 23, 33–4 [44]–[47].

such measures which had the effect of enabling identification of individuals from the collected Wi-Fi header data. All of which points to the conclusion that the Wi-Fi header data collected by Google was personal information in a 'reasonably ascertainable' sense.

In summary, we contend that Wi-Fi header data collected by Google was capable of being classified as personal information under the *Privacy Act*. The Wi-Fi header data was likely to be personal information in an apparent sense due to the customisation of SSID and the collection of SSID and MAC address data in conjunction with location data. Furthermore, the Wi-Fi header data was personal information in a reasonably ascertainable sense as Google would have been able to aggregate the collected data with other data sources to enable identification of individuals. The next step is to examine whether Google's collection of Wi-Fi header data breached the requirements of *NPP* 1.

B *Was Google's Collection of Wi-Fi Header Date in Breach of* NPP *1?*

The *Privacy Act* regulates the collection of personal information.[123] The concept of collection is construed broadly under the Act, and a collection takes places when an organisation gathers, acquires or obtains personal information from any source and by any means.[124] The act of collection requires taking active steps to obtain information.[125] Collection will be perceived to have taken place in situations where the organisation intends to retain the collected information for present or future uses.[126] It should also be noted that, in general, the consent of an individual is not required for collections of personal information under the NPPs. However, the consent of the individual is required for the collection of sensitive information.[127] As regards the application of *NPP* 1, three issues have to be addressed. They are whether Google's collection of Wi-Fi header data was:

1. Necessary and directly related to one of Google's functions;
2. Fair and lawful; and
3. Whether individuals were notified about the collection of Wi-Fi header data.

123 See *Privacy Act* s 8.

124 Office of the Privacy Commissioner, 'Guidelines to the National Privacy Principles' (2001) 22 ('*NPP Guidelines*').

125 See *Seven Network* (2004) 148 FCR 145, 166–7 [45]–[46] (Gyles J).

126 *NPP Guidelines*, above n 124, 22.

127 The collection of sensitive information is not covered in this article, but it is likely that it would have been a relevant consideration given the ability to customise SSIDs.

1 NPP *1.1 — Necessary and Directly Related*

An organisation must only collect information that is 'necessary' for one or more of its prescribed functions or activities.[128] The requirement of necessity is based on the present actualities of the collecting organisation and it would generally not be acceptable for an organisation to collect personal information for a prospective future use. The Australian Privacy Commissioner interprets questions of necessary collection in a practical sense, taking into account the organisation's functions and requirements. The Commissioner has said: 'If an organisation cannot in practice effectively pursue a legitimate function or activity without collecting personal information, then the Commissioner would ordinarily consider it necessary for that function or activity'.[129]

The word 'necessary' has undergone considerable judicial discussion in a constitutional context, but remains relatively untouched in relation to the *Privacy Act*.[130] 'Necessary' is contextual: it attracts 'different degrees of scrutiny'[131] or 'shades of meaning'.[132] It connotes more than mere utility or desirability,[133] but does not necessarily mean absolutely essential, 'indispensable' or unavoidable.[134] Rather, information is necessary when it is reasonably appropriate and adapted to the functions and activities of an organisation.[135] Expressions commonly employed in substitution of the word 'necessary' include 'fulfilment of a legitimate purpose' or 'proportionality'.[136] Baroness Hale in *Campbell v MGN Ltd* further extended the description of 'necessary' in a privacy context as meeting a 'pressing social need' through including 'no greater than is proportionate to the legitimate aim pursued' and providing 'relevant' and 'sufficient' reasons 'for this purpose'.[137] The 'necessity' of collection methods therefore requires a consideration of 'what [an] organisation says it does and what it actually does'.[138] Thus the purpose of *NPP* 1.1 is to 'regulate the manner by which the [collection] function is carried

128 *Privacy Act* sch 3 cl 1.1 ('*NPP*').

129 *NPP Guidelines*, above n 124, 27.

130 *Mulholland v Australian Electoral Commission* (2004) 220 CLR 181, 194–5 ('*Mulholland*').

131 Ibid 195 [39].

132 *Mulholland* (2004) 220 CLR 181, 195 [41] (Gleeson CJ).

133 *Seven Network* (2004) 148 FCR 145, 166 [46] (Gyles J); *Mulholland* (2004) 220 CLR 181, 195; *Re An Inquiry under the Company Securities (Insider Dealing) Act 1985* [1988] AC 660, 704. In the context of s 236(1) of the *Telecommunications Act 1991* (Cth), see *General Newspapers Pty Ltd v Telstra Corporation* (1993) 45 FCR 164, 202 (Gummow J), citing *Re An Inquiry under the Company Securities (Insider Dealing) Act 1985* [1988] AC 660, 704, cited with approval in Office of the Federal Privacy Commissioner, *Complaint Determination No 4 of 2004*, 16 April 2004, para 48 ('*Tenants' Union Determination*'). The Federal Privacy Commissioner said: 'in ordinary usage it may mean, at one end of the scale, "indispensable" and at the other end "useful" or "expedient"'.

134 *Mulholland* (2004) 220 CLR 181, 194–5 [39]; *Ronpibon Tin NL v Federal Commissioner of Taxation* (1949) 78 CLR 47, 56, citing *Commonwealth v The Progress Advertising and Press Agency Co Pty Ltd* (1910) 10 CLR 457, 469 (Higgins J); *McCulloch v Maryland*, 17 US 316, 413–14 (1819), cited in *Tenants' Union Determination* para 49.

135 *Mulholland* (2004) 220 CLR 181, 194–5 [39], citing *McCulloch v Maryland*, 17 US 316, 413-414 (1819); *Ronpibon Tin* (1949) 78 CLR 47, 56; *Commonwealth v The Progress Advertising and Press Agency Co Pty Ltd* (1910) 10 CLR 457, 469 (Higgins J).

136 *Mulholland* (2004) 220 CLR 181, 192.

137 *Campbell v MGN Ltd* [2004] 2 AC 457, 497 [139], cited in *Mulholland* (2004) 220 CLR 181, 194–5.

