Bond Law Review

Volume 25 | Issue 1 Article 3

2-25-2014

Facebook and face recognition: kinda cool, kinda creepy

Anna Bunn
Curtin University Law School, Anna.Bunn@cbs.curtin.edu.au

Facebook and face recognition: kinda cool, kinda creepy

Abstract
Facebook has recently been subject to scrutiny by privacy regulators in Europe, as well as by the US Federal Trade Commission, in relation to the introduction of its 'tag suggest' feature. This feature uses face recognition technology to create a biometric template of users' faces, and had been introduced to Facebook users as a default (opt-out) setting. One outcome of the recent scrutiny has been the temporary deactivation of the tag suggest feature. However, there is every indication that Facebook intends to re-introduce the feature in the not too distant future. This article canvasses some of the privacy implications of face recognition technology, particularly as it is used by Facebook, and in the private sector generally. Legal implications of Facebook's use of biometric templates and the generation and use of biometric information are considered by reference to the Privacy Act 1988 (Cth) as recently amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth). In particular, the threshold issue of the application of Australia's federal information privacy laws to overseas organisations that have no presence in Australia and do not have servers in the country is considered. Definitional issues around the fundamental terms 'collect' and 'receive', as used in the amended Privacy Act, are also discussed, along with an overview of possible compliance risks for Facebook arising from Australia's information privacy regime. Finally, the article offers some reflections on the efficacy of Australian information privacy laws in regulating the creation and use of biometric face templates and associated information in the social media context.

Keywords
Facebook, face recognition technology, biometric information, information privacy laws

FACEBOOK AND FACE RECOGNITION: KINDA COOL, KINDA CREEPY

ANNA BUNN*

ABSTRACT

Facebook has recently been subject to scrutiny by privacy regulators in Europe, as well as by the US Federal Trade Commission, in relation to the introduction of its 'tag suggest' feature. This feature uses face recognition technology to create a biometric template of users' faces, and had been introduced to Facebook users as a default (opt-out) setting. One outcome of the recent scrutiny has been the temporary deactivation of the tag suggest feature. However, there is every indication that Facebook intends to re-introduce the feature in the not too distant future. This article canvasses some of the privacy implications of face recognition technology, particularly as it is used by Facebook, and in the private sector generally. Legal implications of Facebook's use of biometric templates and the generation and use of biometric information are considered by reference to the Privacy Act 1988 (Cth) as recently amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth). In particular, the threshold issue of the application of Australia's federal information privacy laws to overseas organisations that have no presence in Australia and do not have servers in the country is considered. Definitional issues around the fundamental terms 'collect' and 'receive', as used in the amended Privacy Act, are also discussed, along with an overview of possible compliance risks for Facebook arising from Australia's information privacy regime. Finally, the article offers some reflections on the efficacy of Australian information privacy laws in regulating the creation and use of biometric face templates and associated information in the social media context.

The use of biometric information and face recognition technology is no longer the domain of government security agencies and science fiction films. One expert has conservatively estimated that 54% of the US population already has a biometric template of their facial features (or a 'face print') stored, not in an FBI computer database but on a Facebook server.[1] Face recognition technology has traditionally

* Lecturer, Curtin Law School, Curtin University. This article, as well as its title, was inspired by a piece by Nick Schifrin, for *Nightline*, ABC News (US), broadcast 10 June 2011.

1 Jennifer Lynch, Submission to Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, *What Facial Recognition Technology Means for Privacy and Civil Liberties*, 18 July 2012, 2. While Facebook has temporarily disabled its face recognition tool in the US, this does not necessarily mean that Facebook has deleted templates it already holds in its database: this is discussed further below.

been used by governments and organisations to verify identities for the purpose of security [2] and law enforcement. [3] More recently, however, applications of the technology target its use by individuals for their own purposes, whether that is the easy identification of friends in photographs uploaded on social media sites or to access personal information about people from their photograph.[4]

While there are no doubt many positive uses of facial recognition technology, at both an individual and a societal level,[5] the technology also poses a number of risks and may be intrusive of an individual's privacy.[6] In 2008 the Australian Law Reform Commission (ALRC) released a comprehensive report into Australian Privacy Law and Practice.[7] One section of the report deals specifically with biometric technology and notes some of the concerns around its use. Broadly, these concerns relate to the fact that the widespread use of biometric systems allows for mass surveillance of individuals; that technology such as facial recognition may allow people to be

---

2 Such as systems used to control access to physical spaces and computer systems, as well as those used at airports: see generally Thomas Huang, Ziyou Xiong and Zhenqiu Zhang, 'Face Recognition Applications' in Stan Z. Li and Anil K. Jain (eds), *Handbook of Face Recognition (*Springer, 2nd ed, 2011) 617 and the use of biometrics in passports: Jens-Martin Loebel, 'Is Privacy Dead? - GPS-Based Geolocation and Facial Recognition Systems' in, Hercheui, M.D. et al. (Eds.): *ICT Critical Infrastructures and Society: 10th IFIP TC 9 International Conference on Human Choice and Computers*, International Federation for Information Processing (Springer-Verlag 2012) 338, 342.

3 Applications of facial recognition technology for law enforcement include suspect identification and the exclusion of specific individuals from venues, such as casinos: see generally Huang, Xiong, and Zhang, above n 2, 617.

4 See, eg, Emma Woollacott, *Google Snaps Up Facial Recognition Firm* (25 July 2011) TG Daily <http://www.tgdaily.com/business-and-law-features/57446-google-snaps-up-facial-recognition-firm>.

5 One application of facial recognition technology is in the verification of individual identities, or identity management. A former Australian Federal Privacy Commissioner noted that this can assist in fraud prevention, the enhancing of national security and even improved targeting of goods and services to customers, particularly in an electronic environment: see Malcolm Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at the Australia IT Security Forum, 30 March 2004).

6 See, eg, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 1, 409 [9.72] ('*ALRC Report*') quoting the Council of Europe which cautions that before the introduction of a biometric system: '[t]he controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider other alternatives that are less intrusive for private life' (reference omitted).

7 Ibid.

identified without their knowledge or consent; and that the use of this technology could reveal sensitive information about an individual, such as information about the individual's health or religious beliefs.[8] Concerns were also expressed around the security of information gathered by biometric systems and the dangers that would be presented should that information fall into the wrong hands. The ALRC also noted that concerns have been raised regarding the accuracy of biometric technology, and that where such technology is inherent in identification systems individuals may be misidentified (or not identified at all when they should be).[9]

Since the mid-1990s the number of face recognition systems and the commercial exploitation of those systems has grown exponentially. Some have attributed this growth to the emergence of new applications and the growing sophistication and increased affordability of the technology.[10] One current application of face recognition technology is in enabling social network users to quickly attach a name, or 'tag', to photographs of individuals uploaded onto a social media website. This technology is in use by Facebook in the form of its 'tag suggest' feature and has attracted significant attention from the public, the media, and governments, particularly in Europe and the US.