138 *Tenants' Union Determination* para 58.

out' and to assist in the prevention of surreptitious behaviour outlined below in relation to *NPP* 1.2.[139] The 'necessary' requirement consequently is a balancing factor that serves to limit the information justifiably obtained by organisations.[140]

The necessity of Google's collection was a contentious issue in the regulatory investigations. The Canadian Privacy Commissioner stated that Google's 'secret and sweeping' data mining of Wi-Fi payload data exceeded the organisation's stated purposes and was therefore unnecessary.[141] However, the New Zealand Privacy Commissioner found that Google's collection of Wi-Fi header data was a necessary collection in light of Google's functions.[142] Google's purpose for collecting Wi-Fi header data was to improve its geolocation services and thus the collection of 'open Wi-Fi information' was for a necessary purpose especially in the absence of better indicators of location.[143] Both the Dutch DPA and CNIL also reached similar conclusions.[144] The Dutch DPA concluded that Google's collection was legitimate as it would have led to the development of new, in demand and innovative services.

Under *NPP* 1.1, the necessity of Google's actions requires an assessment of its functions and activities including the appropriateness of the software code adopted and its method of collection. Google claimed that its purpose for collecting Wi-Fi header data was to create a Wi-Fi mapping system in order to improve the accuracy of its geolocational services.[145] Google's Wi-Fi header data collection therefore must be examined to ascertain whether the collection was necessary to improve Google's geolocation services. On its face, the collection of Wi-Fi header data could be an appropriate function of Google within the context of product improvement. Google's Wi-Fi access point map would enable Google Map users to turn on 'My Location' and discover their approximate location in relation to cell towers and Wi-Fi access points that were visible to their device.[146] In that sense, it could be strongly argued that Google's collection of Wi-Fi header data was necessary. However, a closer inspection of Google's activities gives rise to alternative interpretations.

139 *Seven Network* (2004) 148 FCR 145, 167 [49] (Gyles J).

140 See ibid 167 [49].

141 Office of the Privacy Commissioner of Canada, 'Report of Findings: Google Inc. WiFi Data Collection' (PIPEDA Report of Findings No 2011-001, 6 June 2011) [21] <http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.asp> ('*Canadian Report of Findings*').

142 Privacy Commissioner (New Zealand), above n 50.

143 Ibid.

144 *Dutch DPA Final Findings*, above n 40, 35, describing the collection as 'a de facto secret collection'. See also *Commission Nationale de l'Informatique et des Libertes* [National Commission on Informatics and Liberty], decision n° 2011-035, 17 March 2011, 17 <http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>.

145 Raphael Leiteritz, *Copy of Google's Submission Today to Several National Data Protection Authorities on Vehicle-Based Collection of Wifi Data for Use in Google Location Based Services* (27 April 2010) Google <http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//googleblogs/pdfs/google_submission_dpas_wifi_collection.pdf>; David Meyer, *Google Explains Why Street View Cars Recorded Wi-Fi Data* (28 April 2010) ZDNet <http://www.zdnet.com/google-explains-why-street-view-cars-record-wi-fi-data-3040088799/>; Fleischer, 'Data Collected by Google Cars', above n 23, 2.

146 Leiteritz, above n 145.

NPP 1 regulates organisational collections of personal information and indicates how those collections should be carried out.[147] For example, in *D v Banking Institution*,[148] the collection of marital status was deemed unnecessary, as it had no bearing on the complainant's eligibility to open an account. Google's collection and storage of SSIDs could be similarly deemed unnecessary regarding the creation of a Wi-Fi map to improve its geolocation services[149] because location services only require signal strength and MAC address data to provide an approximate user location.[150] Thus any collection of personal information, such as a customised SSID, is unnecessary.

It should be noted that there is a broad degree of leeway accorded to organisations regarding the necessity of a collection purpose and how that purpose meets a corresponding business function. Even though Google used a collection process that collected SSID data, Google could still claim that the Wi-Fi header data collected was necessary because of the process of collection. The collection process operated by Google is commonly known as 'wardriving',[151] and it is an easy and cost-effective method of obtaining a large quantity of signals from Wi-Fi enabled devices. The technological limitations of the collection process employed by Google would not necessarily make it an illegitimate collection tool.[152] The collection of SSIDs through wardriving is generally unavoidable and, in the absence of an efficient and cost-effective alternative, Google could argue that it would be inappropriate to alter an existing generally accepted practice.

However, there was no reason for Google to retain the SSIDs, and this information could quite easily have been deleted upon collection. Google's Wi-Fi mapping system was also an aspiration. The collection and retention of data that may or may not be useful in the future could therefore not be classed as necessary.[153] Furthermore, Google's initial assertion that the Wi-Fi data was unknowingly collected through software designed by a rogue engineer also gives rise to questions about the necessity of the collection. An organisation cannot claim that it did not 'expect' or 'intend' to collect personal information[154] but still claim that the collection was necessary to fulfil a business function. Google's initial admission that it did not know about the collection cannot be used to support the contention that it was a necessary collection of Wi-Fi header data.

Accordingly, and in the absence of evidence relating to Google's Australian collection practices, it is not possible to determine specifically whether Google's collection of Wi-Fi header data was in breach of *NPP* 1.1. However, our examination shows that this is a contentious issue and there are strong arguments

147 *Seven Network* (2004) 148 FCR 145, 167 [49].

148 *D v Banking Institution* [2006] PrivCmrA 4 (1 February 2006).

149 See, eg, *Dutch DPA Final Findings*, above n 40, 36.

150 Ibid 30.

151 Edward H Freeman, 'Wardriving: Unauthorized Access to Wi-Fi Networks' (2006) 15(1) *Information Systems Security* 11, 11: wardriving is 'the practice of seeking out and taking advantage of free connection to unsecured wireless networks'.

152 *Tenants' Union Determination* para 47.

153 See, eg, *N v Private Insurer* [2004] PrivCmrA 1 (1 January 2004).

154 See, eg, *M v Financial Institution* [2009] PrivCmrA 16 (November 2009).

both for and against the existence of a breach. It is therefore necessary to examine *NPP* 1.2 and whether Google's collection was fair and lawful.

2 NPP *1.2 — Fair and Lawful Collection*

Under *NPP* 1.2, organisations must collect personal information through 'lawful and fair means and not in an unreasonably intrusive way'.[155] The collection of Wi-Fi header data must not conflict with any existing laws[156] and a 'lawful' collection of data simply means that it is 'authorised, as opposed to not forbidden, by law'.[157] The Australian Government referred the Street View Wi-Fi scandal to the Australian Federal Police (AFP) to investigate whether Google breached the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIA Act*'). Legal advice received by the AFP suggested that Google may have breached the *TIA Act*. However, a prosecution was not pursued due to 'the difficulty in gathering sufficient evidence' and because Google's collection appeared to be 'inadvertent'.[158] The AFP concluded that it was unlikely to secure a prosecution and 'it would not be an efficient or effective use of … resources to pursue [the] matter … further'.[159] It is therefore possible that Google breached the lawful element of *NPP* 1.2 regarding application of the *TIA Act*, but the AFP indicated that it would be difficult, if not impossible, to prove in practice. As such, we consider the complex issue of whether the collection was unfair.