In 2011 and 2012 the Irish Data Protection Commissioner (DPC) conducted audits of Facebook that focussed, inter alia, on the use by the organisation of face recognition technology.[11] Facebook has also been subject to investigation by German and Norwegian data protection authorities for the use of its face recognition technology.[12] One outcome arising from this scrutiny has been Facebook's agreement to disable the tag suggest feature for European users, at least temporarily.[13] Although this decision hit headlines, the subsequent disabling of the tag suggest feature in the US (and, it would seem, globally) happened much more quietly, with Facebook being reported as saying that its decision to turn off the tag suggest tool was to allow for

8 Ibid, vol 1, 408-409 [9.71].

9 Ibid.

10 Huang, Xiong, and Zhang, above n 2, 617.

11 Data Protection Commissioner (Ireland), *Facebook Ireland Ltd: Report of Audit*, 21 December 2011; Data Protection Commissioner (Ireland), *Facebook Ireland Ltd: Report of Re-Audit*, 21 September 2012.

12 'Germany Re-opens Facebook Facial Recognition Probe' *BBC Technology News* (online), 15 August 2012, <http://www.bbc.co.uk/news/technology-19274341>; Stephanie Bodonie, 'Facebook Faces Norway Probe Over Facial-Recognition Tags', *Bloomberg Business Week* (online), 2 August 2012 <http://www.businessweek.com/news/2012-08-02/facebook-faces-norway-probe-over-facial-recognition-photo-tags>.

13 'Germany Re-opens Facebook Facial Recognition Probe', above n 12.

improvements in its efficiency.[14] At the time of writing the tag suggest feature is still not available for users of Facebook, including for those in Australia, where the feature had previously been enabled as a default setting (opt-out not opt-in) on user accounts. Despite the fact that the tag suggest feature is still unavailable, there is every indication that it will be reinstated. Facebook's user settings still refer to tag suggest (albeit showing that the tool is not yet available) and the Facebook Data Use Policy (amended as recently as December 2012) makes reference to the fact that Facebook is able to suggest tags by scanning and comparing photographs uploaded by friends to information gathered from other photographs in which an individual has been tagged.[15] Given this, and the fact that Facebook has only recently acquired Face.com, a large face recognition technology firm, for a price in the tens of millions of dollars,[16] it seems likely that the tag suggest feature will be re-launched in the near future.

This article considers the efficacy of Australia's recently amended information privacy laws in dealing with privacy risks posed by facial recognition technology, particularly in the context of the use of that technology by private sector organisations. Given the fact that Facebook holds such a large repository of images[17] and probably operates (or has the ability to operate) one of the most well-developed face recognition systems of all private sector entities,[18] the social-media giant is the focus of this discussion. However, many of the issues canvassed arise from technological advancements and social media trends more generally, and the legal position discussed has broader application for organisations outside of Australia. This article considers some of the threshold and definitional issues which determine whether the recently amended Australian information privacy laws are capable of

---

14 Somini Sengupta and Kevin J O'Brien, 'Facebook can ID Faces, But Using Them Grows Tricky', *NYTimes* (online), 21 September 2012 <http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html?_r=0>.

15 Facebook, *Data Use Policy* (11 December 2012) <http://www.facebook.com/full_data_use_policy>; Facebook, *Statement of Rights and Responsibilities* (11 December 2012) <http://www.facebook.com/legal/terms>.

16 Alexia Tsotsis, 'Facebook Scoops Up Face.com for $55-60 to Bolster Its Facial Recognition Tech (Updated)', *TechCrunch* (online), 18 June 2012 <http://techcrunch.com/ 2012/06/18/facebook-scoops-up-face-com-for-100m-to-bolster-its-facial-recognition-tech/>.

17 See, eg, Electronic Privacy Information Centre (EPIC) noting 'Facebook is the largest photo-sharing site in the world by a wide margin': EPIC, *In re Facebook and the Facial Identification of Users*, Complaint to Federal Trade Commission (US), 10 June 2011, 8 [36]. See also Lynch, above n 1, 10: 'Facebook has amassed possibly the largest database of face prints in the world.'

18 Lynch, above n 1, 9-10.

applying to organisations, such as Facebook, which do not have a physical presence in Australia.[19] This involves consideration of the extra-territorial application of the *Privacy Act 1988* (Cth) (*'Privacy Act'*) in its amended form,[20] and consideration of whether photographs, associated information and biometric templates constitute personal information and sensitive information for the purposes of the Act. There then follows an overview of some of the possible areas of non-compliance with the amended *Privacy Act* in relation to Facebook's use of face recognition technology and a discussion as to the efficacy of Australian information privacy laws in regulating the creation and use of face templates and associated information.

I FACEBOOK AND FACIAL RECOGNITION TECHNOLOGY

The fact that Facebook has the ability to use face recognition technology may not be immediately apparent, even to Facebook users, as there is no mention of the words 'face recognition', or similar terms, in any of the Facebook terms of use, nor in its Privacy Policy.[21] However, a Facebook information page describes how face recognition technology enables the 'tag suggest' feature, first introduced in 2011.[22] Facebook describes that feature as follows:

> We currently use facial recognition software that uses an algorithm to calculate a unique number ("template") based on someone's facial features, like the distance between the eyes, nose and ears. This template is based on photos you've been tagged in on Facebook. We use this template to suggest tags to you when you're adding a new photo to Facebook … Thus, when a new photograph of an individual in the 'face print' database is uploaded to

---

19 Although Facebook has a registered company (Facebook Pty Ltd) in Australia, the Australian company has been established to deal directly with advertisers. To the extent that the Australian company deals with personal information, it would be subject to the *Privacy Act 1988* (Cth) (*'Privacy Act'*) similar to any other Australian organisation. However, this article deals with the personal information collected, received, created, held and used about individuals in Australia through the Facebook website. The Facebook statement of rights and responsibilities, which forms part of the contract between Facebook and registered users who are outside the US, is made with Facebook Ireland Ltd. Facebook has also insisted that Irish law applies to its entire European operation: Anupam Chander, 'Facebookistan' (2012) 90 *North Carolina Law Review* 1807, 1835.

20 *Privacy Act* s 5B and *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 4 *('Privacy Amendment Act')*.