An unfair collection can be one that involves 'intimidation or deception' by the collecting organisation.[160] The relationship between the collecting organisation and the individual, and the degree of inequality that exists between the two, is therefore a key point of analysis.[161] In the Street View scandal, there is no pre-existing relationship between Google and the Wi-Fi access point holders. The presence of a pre-existing relationship may provide a degree of adequate notice[162] or demonstrate that the individuals were trading their Wi-Fi header data for the provision of a valuable service. Google could have balanced this inequality by providing sufficient notice of its Wi-Fi collection intentions or by providing an opt-out option.[163] The latter would have established a relationship and would have engendered a higher degree of equality through advance notification and

155 *NPP* cl 1.2.

156 Ibid.

157 *Taikato v The Queen* (1996) 186 CLR 454, 460 (Brennan CJ, Toohey, McHugh and Gummow JJ), quoted in *NX v Office of the DPP (NSW)* [2005] NSWADT 74 (4 April 2005) [21], in turn quoted in *WL v Randwick City Council* [2007] NSWADTAP 58 (5 October 2007) [45].

158 Australian Federal Police, 'Media Release: Finalisation of Google Referral' (Media Release, 3 December 2010) <http://www.afp.gov.au/media-centre/news/afp/2010/december/finalisation-of-google-referral.aspx>.

159 Ibid.

160 *Seven Network* (2004) 148 FCR 145, 167 [48].

161 Ibid.

162 See, eg, *I v Contracted Service Provider to Commonwealth Agency* [2008] PrivCmrA 9 (26 June 2008).

163 This point was also a key element in the Dutch DPA's examination of the issue. See *Dutch DPA Final Findings*, above n 40, 39.

an opportunity for Wi-Fi access point holders to not participate in Google's collection.[164]

This is an important point because a relevant consideration regarding the 'fairness' of Google's collection is how it represented its actions to the public.[165] For example, in *J v Utility Co and Industry Group*, the Australian Privacy Commissioner took into consideration that the company had acted contrary to its own privacy policy.[166] A fair collection is consequently undertaken in circumstances that give rise to a reasonable expectation that the collected information would be recorded. An unfair collection can therefore arise in circumstances where the collector misleads or deceives the information holder concerning collection, the identity of the collector and the use of information. The Dutch DPA argued that Google's collection was de facto secret and thus deceptive because it was conducted under the guise of a photographic exercise. Accordingly, Wi-Fi access point holders were denied an opportunity to opt-out of the collection by adjusting their standard behaviour, such as switching off the access point at the time of Google's collection.[167]

Google could counter-argue that its collection of Wi-Fi header data was compatible with its privacy policy in place at the time of the Street View scandal. Google's policy stated that it only processed personal information for specified purposes and that it would only collect personal information needed to provide or improve its services.[168] However, it is questionable whether Google's Wi-Fi collection was in compliance with its own privacy policy. First, regardless of whether SSIDs were inadvertently collected in the wardriving process, Google's retention and storage of SSID data contravenes its own privacy policy as the data was not needed by Google to improve its geolocation services.[169] Second, a public statement made by Google at the time of the Street View collection also casts doubt on the veracity of Google's compliance with its own privacy policy. In 2009, Google's Global Privacy Counsel, Peter Fleischer, rebutted criticism by a British MP in an article published in *The Times*: 'We're proud of our track record of protecting user privacy. We work hard to make sure our users understand what

164 See ibid 39. However, the complexity of the opt-out system was criticised as it is based on the requirement of Wi-Fi access point holders to change their SSID.

165 See, eg, *Tenants' Union Determination* paras 57–8.

166 [2006] PrivCmrA 9 (1 April 2006).

167 *Dutch DPA Final Findings*, above n 40, 35.

168 See, eg, Google Inc, *Policies and Principles: Privacy Policy* (11 March 2009) <http://www.google.com.au/policies/privacy/archive/20090311-20101003/>. Google's data integrity policy stated:

> Google processes personal information only for the purposes for which it was collected and in accordance with this Privacy Policy or any applicable service-specific privacy notice. We review our data collection, storage and processing practices to ensure that we only collect, store and process the personal information needed to provide or improve our services or as otherwise permitted under this Policy. We take reasonable steps to ensure that the personal information we process is accurate, complete, and current, but we depend on our users to update or correct their personal information whenever necessary.

169 See *Dutch DPA Final Findings*, above n 40, 38: 'Google can leave the SSIDs (network names) out of the Google CLS and limit itself to the combination of the BSSIDs and their calculated locations to offer location approximation services. The lack of a need to process the SSIDs means that there is no justified purpose for their collection'.

data we collect and how we use it, because we are committed to transparency and user choice'.[170]

Google's Street View Wi-Fi collection contravenes Fleischer's statement because Google failed to notify Wi-Fi access point holders about the collection of their Wi-Fi header data and initially tried to deny its collection.[171] At the time Fleischer made this statement, Google was secretly collecting Wi-Fi data across the globe which in no sense accords to the commitment to transparency and user choice professed in the statement.[172] Google could argue that it did not consider Wi-Fi data to be personal information, so it therefore did not intend to breach information privacy law and the privacy of its users. However, it is important to note that Fleischer's statement simply refers to 'data' that Google collects and uses. Google's commitment to transparency does not simply involve personal information.

Finally, and most importantly, it is the surreptitious nature of Google's Wi-Fi collection that is most likely to make the collection of Wi-Fi header data an unfair collection under *NPP* 1.2. Google admitted to the collection three years after the collection started, and only because of vigorous questioning by German privacy regulators. Putting these two facts together, it would seem that Google had no intention of notifying anyone about the Wi-Fi collection which makes it more likely that the collection would be deemed to be deceptive and thus unfair. Google's fabricated 'rogue engineer' defence would also indicate that there was a concerted effort to deceive individuals and regulators about the collection. We contend that Google breached *NPP* 1.2 and will now conclude our investigation of Google's *NPP* 1 obligations by examining the requirements of *NPP* 1.3.

3 NPP *1.3 — Notification to Individuals*

NPP 1.3 has a direct connection to the unfair collection of personal information. It requires organisations that collect personal information from an individual to take reasonable steps to notify the individual about the collection.[173] Although it is a requirement to take 'reasonable steps' to provide notification,[174] the Australian Privacy Commissioner has not recommended any particular method of notification.[175] Instead, it is left to organisations to determine the most appropriate form of notice. Hence, the insertion of a reasonableness element in *NPP* 1.3 provides a standard of what is realistically expected from the organisation. Under

170 Peter Fleischer, 'British MP David Davis, Google, and Setting the Record Straight' on *Google Europe Blog* (27 July 2009) <http://googlepolicyeurope.blogspot.com.au/2009/07/british-mp-david-davis-google-and.html>.

171 See *FCC Liability Notice*, above n 11, 1 [2].

172 See *Canadian Report of Findings*, above n 141, [51]. For an examination of how Google constructs the concept of privacy, see Chris Jay Hoofnagle, 'Beyond Google and Evil: How Policy Makers, Journalists and Consumers Should Talk Differently about Google and Privacy' (2009) 14(4) *First Monday* <http://journals.uic.edu/ojs/index.php/fm/article/view/2326/2156>.

173 *NPP* cl 1.3.

174 *NPP* cl 1.5, cited in *Tenants' Union Determination* para 70.

175 See *Tenants' Union Determination* para 72.

this flexible standard, notification is not always required prior to the collection of personal information.[176] Reasonable steps as regards the timing of notice therefore depend on balancing organisational business requirements and individual privacy interests.[177]

Indeed, the NPPs are not intended to prescribe requirements that could limit the effective operation of organisations.[178] Consequently, organisational cost, convenience and practicality of prior notification are key factors regarding the need to notify and the appropriate choice of notification under *NPP* 1.3.[179] Determinations regarding notification are also contextual because the nature of the organisation, the type of information collected and the potential detrimental impact on an individual are other significant factors in deciding the appropriate method of notification.[180] The content of notice should also include certain elements such as the contact details of the collecting organisation, the purpose of collection and whether the collection was required or authorised under law.[181] For example, in *I v Contracted Service Provider to Commonwealth Agency*, notification through a signed Conditions of Entry form was deemed inadequate because the form used for notification did not disclose the purpose of the collection.[182] Transparency of information collection processes is thus a key element of the rationale behind notification.

Notification does not have to be made to each individual as this may be impractical and costly. In such situations, a public notice or visible signage may suffice.[183] Furthermore, it is possible to disclose more than one 'purpose' when notifying individuals about the collection of information, unless that information is prone to misinterpretation.[184] In *P and Retail Co*, a complaint that involved the recording of telephone conversations with a customer without proper authorisation, the Australian Privacy Commissioner decided that a degree of specificity was required for notification, such that a notification of the recording of inbound calls did not amount to sufficient notice for the recording of outbound calls.[185]

There is a large degree of flexibility for organisations when taking reasonable steps to provide notification as regulatory requirements are weighted significantly against organisational exigencies. Organisations are only required to take reasonable steps to notify individuals and it is not intended that the obligations of *NPP* 1.3 have absurd implications.[186] Nevertheless, it is likely that Google failed to provide adequate notification in relation to its collection of Wi-Fi header data.

176 See ibid paras 34–6.

177 Ibid.

178 Ibid para 35.

179 *NPP Guidelines*, above n 124, 28.

180 *Tenants' Union Determination* paras 85, 87.

181 *NPP* cls 1.3(a)–(f).

182 *I v Contracted Service Provider to Commonwealth Agency* [2008] PrivCmrA 9 (26 June 2008).

183 *H and Registered Club* [2011] AICmrCN 2 (22 December 2011); *T v Private Community Centre* [2008] PrivCmrA 20 (29 August 2008).

184 *Tenants' Union Determination* paras 72–3.

185 [2011] AICmrCN 10 (22 December 2011).

186 Ibid.

Google dominates the online advertising market and controls the world's most popular online search engine. Google has a mechanism to communicate directly and instantaneously to an international audience of Wi-Fi access point holders. This point goes against Google because it would have been relatively easy for it to take reasonable steps to notify individuals about the collection. Google had already developed a site that provided details about the employment of Google Street View vehicles to assuage concerns about surreptitious photography.[187] It would have been a trivial matter for Google to add details about its Wi-Fi collection practices and thus provide notification of the collection. For instance, the Dutch DPA deemed Google had sufficient means to inform Dutch Wi-Fi access point holders about the Wi-Fi data collection through its websites, press releases and targeted advertisements, and by making its cars more identifiable. Google had already undertaken similar activities in Germany and it would not have been burdensome to expect Google to undertake similar processes in Holland.[188]

Under *NPP* 1.3, an organisation may not have to provide notice where the collection is 'obvious' or readily apparent.[189] The process of collection is an important consideration especially regarding the use of new technologies which may make it impracticable for an organisation to notify every individual about a collection of personal information.[190] Google could argue that the Street View image collection was apparent as it provided public notice of the collection. However, Google cannot claim that individuals should have known about the collection of Wi-Fi header data, as part of the Street View image collection, because the corporation effectively kept it secret and thus any defence that Wi-Fi access point holders should have reasonably expected Wi-Fi header data to be collected would fail,[191] as highlighted by the Canadian Privacy Commissioner.[192]

In conclusion, we contend that Google breached *NPP* 1.3 by failing to provide notification to wireless access point holders about the Street View Wi-Fi collection. A greater focus on notification would also have created a more rigorous process of risk assessment regarding the necessity of collecting Wi-Fi header data in the first place.[193] If Google had undertaken such a process, it is likely that the scandal would not have manifested in the way it did.

IV REPERCUSSIONS FOR PRIVACY REGULATION

We contend that the collected Wi-Fi header data should have been classed as personal information and that Google may have breached certain elements of

187 Google Inc, *Behind the Scenes: Street View* <http://www.google.com.au/maps/about/behind-the-scenes/streetview/>.

188 See *Dutch DPA Final Findings*, above n 40, 35–6.

189 *NPP Guidelines*, above n 124, 28.

190 Tim Dixon, CCH, *Australian Privacy Commentary* (at 21 March 2013) ¶5-250.

191 See, eg, *Tenants' Union Determination* para 73.

192 See *Canadian Investigation Letter*, above n 33.

193 See, eg, *NPP Guidelines*, above n 124, 28.

NPP 1. The findings of our research accordingly raise questions about the efficacy of the Australian response to the scandal. We therefore conclude our article by: (a) examining the immediate actions taken by the then Privacy Commissioner; (b) examining the subsequent attempts to clarify the legal position of Wi-Fi header data, both from an Australian and EU perspective; and (c) identifying the lack of a reasoned based for regulatory decision-making in Australia.