21 Facebook, *Data Use Policy*, above n 15.

22 EPIC, above n 17, 10 [49].

> Facebook, the facial recognition software is able to automatically suggest the name of the person in the new photograph.[23]

In its information page on tagging, Facebook informs users that if, for any reason, the user does not want automatic tag suggestions of their name to be made when photographs of them are uploaded to Facebook, the user is able to disable the automatic tagging feature in their privacy settings. According to Facebook, individual biometric templates that enable the tag suggestions feature, often colloquially referred to as 'face prints',[24] are deleted when that user disables the automatic tagging feature.[25]

However, certain aspects of the way in which Facebook uses the technology behind this feature remain unclear. In a report to the US Senate in 2012, an attorney with the Electronic Frontier Foundation noted that Facebook refuses to reveal the number of actual photographs it holds in its database and whether or not it creates a face print for non-Facebook users.[26] Certainly Facebook users are able to manually tag *anyone* who appears in a photograph uploaded to Facebook, whether the person is a Facebook user or not.[27] In addition, even if a Facebook user has disabled the tag suggest feature for photographs of themselves (or if the feature is not available), other users are still able to manually tag the user in photographs. Those tags will exist unless and until such time as the user deletes the tag.[28] Despite the fact that Facebook confirms that it deletes the face print for a user who has disabled tag suggestions, this does not mean that the template will not be or cannot be recreated as a result of others manually tagging photographs of the user thereafter. Facebook informs users that whenever they are tagged in a photograph, that tag will be associated with the user's account and compared with all other tags associated with the user's account to create, what Facebook terms, a 'summary of this comparison'.[29] It is this summary information that is used to generate a 'template'. Importantly, Facebook does *not* represent to users that summary information will not be collected

---

23 Facebook, *Tagging Photos* <http://www.facebook.com/help/463455293673370/>.

24 See generally Lynch, above n 1.

25 Facebook, *Tagging Photos*, above n 23. This is also confirmed by the Irish Data Commissioner Office's 2012 audit review of Facebook: Data Protection Commissioner (Ireland), *Facebook Ireland Ltd: Report of Re-Audit*, 21 September 2012, 54 [2.8].

26 Lynch, above n 1. Information provided by Facebook itself would seem to suggest that a face-print is not actually created in respect of those who are not users of Facebook. Although, information from which a template is able to be created is probably retained: see Facebook, *Tagging Photos*, above n 23 and EPIC, above n 17, 25 [109].

27 Facebook, *Tagging Photos*, above n 23.

28 Ibid.

29 Ibid.

when a user is manually tagged in a photograph: in fact, to the contrary, Facebook informs users that, to avoid this summary information being held by Facebook, it would be necessary for a user either to never have been tagged or to have untagged themselves in every photograph that exists on the site.[30]

II PRIVACY IMPLICATIONS OF FACIAL RECOGNITION TECHNOLOGY

One consequence of recent advances in face recognition technology was illustrated in an experiment carried out by researchers from Carnegie-Mellon University.[31] The research proved, conceptually at least, that a combination of publicly available Web 2.0 data (such as photographs posted to Facebook), cloud computing, data mining, and face recognition software is 'bringing us closer to a world where anyone may run face recognition on anyone else, online and offline - and then infer additional, sensitive data about the target subject, starting merely from one anonymous piece of information about her: the face.'[32] In the social media context, the combination of face recognition technology capabilities with information posted by social media users themselves - such as the identification of friends (through the practice of naming or 'tagging' people in photographs) and the provision of geolocation data (whereby users allow their GPS coordinates at given times to be posted to their social media sites[33]) - allows what one researcher has described as 'unprecedented tracking' of social media users and as something that poses a 'very real threat of abuse.'[34] The Organisation for Economic Co-operation and Development (OECD) also recognises the danger that biometric systems in general increase the ease by which large-scale surveillance can be undertaken.[35]

---

30 Ibid.

31 Alessandro Acquisti, Ralph Gross and Fred Stutzman, *Faces of Facebook: Privacy in the Age of Augmented Reality*, 4 August 2011, <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ>.

32 Ibid.

33 For a description of how this works in relation to Facebook see Jacqui Cheng, 'Facebook Adds Geolocation, Check-ins to iPhone and Web apps', *arstechnica* (online), 19 August 2010 <http://arstechnica.com/business/2010/08/facebook-adds-geolocation-to-iphone-web-apps/>.

34 Jens-Martin Loebel, above n 2, 62-63.

35 Organisation for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Technology, *Biometric Based Technologies* (2004), 12.

Specific concerns relating to the use of face recognition technology by Facebook have been raised by a number of public interest groups. For example, a complaint submitted to the US Trade Commission by the Electronic Privacy Information Center (EPIC), a US not-for-profit privacy research centre, notes that Facebook's size and reach is 'unparalleled' among social networking services.[36] According to EPIC, Facebook is not only the world's largest social networking site but holds the largest collection of photographs of any corporation in the world by a considerable margin.[37] The size of the collection of images on Facebook, and the fact that many of these can be linked to individuals, is significant given that, as EPIC notes in its complaint, government has an interest in accessing information held on social networking sites and law enforcement agencies have previously used information stored by Facebook in the pursuit of their investigations.[38] The Australian government readily acknowledges the importance it attaches to having the ability to access data and the content of certain communications in the interests of national security and crime prevention.[39] Currently Australian law allows a broad range of enforcement agencies to intercept or obtain information communicated through or stored by telecommunication providers and Internet Service Providers (ISPs).[40] However, proposals recently advanced by the Australian government, and the subject of a government inquiry,[41] seek to extend this regime to a broader range of communication providers, including the operators of social media sites.[42] While consideration of the proposed reforms to national security laws is beyond the scope of this article, it is worth noting that the extent to which the reforms could allow relevant authorities to access templates, or 'face prints', held by social network

---

36 EPIC, above n 17, 8.

37 Ibid [36]. See also Lynch, above n 1, 10.

38 EPIC, above n 17, 19 [78]. See also *LaLonde v LaLonde* (Ky Ct App, No 2009-CA-002276-MR) discussed here: <http://blog.internetcases.com/2011/03/12/facebook-privacy-photo-tagging-attorney-chicago-lawyer-social-media/> in which a woman sought to appeal an order awarding custody of her daughter to the child's father on the basis that, among other things, the court 'improperly considered Facebook photos showing her drinking.' The photographs were harmful to the woman's custody claim because her psychologist had testified that the medication prescribed for her bipolar disorder would be adversely affected by the alcohol. See also Lynch, above n 1, 11, especially nn 60-62.

39 'Equipping Australia against Emerging and Evolving Threats' (Discussion Paper, Commonwealth Attorney-General, July 2012) 28.

40 Ibid 27; Nigel Brew, 'Telecommunications Data Retention – an Overview' (Background Note, Parliamentary Library, Parliament of Australia, 24 October 2012) 7.

41 House of Representatives Joint Parliamentary Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of National Security Legislation* (2012).