A *The Immediate Response*

Part II detailed the regulatory investigations prompted by Google's collection of Wi-Fi header data. Most notably, the regulators in France and Holland concluded — after technologically rigorous and legally sophisticated analysis — that Wi-Fi header data should be classed as personal information under their respective laws. The then Australian Privacy Commissioner decided that a formal investigation was not required. We now outline the immediate response of the Privacy Commissioner. By doing so, we highlight some significant differences in regulatory approach involving the willingness to examine contemporary privacy issues derived from technological developments.

As highlighted in Part II, the Australian Privacy Commissioner conducted an OMI into the collection of payload data. The Commissioner adopted a conciliatory approach with Google due to the lack of powers in relation to OMIs, as highlighted by the following media statement:

> Under the current Privacy Act, I am unable to impose a sanction on an organisation when I have initiated the investigation. My role is to work with the organisation to ensure ongoing compliance and best privacy practice. This was an issue identified by the Australian Law Reform Commission (ALRC) inquiry into Australian privacy laws. The ALRC recommended that the enforcement regime be strengthened. My Office supports these recommendations, and the Australian Government has announced its intention to adopt them.[194]

As a consequence of the Commissioner's approach, the discussions between Google and the OAIC were kept confidential and so the only publically available information that provides an insight into the Commissioner's actions are media statements. The entirety of the Commissioner's published legal analysis of whether the Wi-Fi header data collected by Google constituted 'personal information' under s 6(1) of the *Privacy Act* is encapsulated in two statements to the media. The first statement, in a Fairfax media article, put the view that '[f]rom a privacy perspective, our preliminary inquiries have indicated that the information about Wi-Fi data that Google is collecting would not be considered personal information

194 Office of the Australian Information Commissioner, 'Australian Privacy Commissioner Obtains Privacy Undertakings from Google' (Privacy Statement, 9 July 2010) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/google-street-view-wi-fi-collection/australian-privacy-commissioner-obtains-privacy-undertakings-from-google>. The current Privacy Commissioner will receive a suite of new powers in relation to OMIs flowing from the implementation of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

under the *Privacy Act*'.[195] The second statement, on ABC Radio National's PM programme, was that '[o]ur preliminary inquiries have indicated generally that the information about WiFi networks that Google is collecting would probably not on its own be considered personal information under the *Privacy Act*'.[196]

Given the detailed legal and technical analysis that was conducted in other jurisdictions, it is surprising that this complex legal issue was dealt with in such a brief manner. What is astonishing, however, is the fact that the two media statements are incompatible. The first statement clearly indicated that the Commissioner's preliminary inquiries did not consider 'information about Wi-Fi data', which presumably means Wi-Fi header data, to be personal information under the *Privacy Act*. However, the second statement, which was made on the same day, indicated the Commissioner's preliminary inquiries found that 'information about WiFi networks', which again is presumably Wi-Fi header data, would generally not be personal information if it was collected on its own.

The second statement therefore contradicts the first statement because it is possible for Wi-Fi header data to be personal information if it is collected with other information that can be aggregated to reveal an identity, such as location data, as highlighted above. It is difficult to determine what the Commissioner was actually trying to say with these two statements but she seemed to be referring to the crucial distinction between context dependent and context independent approaches to classifications of personal information. As highlighted in Part III(A), this distinction plays a crucial part in any attempt to determine whether Google's collection of Wi-Fi header data breached the *Privacy Act*. We concluded that Wi-Fi header data was likely to be personal information in both an apparent and reasonably ascertainable sense. This corresponds with the New Zealand investigation which is important given the similarities between the New Zealand and the Australian privacy legislation.

The Commissioner's analysis of 'information about Wi-Fi data' or 'information about Wi-Fi networks' was incomplete, but more importantly, was also incorrect. This would indicate that the 'preliminary inquiries' conducted by the Commissioner were ineffective which is signified by the use of 'probably' in the Commissioner's second statement. Moreover, given the level of Google's obfuscation in the inquiries conducted by the Dutch DPA and the FCC,[197] it should be no surprise at all that the Commissioner's 'preliminary inquiries' did no more than produce a result that was undoubtedly favourable to Google. As such, it could be argued strongly that the regulatory response to this issue was simply inadequate and did not attempt to examine the complex legal issues that arise

195 Hearn, 'Please Explain: Why Google Wants Your Wi-Fi Data', above n 56.

196 Griffiths, above n 56.

197 *Dutch DPA Final Findings*, above n 40, 4–5, regarding Google's continuous delays. See also *FCC Liability Notice*, above n 11, 2 [4], detailing Google's attempt to deliberately impede and delay the investigation and Google's wilful and repeated violations of Commission orders.

in any meaningful sense.[198] Furthermore, the lack of appropriate response has significant implications for the development of a regulatory discourse emanating from the application of the *Privacy Act* which is exemplified by the decisions made subsequent to the Google scandal.

B *Comparison of Subsequent Legal Determinations*

The importance of the Google scandal does not just lie in the immediate actions or inactions of regulatory authorities. As highlighted in Part I, the issue of whether Wi-Fi header data is personal information is of material importance because it potentially could have a significant effect on the collection practices of new Location-Based Service industries. We therefore examine regulatory opinions about whether Wi-Fi header data is personal information in Australia and the EU. We contrast the opinion produced by the EU's Article 29 Data Protection Working Party with the only direct statement on this topic produced by the OAIC, a report of an OMI into a potentially similar fact situation to the Google scandal. Again, this comparison highlights significant differences in the consideration of policy and the role of a privacy regulator as a developer of information privacy related guidance and law.

Following the Google scandal, the Article 29 Data Protection Working Party published an opinion on geolocation services that examined whether Wi-Fi header data should be considered personal data under the *Data Protection Directive*.[199] The *Working Party Opinion* details the data protection implications of different types of organisations using different types of geolocation services and the three different types of geolocation infrastructure, GPS, Global System for Mobile Communications (GSM) and Wi-Fi. The *Working Party Opinion* provides a detailed overview of the legal implications of collecting geolocation data, including Wi-Fi header data, across a number of different telecommunications sectors that involve a number of different actors. For the purpose of this article, it is only necessary to focus on the Article 29 Data Protection Working Party's perspective on whether Wi-Fi header data transmitted from Wi-Fi access points is personal data.