42 'Equipping Australia against Emerging and Evolving Threats', above n 39, 27.

providers such as Facebook is, as yet, undetermined.[43] In this context it is also worth noting that Australia's federal information laws allow organisations and agencies to disclose personal information where, inter alia, they believe that the information is necessary to prevent or detect a criminal offence or certain other breaches of law.[44]

Another tangible risk arising from the use of face recognition technology to create 'face prints' relates to the security and integrity of the biometric templates themselves. As one expert has noted in a submission to a US Senate Committee, the fact that face prints are not stored as images, but rather as algorithms, gives rise to the possibility that the algorithms could be changed within a particular database, or that the information may be leaked or stolen from the system.[45] This would, in turn, have potentially serious consequences for misidentification, impersonation or identity theft.[46] The accuracy of face recognition systems employed on a large-scale is also questionable.[47] Although, given the size of its database, Facebook's system has been described as more robust than most.[48] There are also risks that the vast amount of data that can be generated by coupling face recognition with other technologies, such as geolocation (described above), may be misused. In its complaint to the US Federal Trade Commissions, EPIC averred that Facebook had failed to establish that applications developers, the government and other third parties would not be able to access the template information generated by Facebook.[49] In relation to the issue of Facebook's sharing of user data with applications, the Irish DPC's office reported that it did not consider that Facebook's 'reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data.'[50] Moreover, while the Irish DPC did not regard the information security practices of Facebook in general as unsatisfactory or problematic, a number of concerns were raised by that office around the protection of user data from employee abuse.[51] There

43 Office of the Australian Information Commissioner (OAIC), Submission No 183 to House of Representatives Joint Parliamentary Committee on Intelligence and Security, above n 41, 15 [44], [45] and see especially n 35.

44 *Privacy Act* sch 3, National Privacy Principle (NPP) 2.1; *Privacy Amendment Act* sch 1, Australian Privacy Principle (APP) 6.2.

45 Lynch above n 1. See also OECD, above n 35, 13-15.

46 Lynch above n 1 and OECD, above n 35, 13-15.

47 Huang, Xiong, and Zhang, above n 2, 635.

48 Lynch, above n 1, 9.

49 EPIC, above n 17, 17 [71].

50 Data Protection Commissioner (Ireland), above n 25, 8.

51 Ibid 9.

have also been a number of reported incidents of security breaches in relation to Facebook itself,[52] as well as other organisations holding large amounts of user data.[53]

Aside from the various concerns discussed above, it has been noted that face recognition technology itself is becoming increasingly sophisticated.[54] Various new integrations of that technology into people's daily lives may be realised in the not too distant future.[55] One possible new application of the technology is in targeted marketing. For example, a US advertising agency has recently announced that it is finalising testing of technology that uses face recognition to automatically identify people captured on cameras installed in shops.[56] Those individuals are then notified, via their smartphones, of customised deals in their location. Identification using face recognition technology is made possible by individuals authorising the marketing application to compare their image with photographs in which they have recently been tagged on Facebook; and the deals are customised by the application scanning information from the individual's Facebook account.[57] The risk of data being used in ways as yet unimagined is also compounded when data is retained for a long period of time. Today it may be the case that the sophistication of face recognition technology is not accurately able to link a photograph of an adult with biometric information extracted from photos of the same person as a child, but over a period of

---

52 See, eg, Hayley Tsukayama 'Facebook Security Breach Raises Concerns', *The Washington Post* (online), 16 November 2011 <http://www.washingtonpost.com/business/economy/facebook-hack-raises-security-concerns/2011/11/15/gIQAqCyYPN_story.html>; Paul Lilly, *Facebook Confirms Data Breach and Massive Vulnerability* (11 October 2012) Hot Hardware <http://hothardware.com/News/Facebook-Confirms-Massive-Data-Breach-and-Vulnerability/>.

53 See, eg, Angela Moscaritolo, 'Skype Reveals Security Breach; Facebook Launches Job App; Nexus 4 Sells Out', *PC Mag* (online), 15 November 2012 <http://www.pcmag.com/article2/0,2817,2412148,00.asp>; Benn Grubb, 'Hackers Steal Customer Data to Prove Risk of Retention Proposal', *The Sydney Morning Herald* (online), 27 July 2012 <http://www.smh.com.au/it-pro/security-it/hackers-steal-customer-data-to-prove-risk-of-retention-proposal-20120726-22v67.html>; 'AAPT Confirms Hackers Stole Customer Data', *ABC News* (online), 27 July 2012 <http://www.abc.net.au/news/2012-07-26/aapt-confirms-hackers-stole-customer-data/4157946>.

54 Lynch, above n 1, 14.

55 See Huang, Xiong, and Zhang, above n 2, 636.

56 Michael Walsh, 'Facedeals: Facial Recognition Marketing Stirs Privacy Discussion Along With Excitement', *Daily News* (online), 15 August 2012 <http://www.nydailynews.com/news/national/facedeals-facial-recognition-marketing-stirs-privacy-discussion-excitement-article-1.1137240>.

57 RedPepper, *Facedeals*, <http://redpepperland.com/lab/details/check-in-with-your-face>.

time, and in parallel with improvements in technology, far more accurate comparisons across large age discrepancies may become possible.[58]

Given that photographs on Facebook will remain on Facebook indefinitely, at least until a user deletes photographs which they have uploaded, the risk that such photographs may be subject to increasingly sophisticated face recognition techniques is very real. In addition, given that Facebook enshrines within its Data Use Policy the right to change that policy from time to time (and does indeed make frequent changes to that policy, none of which require a user's specific consent)[59] there is the ever-present risk that photographs and face prints could be used in the future in ways not currently envisaged. The likelihood of this risk eventuating is not negligible when one considers that Facebook's pictures may be its 'most vital assets' [60] and that increasing pressure is likely to be brought to bear on the organisation, by its investors, to monetize the information it holds.[61] Indeed there may be inherent risks involved whenever a private company with access to face recognition technology, or the rich data source which such technology is able to provide, also has business interests in marketing and profiling.[62] This risk is one that is recognised by the Office of the Australian Information Commissioner (OAIC). Noting that the outlay incurred by media platforms in providing services at no cost to users will, in many cases, be recovered through advertising, the OAIC observes that:

> [t]here is an inherent tension between this business model and the requirement to give individuals the ability to control, to the greatest extent possible, what happens to their personal information ... This tension will continue to challenge the traditional concepts of the regulation of the handling of personal information into the future.[63]

Given the various ways in which the use of face recognition technology can implicate privacy, this article now turns to consider the extent to which Australian federal information privacy laws may be used to regulate the collection, creation and use of biometric information and biometric templates in the form of 'face prints'.

---

58 Lynch, above n 1, 14.

59 Facebook, *Data Use Policy* above n 15.

60 Sengupta and O'Brien, above n 14.

61 Anna Johnston and Stephen Wilson, 'Privacy Compliance Risks for Facebook' (2012) *IEEE Technology and Society Magazine* 59, 63.

62 Jens-Martin Loebel, above n 2, 343.

63 Office of the Australian Information Commissioner, *Annual Report 2011-2012* (2012), xiv.

III LEGAL POSITION

According to EPIC, the US Supreme Court has made it clear that 'both the common law and literal understanding of privacy encompass the individual's control of information concerning his or her person.'[64] In Australia, however, an individual's control of information concerning his or her person is more limited: there is no constitutional or common law right to privacy as such,[65] and generally the extent of privacy protection at common law is essentially confined to actions for breach of confidence and a limited range of torts, such as defamation and trespass, dealing with particular aspects of privacy.[66] Information privacy in Australia is dealt with through a range of state-based and federal legislation. The *Privacy Act* regulates the handling of personal information by federal government agencies[67] and certain private sector organisations.[68] Amendments to the *Privacy Act* have recently been passed in the form of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) ('*Privacy Amendment Act*'), although most of the amendments will not commence until March 2014.[69]

Private sector organisations bound by the *Privacy Act* are required to comply with certain baseline privacy standards, such as those set out in the National Privacy Principles enshrined within the Act itself,[70] or in a binding privacy code which has been approved by the OAIC.[71] When amendments contained within the *Privacy Amendment Act* take effect, the National Privacy Principles (NPPs) will be replaced by a set of Australian Privacy Principles (APPs). These APPs will bind both relevant private sector organisations and government agencies alike, such bodies being referred to in the legislation as 'APP entities'.[72] The remainder of this article will focus

---

64 EPIC, above n 17, 4 [14] quoting *US Department of Justice v Reporters Comm for Freedom of the Press*, 489 US 749, 463 (1989).

65 Although the ACT and Victoria have enacted legislation guaranteeing a right to privacy: see *Human Rights Act 2004* (ACT) s 12; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.

66 For more detailed consideration of Australian laws that protect aspects of personal privacy see, eg, *ALRC Report*, above n 7, vol 3, 2550-2552 and New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper No 1 (2007) 35-58.

67 As defined in the *Privacy Act* s 6 but note that certain public sector agencies are completely exempt from the *Privacy Act*: at s 7.

68 Ibid s 6C (definition of 'organisation').

69 *Privacy Amendment Act* s 2.

70 *Privacy Act* s 16A. The NPPs are set out at sch 3.

71 Ibid s 16A.

72 *Privacy Amendment Act* s 15. The APPs themselves are set out at sch 1. The APPs will bind all 'APP entities' defined as 'an agency or organisation': at sch 1(6).

on the possible application of the amended *Privacy Act* and the new APPs to Facebook, particularly in relation to that organisation's use of face recognition technology.

A Does the Amended Privacy Act Apply to Facebook?

A number of commentators have specifically discussed the application of the *Privacy Act* to personal information held by Facebook.[73] A former Australian Privacy Commissioner has indicated that Facebook's practices may not comply with the privacy principles under the *Privacy Act*.[74] Before recent amendments to the *Privacy Act* were introduced, however, it was at best unclear whether the Act was intended to apply to the acts and practices of organisations such as Facebook (that is, to organisations which are incorporated outside of Australia, do not have a physical presence in Australia, and whose servers are all located outside of Australia[75]). This is because the extra-territorial provisions of the Act provide that the legislation will only apply to the acts or practices of an organisation not incorporated in Australia (and not otherwise described in the section) if it fulfils two specified conditions: first, that the organisation carries on business in Australia; and secondly, that the organisation collects or holds information *in* Australia.[76] The OAIC has submitted that the meaning of 'in Australia' is unclear, particularly in the online context.[77]

---

73 See, eg, Johnston and Wilson, above n 61; Veronica Scott and Kate Ballis, *Facebook, Photos, Journalists, and Privacy – Some Legal Issues Arising From the Ben Grubb Affair* (24 May 2011) Intellect <http://tmtblog.minterellison.com/2011/05/facebook-photos-journalists-and-privacy.html>.

74 Asher Moses, 'Privacy Watchdog Puts Bite on Facebook', *The Sydney Morning Herald* (online), 23 July 2009 <http://www.smh.com.au/technology/biz-tech/privacy-watchdog-puts-bite-on-facebook-20090723-du79.html>. This is not to say that the former Privacy Commissioner, quoted in the article, suggested that Facebook was in breach of Australian information privacy law and was actually bound by the Act.

75 Facebook servers are located in the US and Sweden: Rob Waugh, 'That's Really Cool: Facebook Puts Your Photos Into the Deep Freeze as it Unveils Massive New Five Acre Data Centre Near Artic Circle', *Mail Online* (online), 28 October 2011 <http://www.dailymail.co.uk/sciencetech/article-2054168/Facebook-unveils-massive-data-center-Lulea-Sweden.html>; Rich Miller, *The Facebook Data Center FAQ* (27 September 2010) Data Center Knowledge <http://www.datacenterknowledge.com/the-facebook-data-center-faq>.

76 Privacy Act s 5B.

77 Office of Australian Information Commissioner, Submission No 14 to House of Representatives Standing Committee on Social Policy and Legal Affairs, *Inquiry into Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, 24 July 2012, 15.

The *Privacy Amendment Act* makes some changes to the wording of the extra-territorial provisions of the *Privacy Act*.[78] Those changes do not, however, alter the wording of the two conditions described above, which must still be met before an organisation that is not incorporated in Australia will be considered to have an Australian link and be bound by the legislation in respect of acts and practices engaged in outside of Australia. Nevertheless, the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) ('Explanatory Memorandum') does seek to clarify that the requirement that information be collected in Australia 'includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity'[79] and will also include information collected via a website hosted outside Australia and owned by a foreign company that is based outside of Australia and not incorporated within Australia.[80] The Explanatory Memorandum also clarifies that those entities which 'have an online presence (but no physical presence in Australia), and collect personal information from people who are physically in Australia, 'carry on a business in Australia or an external Territory'.[81]

Despite the clarification of the extra-territorial provisions offered in the Explanatory Memorandum the OAIC has suggested that the intended meaning of the requirement that information must be collected 'in Australia' should be made explicit by amending 'in Australia' to 'from Australia'.[82] This recommendation has not been incorporated into the wording of the legislation, which is unfortunate given the importance of those provisions in clarifying the entities subject to the *Privacy Act* and in respect of which the OAIC is able to take enforcement action.[83]

Even so, the way in which the words 'in Australia', as used in the Australian link provisions of the amended *Privacy Act*, are to be interpreted is not the only ambiguity related to those provisions. Given that Facebook's servers are all outside of Australia,[84] it is clear that personal information is not held in Australia. What is less clear is whether Facebook can be said to *collect* information in Australia (or from

78 *Privacy Amendment Act* sch 4.

79 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 218.

80 Ibid.

81 Ibid.

82 Office of the Australian Information Commissioner, Submission No 47 to Senate Standing Committee on Legal and Constitutional Affairs, *Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) 23 July 2012, 17.