The Article 29 Data Protection Working Party concluded that a MAC address of a Wi-Fi access point is capable of being personal data when it is collected with location data because the location of the Wi-Fi access point is 'inextricably linked' to a property location which can then be linked to the owner of the access point.[200] The location of a Wi-Fi access point can be fine-tuned by further analyses,

198 This is potentially an example of Lindsay's conceptualisation of the 'purely consequentialist considerations' of certain applications of information privacy law, and the reduction of the complex social and legal issues inherent in the 'privacy implications of data processing' to 'narrowly focused technocratic procedures of information management': see David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131, 165.

199 See generally *Working Party Opinion*, above n 4.

200 Ibid 11.

such as the use of signal strength and through the ongoing use of the geolocation service which creates further precision.[201] As such, in sparsely populated areas, the MAC address will point towards a single property from which the owner can be identified easily by aggregating home ownership details, electoral register details or white page directories. In more densely populated areas, the use of MAC address with signal strength and SSID can be used to determine the precise location of an access point and to ascertain the identity of an individual where the access point is located. However, in very densely populated areas, it would not be possible to precisely identify the location of an individual from a MAC address and other information collected without 'unreasonable effort'.[202]

Nevertheless, the Article 29 Data Protection Working Party concluded that a combination of a Wi-Fi access point MAC address collected with other Wi-Fi header data and location data should always be treated as personal data even if, in some cases, it is not possible to identify an individual without unreasonable effort:

> Under these circumstances and taking into account that it is unlikely that the data controller is able to distinguish between those cases where the owner of the WiFi access point is identifiable and those that he/she is not, the data controller should treat all data about WiFi routers as personal data.[203]

The Article 29 Data Protection Working Party also concluded that even though geolocation service data controllers did have a legitimate interest in the collection of Wi-Fi header data, this interest had to be balanced by the provision of opt-out mechanisms for collection and by not collecting or processing SSID data.[204] Thus the Article 29 Data Protection Working Party has provided a clear, detailed and sophisticated opinion of the legal status of Wi-Fi header data under the *Data Protection Directive*. It should also be reiterated that the *Working Party Opinion* goes much further than the implications of Wi-Fi access points and provides a detailed consideration of the complex legal issues on an industry-wide basis. The *Working Party Opinion* therefore provides clear and unambiguous guidance that sets out identifiable legal obligations for geolocation service industries.

We can contrast this with the only available analysis produced by the OAIC in *Own Motion Investigation v Information Technology Co*.[205] In December 2010, the OAIC, under the leadership of the newly appointed Australian Privacy Commissioner, Timothy Pilgrim, published the results of an OMI against an unnamed information technology company. The report is only 246 words in length and it is not clear on what basis an investigation was conducted. OMIs are often instigated following the reporting of a suspected breach of privacy via the

201 Ibid.
202 Ibid.
203 Ibid.
204 Ibid 17.
205 [2010] PrivCmrA 24 (24 December 2010) ('*ITC Investigation*').

media or by an organisation self-reporting an incident.[206] The only reference to the investigation's basis is a rather cryptic version of the facts: 'The Commissioner received information that suggested that an information technology company was collecting geographical location data about mobile phone customers who used its location-based services'.[207]

It is unclear whether the Commissioner received a complaint about the collection or even what the collection actually entailed. For example, was it Wi-Fi header data transmitted from Wi-Fi access points or Wi-Fi header data from smart mobile devices?[208] The facts seem to indicate that collected data was 'about mobile phone customers' rather than Wi-Fi devices which again causes confusion.[209] It is even uncertain what type of Location-Based Service was used. It is therefore difficult to understand the factual circumstances of this investigation as it is unclear from the stated facts what the investigation actually referred to. Furthermore, it is not even clear on what legal basis the Commissioner believed that the *Privacy Act* may have been breached. The definition of personal information is mentioned and there is a passing mention of *NPP* 1.2 without any reference to the facts at hand.

The substantive outcome of the investigation was:

> The investigation revealed that the information technology company was not collecting personal information through the use of its location-based services, as defined in the Privacy Act.
>
> Instead, when the information technology company received a customer request for data about their current location from a mobile device, it collected information about nearby cell towers and Wi-Fi access points, and then sent this information back to the customer's device. The customer's device then used this information to determine the customer's exact location. Neither the exact location of the device nor identifying information about the customer was sent back to the information technology company.
>
> The Commissioner considered that individuals could not be identified from the information collected by the information technology company through its location-based services. As the information did not meet the definition of 'personal information', the information technology company's activities in relation to this matter were not subject to the Privacy Act. Therefore the Commissioner ceased the own motion investigation into the matter.[210]

We do not intend to critically analyse the outcome of this investigation as it is impossible to do so without a clearer set of facts. However, as highlighted

206 Paterson, above n 57, 62 [2.58].

207 *ITC Investigation* [2010] PrivCmrA 24 (24 December 2010).

208 This is an important point because the information privacy considerations are very different depending on what type of device the data is collected from, as highlighted in *Working Party Opinion*, above n 4, 7.

209 For example, contrast the facts of the OMI with the previous Privacy Commissioner's statements made during the Google scandal 'information about Wi-Fi data' or 'information about WiFi networks': see Part IV(A).

210 *ITC Investigation* [2010] PrivCmrA 24 (24 December 2010).

throughout the course of this article, the use of MAC address data is integral to the operation of Location-Based Services. For a customer's device to receive location data from the information technology company's Location-Based Services, the MAC address of the device would have to be provided.[211] This may or may not be implicitly confirmed by the Commissioner's determination that '[n]either the exact location of the device nor identifying information about the customer was sent back to the information technology company'.[212] There is nothing in this statement to confirm that the MAC address was not sent by the device to the company as would be expected. This is an important point as the *Working Party Opinion* clearly indicates that a MAC address, particularly of a mobile device,[213] should be classed as personal data, and the legal analysis conducted in this article also supports that proposition. Consequently, on one interpretation of the *ITC Investigation*, it is possible to reach the conclusion that a MAC address of a mobile Wi-Fi device, particularly a mobile phone, should not be classed as personal information, which is in direct disagreement with the policy position being put forward in the EU. That itself is not problematic as it has been well documented that different jurisdictions have different interpretations and priorities regarding information privacy protection.[214] The levels of legal protection accorded to personal information are not fixed and are sensitive to the needs of each individual jurisdiction.

The *ITC Investigation* was published before the *Working Party Opinion*, so the OAIC obviously would not have been able to consider its content in drafting the report. However, the detailed reports of the Dutch and French DPAs were available but were not referred to. More importantly, the OAIC has done little since the publication of the *Working Party Opinion* to clarify its own interpretation of whether a MAC address broadcast from a Wi-Fi access point or a Wi-Fi enabled smart device should be classed as personal information. In fact, a recent guideline produced by the OAIC further confuses this important issue.