83 Office of Australian Information Commissioner, above n 77, 15.

84 Rob Waugh, above n 75; Rich Miller, above n 75.

people in Australia) within the meaning of the provisions. This is fundamental because the Facebook model necessitates the gathering, processing, holding, and storage of vast amounts of information, much of which may not have been requested by Facebook, but which has certainly been received by Facebook (via its users or applications developers and other third parties).[85] Facebook also aggregates existing information and creates new information: for example, the summary information from which biometric templates are collated involves the aggregation and comparison of photographs in which individuals have been tagged.[86] Biometric templates (or face prints) themselves are information created by the organisation from other information in its possession. Whether all of these activities fall within the meaning of 'collect' in the Australian link provisions depends on how broadly the term is interpreted: does it include, for example, the gathering of information other than at the request of the organisation involved, and will it include information that is created or internally generated by the organisation and then included in a record or generally available publication?

The word 'collect' is not currently defined in the *Privacy Act* but the *Privacy Amendment Act* inserts a definition of 'collects' into the *Privacy Act* to provide that 'an entity collects personal information only if the entity collects information for inclusion in a record or generally available publication.'[87] This definition limits the scope of 'collect', but the repetition of the verb also implies that it is not to be treated as synonymous with the inclusion of personal information in a record or generally available publication.[88] This is probably due to the fact that the APPS (as with the current NPPs) are intended to apply both to the *process* of collecting information (for example, the requirement in APP 3 that information must be collected by lawful and fair means)[89] as well as to the information itself once it has been retained.[90] However, the lack of any definition of 'collect' is problematic because it leaves open the question as to whether all personal information included in a record or generally available publication, howsoever an entity has come by that information, has been 'collected' for the purpose of the Australian link provisions.

---

85 Facebook, *Data Use Policy*, above n 15.

86 Facebook, *Tagging Photos*, above n 23 [What information does Facebook use to tell that a photo looks like me and to suggest that friends tag me].

87 *Privacy Amendment Act* sch 1 item 10.

88 The *Privacy Act* distinguishes between the collection of personal information and information that has been collected, and this distinction is necessary because the NPPs relate both to the process of collection as well as the retention of information once collected: at s 16B and sch 3.

89 *Privacy Amendment Act* sch 1 [APP 3].

90 Ibid sch 1 [APP 5]-[APP 13].

B Should 'Collect', as Used in the Australian Link Provisions, Have a Broad or Narrow Interpretation?

There are a number of arguments supporting the proposition that the word 'collect', as used in the Australian link provisions of the *Privacy Amendment Act*, should be given a broad interpretation. That is, a broad interpretation of 'collect' would be the obtaining or creation of information – by whatever means, including internal generation - of personal information, which information is then included in a record or generally available publication, and the retention of personal information in a record or generally available publication.

Part 2 of the APPs, encompassing APPs 3-6, is headed 'Collection of Personal Information'. APP 3 relates to the collection of solicited personal information and applies to information that is both collected *and* solicited.[91] The implication being that 'collect' is the broader term. A number of the other APPs,[92] as well as the body of the Act,[93] refer to the collection of information but are not expressed to be limited to collection by solicitation. It seems clear, therefore, that the word 'collect' as used in the *Privacy Amendment Act*, including its use in the Australian link provisions, is not intended to be limited to solicitation of information. What is less clear is the question of whether an organisation can properly be regarded as collecting information where the information is not obtained from outside of the organisation, but is internally generated.

In favour of an interpretation of 'collect' that would include the internal generation of information is the fact that the dictionary meaning of the verb collect includes bringing together, assembling or accumulating.[94] There is no reference in this definition to the object of the action and, thus, no suggestion as to how that object has

---

91 Ibid sch 1 [APP 3]. This wording seeks to clarify an ambiguity over the interpretation of the word 'collect' in the National Privacy Principles, namely whether the word 'collect' refers only to collection by solicitation or whether it refers to information received by an entity, regardless of whether or not that information had been requested: Graham Greenleaf, 'Private Sector Privacy: Problems of Interpretation' (Paper presented at The New Australian Privacy Landscape Seminar, University of New South Wales Faculty of Law, 14 March 2001) 3; cf Patrick Gunning, 'Central Features of Australia's Private Sector Privacy Law' (2001) 7 *Privacy Law and Policy Reporter* 189, 193-195. Questions around interpretation of the word 'collect' have mostly arisen in connection with the use of the word in the NPPs of the *Privacy Act*. Similar debates have also taken place around the word collect as used in the information privacy legislation of other jurisdictions.

92 *Privacy Amendment Act* sch 1 [APP 5] – [APP 6].

93 Ibid sch 1 item 16B.

94 Oxford University Press, The Australian Concise Oxford Dictionary (3rd ed, 1997).

come into existence. What dictionary definitions of the word 'collect' *do* suggest, according to the New Zealand Law Commission, is that 'collection involves making some effort to acquire something, and especially that to collect something is to acquire it or bring specimens of it together systematically or purposefully.'[95]

Thus the natural and ordinary meaning of collect may be said to focus not on the object of the collection so much as the mental element of the collector: this interpretation is one which is supported by the definition of 'collect' as used in the recent amending legislation. It will be recalled that the *Privacy Amendment Act* provides that an entity collects personal information 'only if the entity collects information for inclusion in a record or generally available publication.'[96] As has been noted by Graham Greenleaf, the decision to retain personal information, even information which has not been requested, is what distinguishes the collection of information from mere receipt.[97]

Therefore it is submitted that the key issue in deciding whether information has been collected within the meaning of the Australian link provisions (as well as the current organisational link provisions) will not be how the information was obtained, or whether it was internally generated or received from outside of the organisation in question, but whether or not the information was intended for inclusion or was included in a record or generally available publication.[98]

It has been argued above that the use of the word 'collect' in the Australian link provisions to be inserted into the *Privacy Act* is capable of applying to the obtaining of personal information in Australia or (as per the clarification offered in the Explanatory Memorandum) *from* Australia, as well as to the creation of personal information *about* a person in Australia. However, this is not entirely beyond doubt: indeed, a consideration of the meaning of 'collect' within the context of information

95 New Zealand Law Commission, *Review of the Privacy Act 1993*, Issues Paper No 17, 79.

96 *Privacy Amendment Act* sch 1 item 10.

97 Graham Greenleaf, above n 91, 3.

98 Against the above arguments is the fact that the Explanatory Memorandum explains that the words 'in Australia' as used in the Australian link provisions include collection '*from* an individual within Australia': Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 218 [emphasis added]. The use of the words 'from an individual' rather than, say, 'about an individual' would seem to imply active collection, rather than the mere receipt or creation of information about a person in Australia. That said, the Explanatory Memorandum does not specifically exclude collection about an individual from the meaning of 'collect'.

privacy has also been undertaken in a number of other jurisdictions.[99] It is unfortunate, then, that the *Privacy Act* amending legislation does not more specifically define the term 'collect'.[100] One effect of this ambiguity is that the OAIC may be reluctant to take enforcement action against overseas organisations in respect of personal information about Australians where that personal information has been created by the organisation itself, rather than acquired by the organisation from the individual directly, or from a third party. Nevertheless, given that the Explanatory Memorandum explains that the extra-territorial provisions of the *Privacy Act* are intended to apply to organisations which collect information from Australia, even if they have no physical presence but only an online presence in the country, the *Privacy Act* will likely apply to at least some of the personal information that organisations such as Facebook include in their records.

The next question must be, then, whether biometric templates, and the information from which they are created – namely photographs, associated information, such as tags and summary information − constitute personal information for the purposes of the Australian link provisions and the amended *Privacy Act* more generally.

C Do Biometric Templates, Photographs and Summary Information Constitute 'Personal Information' within the Meaning of the Amended Privacy Act 1988 (Cth)?

The definition of 'personal information' which will be inserted into the *Privacy Act* when the amendments in the *Privacy Amendment Act* take effect is as follows: 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.[101]

---

99 See, eg, New Zealand Law Commission, above n 95, 76-82; Manitoba Government, *Freedom of Information and Protection of Privacy Act Resource Manual*, 2nd ed, 30 <http://www.gov.mb.ca/chc/fippa/public_bodies/resource_manual/index.html>; Office of the Privacy Commissioner for Personal Data, Hong Kong, *Data Protection Principles in the Personal Data (Privacy) Ordinance: from the Privacy Commissioner's perspective*, 2nd ed, 16-23 <http://www.pcpd.org.hk/tc_chi/publications/files/Perspective_2nd.pdf> 16-23; Office of the Privacy Commissioner for Personal Data (UK), 'Installation of CCTV Systems in public places', paper for Legislative Council Panel on Security, No. CB(2)1770/01-02(01), 3 < http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0409cb2-1770-1e.pdf>.

100 As noted below, this is unfortunate not only due to the lack of clarity as to the meaning of the term as used in *Privacy Act* s 5B, but also leads to some ambiguity as to the extent to which some of the APPs will apply where information is created or internally generated about individuals.

101 *Privacy Amendment (Enhancing Privacy) Act 2012* (Cth) sch 1 item 36.

Under this definition, information can be personal information even where it does not identify a person per se, but where it can be combined with other information in the possession of the relevant entity to allow an individual to be identified.[102] In relation to biometric templates created by Facebook, these will be likely to constitute 'personal information' in the hands of the organisation because they are linked to a user's account and are therefore 'about an identified or reasonably identifiable individual'. Although it is possible that the template will be incorrectly linked to an individual account,[103] this will not prevent the template from being considered 'personal information' because the definition encompasses information and opinions, whether true or not.[104]

To create a face print, Facebook needs to compile and use summary information, involving comparisons of photographs and associated data relating to the person about whom the template is to be created.[105] It has been estimated that Facebook holds around 60 billion photographs which have been uploaded by users.[106] These photographs may depict the user him/herself and other users of Facebook, as well as people – including children – who do not have an account with Facebook. Whether these photographs in and of themselves constitute 'personal information' within the meaning of the new definition of that term will depend on whether the person in the photograph is identified, or reasonably identifiable.

As the latest amendments to the *Privacy Act* have only recently been passed, no guidance has yet been provided by the OAIC on the application of this definition to images. In general, however, the Government has indicated a need for more detailed

---

102 This overcomes a limitation inherent in the current *Privacy Act* whereby the definition of personal information is 'information… about an individual whose identity is apparent, or can reasonably be ascertained, *from* the information or opinion': at s 6(1) [emphasis added]. This arguably excludes from the meaning of personal information, information such as biometric templates which, being algorithms, can only identify an individual if the algorithm is linked with other data that identifies the individual and cannot identify an individual *from* the information in and of itself: see *ALRC Report*, above n 7, vol 1, 307 [6.55], 309 [Recommendation 6.1].

103 Stephen Wilson writes that '[b]ecause biometrics are fuzzy, we can regard a biometric identification as a sort of opinion': Stephen Wilson, *The Fundamental Privacy Challenges in Biometrics* (20 October 2012) Lockstep Blog <http://lockstep.com.au/blog/2012/10/20/biometrics-and-privacy-basics>.

104 *Privacy Amendment (Enhancing Privacy) Act 2012* (Cth) sch 1 item 36.

105 Facebook, *Tagging Photos*, above n 23.

106 EPIC, above n 17, 1. Although, according to the Electronic Frontier Foundation, Facebook refuses to reveal the actual number of photographs that it holds in its database.

guidance from the OAIC as to the meaning of the term 'personal information.'[107] As to the application of the current definition of 'personal information'[108] to images, the OAIC has only restated the provisions of the Act and advised that 'images of persons in photographs and films are treated as personal information under the [Privacy] Act where the person's identity is clear or can be reasonably worked out from that image.'[109] More detailed guidance on the application of the current definition to images is provided by state-based Privacy Commissions, such as the Office of the Victorian Privacy Commissioner, which notes that it in determining whether an image constitutes personal information, it is necessary to take into account a number of factors, such as the clarity of the image and the context.[110] This is likely to remain the case under the new definition of personal information.

In terms of whether photographs on Facebook constitute personal information, this will depend on the photograph itself and associated data (such as tags or GPS location coordinates). If a Facebook user is tagged by another user in a photograph, the photograph will be 'personal information' within the meaning of the Act because tags relating to other users are always associated with that user's account and are therefore information about an identified or reasonably identifiable individual.[111] However, where a photograph is tagged with the name of a person who is not a registered Facebook user, the image may still be considered personal information because the name – attached to the image – identifies an individual. Where a photograph of a person who is not a registered user of Facebook is incorrectly

---

107 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), 61.

108 *Privacy Act* s 6(1) currently defines personal information as: '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.'

109 Office of the Australian Information Commissioner, *What Do I Need to Think About if I Want to Put Photos on the Web*? <http://www.privacy.gov.au/faq/business/gen-q5>.

110 Office of the Victorian Privacy Commissioner, *Images and Privacy Information Sheet 01.03* (31 January 2003) <http://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/images-and-privacy/$file/info_sheet_01_03.pdf>.

111 Facebook, *Tagging Photos*, above n 23. Note that even if the tag does not correctly identify a person in a photograph by name, the photograph is still likely to be considered as personal information because the information does not need to be true: *Privacy Amendment (Enhancing Privacy) Act 2012* (Cth) sch 1 item 36.

tagged, it is possible that the photograph will not be considered personal information because it is not about an identified or reasonably identifiable person.[112]

Where a person in an image is not named by the addition of a tag, then the image will not be treated as personal information in the hands of Facebook, unless the person is reasonably identifiable by that organisation. If a biometric template of that person is stored in the Facebook database, however, then the person will be identified or reasonably identifiable by virtue of the face recognition software: indeed the whole purpose of the tag suggest feature is to identify people in images before tags are added.