In September 2013, the OAIC released a guideline regarding better privacy practices for mobile app developers.[215] The *Mobile App Guideline* indicates that certain types of information can be classed as personal information in a reasonably ascertainable sense depending upon the circumstances of collection and use. Two types of information relevant to this article are: Unique Device Identifiers (UDIDs), which can amount to personal information in specified circumstances; and location information, which can reveal user activity patterns

211 See Chow, above n 11, 62: 'the device sends the location provider a request that includes the MAC address, signal strength, SSID, and age of all detected wireless networks. The location provider then uses that data to triangulate a position, and sends back a response that is converted to a usable geolocation for the device' (citations omitted).

212 *ITC Investigation* [2010] PrivCmrA 24 (24 December 2010).

213 *Working Party Opinion*, above n 4, 7: 'A smart mobile device is very intimately linked to a specific individual'.

214 See, eg, Colin J Bennett and Charles D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006).

215 Office of the Australian Information Commissioner, *Mobile Privacy: A Better Practice Guide for Mobile App Developers* (2013) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/better-practice-guide-for-mobile-developers.pdf> ('*Mobile App Guideline*').

and habits.[216] The *Mobile App Guideline* does not provide examples of UDIDs which could be classed as personal information, but it presumably refers to data such as a MAC address. The *Mobile App Guideline* then states that a mobile app privacy policy should inform users about the sharing of behavioural information or *device identifiers* with third parties because '[i]deally, users should be able to opt out of sharing their personal information with third parties'.[217]

Rather than clarifying if and when a MAC address will be personal information, the *Mobile App Guideline* and the *ITC Investigation*, when read in conjunction with each other, produce a confusing array of possibilities. One reading of the *ITC Investigation*, as highlighted above, indicates that a MAC address of a smart mobile device should not be classed as personal information. However, the *Mobile App Guideline* indicates that a MAC address, as a UDID, could be personal information in a reasonably ascertainable sense in certain circumstances. The *Mobile App Guideline* subsequently indicates that users should be able to opt-out of sharing their personal information with third parties and the implication of that statement is that a UDID should therefore always be treated as personal information. Consequently, we have a situation where a MAC address: (1) may not be personal information; (2) could be personal information; and (3) should be personal information. We argue in Part IV(C) that this confused state of affairs arises because of the lack of a reasoned decision-making process founded on clear regulatory and jurisprudential discourse.

C *The Lack of Published Reasoning*

The purpose of the above comparison is not to question the veracity of the *ITC Investigation* and the *Mobile App Guideline* per se. Rather, the comparison of the Article 29 Data Protection Working Party and OAIC approaches to this problem highlights the lack of clarity in the Australian reasoning process, which makes it difficult to generate a healthy and sustained regulatory consideration of vital information privacy law issues.[218]

The *Working Party Opinion* recognises the increasing importance of geolocation information and the privacy implications that arise when location information is aggregated with other information. The purpose of the *Working Party Opinion* is to establish a policy position that accommodates the rapid development of geolocation technologies and their vast uptake on consumer smart mobile devices. These devices have a contingent effect as they not only provide a market for Location-Based Services but they also make it easier to collect location data which in turn provides new opportunities for Location-Based Service industries to expand.

216 Ibid 4.

217 Ibid 12.

218 See Graham Greenleaf, '"Tabula Rasa": Ten Reasons Why Australian Privacy Law Does Not Exist' (2001) 24 *University of New South Wales Law Journal* 262, 266–7, regarding the paucity of determinations and the lack of a meaningful jurisprudence.

Central to the Article 29 Data Protection Working Party's reasoning process is the complex interrelation of rapid technological developments, individual privacy protections and societal benefits that arise from the advent of new technologically oriented markets. It is this reasoning process that founds the scope of the *Working Party Opinion*'s logic, namely, to clearly identify technological infrastructures and the privacy impacts that flow from these infrastructures.[219] The Article 29 Data Protection Working Party is able to consider the implications of technological development in a holistic sense, while clearly indicating the legal protections which individuals can expect and the legal obligations which collectors of personal data are expected to fulfil.

In sum, the *Working Party Opinion* is about establishing a regulatory discourse — a path which enhances legal certainty and which sets the basis for future legal discussion. An example of that path is the *Working Party Opinion*'s consideration of whether a MAC address for a Wi-Fi access point is personal data, as highlighted above. The Article 29 Data Protection Working Party's consideration of this point exemplifies a clear identification of the technological issues, a nuanced understanding of the privacy risks for individuals and the practical consequences that may arise now and in the future for Location-Based Service industries.

However, the same cannot be said be about the OAIC's approach. First, the former Australian Privacy Commissioner's media statements at the time of the Google scandal and the perplexing description of facts in the *ITC Investigation* indicate an imprecise identification of the technological issues. Second, the perceived privacy risks for individuals arising out of the *ITC Investigation* are predicated purely on the basis of being able to identify an individual from the information in question.[220] The *Working Party Opinion*, on the other hand, considers a number of privacy risks that could potentially arise for individuals.[221] The OAIC's limited construction of risk could emanate from the *Privacy Act*'s definition of personal information, which, as previously discussed, requires information to be 'about' an individual rather than information that 'relates to' an individual as in the EU.[222] Wi-Fi header data and a MAC address in particular are information about devices rather than information about individuals. However, such data is of course

219 The identified risks are broad and go beyond mere identification. For example, behavioural risks by being able to identify behaviours of individuals; surveillance risks through the constant monitoring of location data; autonomy risks by being able to identify sensitive facets of an individual's life; potential cyber and physical crime risks and function creep risks arising from unintended uses of personal information. Lindsay contends that the breadth of risk identification is appropriate regarding determinations of what is personal information under information privacy laws. See Lindsay, 'Misunderstanding "Personal Information"', above n 71, 13.

220 See, eg, *ITC Investigation* [2010] PrivCmrA 24 (24 December 2010): 'The Commissioner considered that individuals could not be identified from the information collected by the information technology company through its location-based services'.

221 See, eg, *Working Party Opinion*, above n 4, 7.

222 For the link between information 'about' and information that 'relates to' an individual, see Nouwt, above n 3, 385. Nonetheless, the 'relate to' definition is intended to have a wider application and consideration of privacy harms that arise.

information that relates to an individual.[223] In that sense, it is perhaps easier for the Article 29 Data Protection Working Party to address a wider scope of privacy risks because the definition of personal information in the *Data Protection Directive* affords a wider consideration of the issue.

However, that alone does not explain why the New Zealand Privacy Commissioner in the Google scandal was able to reach a similar conclusion as the Working Group when the definition of personal information in the *Privacy Act 1933* (NZ) is conceptually similar to that in the Australian legislation. It also does not explain why the OAIC's *Mobile App Guideline* now appears to recognise that a MAC address, as a UDID, could potentially be personal information whereas one interpretation of the *ITC Investigation* is that a MAC address is not personal information. The OAIC's *Mobile App Guideline* is based on a similar guideline produced by the Canadian Privacy Commissioner.[224] Like Australia and New Zealand, the Canadian privacy law's[225] definition of personal information stems from the *OECD Guidelines* and is information about an identifiable individual.[226] However, the Canadian Privacy Commissioner has been 'deliberately' active in expanding the construction of personal information.[227] It should not be a surprise therefore that the *Canadian Mobile Apps Guidelines* have a more considered application of when and how a device identifier can, in combination with location information, be considered personal information:

> Location information can reveal user activity patterns and habits. Whatever method is used to link a device to its owner, whether it's a unique device identifier or multiple linked identifiers, it has the potential to combine with personal information to create a profoundly detailed and sensitive profile of a user's behaviour depending on the circumstances.[228]

The OAIC's *Mobile App Guideline* provides a truncated version of this quote that copies the Canadian material about location information, but more importantly, removes the importance of contextual indications about how and when a device identifier can be personal information. The removal of this material is symptomatic of the key difference between the *Working Party Opinion* and the *ITC Investigation*. The former is founded on an identifiable reasoning process whereas the latter is not. It is the lack of reasoned guidance of the applicable

223 For example, Wi-Fi header data broadcast from residential addresses is information about a device but that information relates to an individual because it is inherently linked to an individual's residential address.

224 Office of the Privacy Commissioner of Canada, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* (2012) <http://www.priv.gc.ca/information/pub/gd_app_201210_e.asp#toc3.1> ('*Canadian Mobile Apps Guidelines*').

225 It should be noted that the Canadian federal information privacy law framework is different to that of Australia and New Zealand. There is a separate act for the federal public sector and the private sector. These are the *Privacy Act*, RSC 1985, c P-21 and the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ('*PIPEDA*'), respectively. The Canadian Privacy Commissioner is nonetheless responsible for administering both acts.

226 *PIPEDA* s 2 (definition of 'personal information').

227 Privacy Commissioner of Canada, 'Annual Report to Parliament 2001–2002' (Report, January 2003) 56, quoted in Schwartz and Solove, above n 65, 1876. See also Scassa above n 68, 196–8.

228 *Canadian Mobile Apps Guidelines*, above n 224, 3.

law by the Australian Privacy Commissioner that makes it difficult to determine whether Wi-Fi header data, and even a MAC address of a smart mobile device, constitute personal information in Australia.

Accordingly, regardless of whether Wi-Fi header data is personal information or not, a clear statement is required from the OAIC that provides an insight into the reasoning being applied in such determinations.[229] The need for this type of insight is more important now given that the OAIC has been tasked with developing guidelines on what constitutes reasonable identification under the *Privacy Act*'s new definition of personal information. The prospective guidelines will be integral to determining what constitutes personal information under the new definition and as such will provide guidance on a key threshold issue relating to the *Privacy Act*'s application.

It is therefore essential that the new guideline follow a similar approach to the Article 29 Data Protection Working Party. Doing so will provide the foundation for a more detailed and nuanced understanding of how information privacy law applies in Australia, which can then be measured against the legal and regulatory outcomes of other jurisdictions. This in turn will foster a more sophisticated privacy discourse that moves beyond the rigid confines of information privacy orthodoxy and provides a more suitable basis for the evaluation of perpetual technological developments and their effects on individual and societal notions of privacy in contemporary Australia. Professor Greenleaf decried in 2001 that 'we need more law'.[230] It is now time for that plea to be heard and to be actioned in the form of a reasoned regulatory discourse.

V CONCLUSION

Google clearly broke the laws of many countries when it collected payload data from Wi-Fi access points. The issue of whether Google breached the requirements of the *Privacy Act* in relation to the collection of Wi-Fi header data is more complex. This article put forward the view that Wi-Fi header data is classifiable as personal information under s 6(1) of the *Privacy Act*. Our analysis of the collection obligations under *NPP* 1 indicates that Google was potentially in breach of *NPP* 1.1 regarding the necessity of collection and Google was likely to

229 See Schwartz and Solove, above n 65, 1846:

> The line between [personally-identifiable information] and [non-personally-identifiable information] is not fixed but depends upon technology. Thus, today's [non-personally-identifiable information] might be tomorrow's [personally-identifiable information]. New and surprising discoveries are constantly being made about ways of combining data to reveal other data.

Consequently, the reasoning behind decisions about what is or is not personal information is more important than the decision itself. See also Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 *Computer Law & Security Review* 522, 526–7, regarding both the fundamental differences and the overlap between data protection and privacy rights. The distinction again re-emphasises the need for clarity of reasoning due to the paradoxical and unintended consequences of anonymised data application.

230 Greenleaf, 'Why Australian Privacy Law Does Not Exist', above n 218, 269.

have been in breach of *NPP* 1.2 and *NPP* 1.3 regarding unfair collection and the lack of notification provided respectively.

The preliminary investigations of the then Australian Privacy Commissioner apparently came to a different conclusion because she did not pursue the matter further. Media statements made at the time of the scandal did not make clear whether the then Commissioner concluded that Wi-Fi header data collected by Google was personal information. As a consequence, it is still unclear now what status Wi-Fi header data has under the *Privacy Act* and whether the collection of such data breaches the Act. The scant legal commentary — one reported investigation produced by the OAIC in 2010 and a tangentially relevant guideline — do nothing to clarify this issue. However, the issue demands clarification given the continued expansion of Location-Based Service industries and the fact that the EU has made a clear policy statement on this matter.

The absence of considered opinions on key constructs of the *Privacy Act* can only be addressed by legal decisions and regulatory guidelines that clearly highlight the reasoning processes adopted. Only then will it be possible to work out the substantive, practical and theoretical implications of the *Privacy Act*'s application to new technological challenges, such as those previously presented in the Google Street View Wi-Fi scandal and those to be presented by newly developing Location-Based Service industries.