Therefore, an image may be considered personal information, depending on what it reveals and whether a person in the image is named or otherwise identifiable, whereas a biometric face print in the hands of Facebook will always be personal information under the new definition of that term. Summary information from which a template is created will also be considered personal information under the new definition as it is linked to a particular user.[113]

Reference needs also to be made to the fact that the definition of personal information requires information to be 'about' an individual. It has been said that biometric templates are not so much information about a person as information of and intrinsic to a person.[114] The ALRC discussed the interpretation of the words 'about an individual' and whether they should be amended to 'relate to an individual' – deciding against that change.[115] Although the question of whether information can properly be said to be about an individual will sometimes not be straightforward,[116] it would seem that information can be 'about' an individual where it either identifies the individual or can be linked to other information identifying the individual.[117]

---

112 Although if Facebook does create biometric templates or hold summary information about people who are not Facebook users then this position may be different as the person may be identifiable by comparison of the image in question with the template or summary information.

113 Facebook, *Tagging Photos*, above n 23. As is the case with biometric templates, summary information may not be considered personal information under the current definition in the *Privacy Act* if identification of an individual is not possible from the information itself.

114 Roger Clarke, *Biometrics and Privacy* (15 April 2001) <http://www.rogerclarke.com/DV/Biometrics.html#Thr>.

115 *ALRC Report*, above n 6, vol 1, 306 [6.51].

116 See, eg, ibid vol 1, 304 [6.40]-[6.43].

117 Ibid vol 1, 298 [6.18] referring to a discussion of the term 'about an individual' in a report prepared in 2004.

D Do Photographs, Summary Information and Biometric Templates Constitute 'Sensitive Information' within the Meaning of the Amended Privacy Act 1988 (Cth)?

Under the *Privacy Act*, certain types of personal information are classed as 'sensitive information' and the new APPs include more stringent requirements around the collection, storage and use of that information, to reflect its nature.[118] The ALRC gave consideration, in its 2008 report, to whether biometric information should be regarded as sensitive information and recommended that the definition of sensitive information be amended to include 'biometric information collected for use in automated biometric verification and identification systems and biometric template information.' The *Privacy Amendment Act* adopts this recommendation.[119]

What is meant by 'automated biometric verification and identification' is not clarified in the amending legislation, nor in the Explanatory Memorandum. In making recommendations for the inclusion of biometric templates and certain biometric information in the definition of sensitive information, the ALRC also did not offer any definition of 'automated biometric verification'.[120] Whilst the ALRC refers to a number of automated biometric identification systems, such as the use of a biometric template in a passport or to access an Automated Teller Machine, a building or a computer system,[121] there is no discussion of the use of biometrics in relation to social networking, and no consideration of the fact that a template may be used for a purpose such as 'tag suggest'. On the other hand, it seems quite clear that the tag suggest feature is a form of automated biometric identification: it is difficult to describe it as anything else. Accordingly, any biometric templates held by Facebook will be considered sensitive information when the new definition comes into force.

More difficulty exists around the question of the extent to which a photograph constitutes sensitive information. A photograph *may* be considered sensitive information depending on the information revealed by the image itself and any associated metadata[122] – for example, a photograph of two same sex individuals

---

118 *Privacy Act* sch 3 [NPP 10].

119 *Privacy Amendment (Enhancing Privacy) Act 2012* (Cth) sch 1 item 42.

120 *ALRC Report*, above n 6, vol 1, 324 [6.119] and 326 [Recommendation 6-4].

121 *ALRC Report*, above n 6, vol 1, 406 [9.64].

122 See, eg, Facebook's Data Use Policy in which it is noted that '[w]hen you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video': Facebook, *Data Use Policy*, above n 15.

kissing each other could be considered sensitive information because it reveals information about an identified individual's sexual orientation.[123]

However, photographs are also a form of biometric information.[124] Therefore, when the *Privacy Act* amendments to the definition of sensitive information come into effect in March 2014, photographs and summary information which are used to create a biometric template will probably be regarded as sensitive information, given that they are collected for the purpose of automated biometric identification.[125] It is also possible that, when the tag suggest feature becomes available to users again, all photographs which inspire an automatic tag suggestion will be considered sensitive information.

The extent to which the APPs may present compliance risks for Facebook is now considered, with particular focus on the principles set out in Pt 2 of the Act, namely those relating to the collection and receipt of information, including sensitive information. This discussion is predicated on the assumption that the amended *Privacy Act* could apply to Facebook's activities of collecting, receiving and creating personal information from Australia.

---

123 The *Privacy Amendment Act* amends the definition of 'sensitive information' in the *Privacy Act* to include information about an individual's 'sexual orientation' (as opposed to 'sexual preferences'): at sch 1 item 41.

124 *ALRC Report*, above n 6, vol 1, 323 [6.115]. 'Biometric information' is not defined in the Act but the Explanatory Memorandum notes that the amendment to the definition of sensitive information is to implement ALRC recommendations and the Explanatory Memorandum also notes the broad reach of what is capable of being considered biometric information: Explanatory Memorandum, Privacy Amendment (Enhancing Privacy) Bill 2012 (Cth) 62, Item 42.

125 The term 'automated biometric identification' is not defined in the *Privacy Amendment Act*, nor in the Explanatory Memorandum, although the Explanatory Memorandum notes that amended definition of sensitive information is designed to reflect the ALRC's recommendations in relation to biometric information and templates: Explanatory Memorandum, Privacy Amendments (Enhancing Privacy Protection) Bill 2012 (Cth) 62, Item 42. The ALRC notes that biometric information should be classed as sensitive information when it is collected for use in automated systems and that this protection is necessary 'to address the most serious concerns around biometric information, for example, that such information may be used to identify individuals without their knowledge or consent': ALRC, above n 6, vol 1, 325 [6.120].

E Collection and Receipt of Personal Information, Including Sensitive Information

The new APPs contain a principle relating to the collection of personal information.[126] The collection principle under the APPs only relates to information that has been collected and solicited.[127] As discussed above, there is some ambiguity over the meaning of the term 'collect' as used in the Act, but the term 'solicit' is defined as follows:

> an entity *solicits* personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.[128]

The words 'or to provide a kind of information in which that information is included' are key here as they suggest that information can be solicited even when that information is not specifically requested, but where it is received as part of a *general request* for the provision of information, which will include personal information.[129]

It is, therefore, possible that Facebook would be deemed to collect and solicit personal information in the form of photographs, and tags or other information (such as GPS coordinates) added to or embedded within photographs. This is because, even if Facebook has not actively requested any particular piece of information, the Facebook model itself is premised upon the sharing of personal information by users about themselves and others. Facebook's stated mission is 'to make the world more

---

126 *Privacy Act* sch 3 [NPP 1]; *Privacy Amendment Act* sch 1 [APP 3]. Under the NPPs it is not clear whether this applies to information that has not been solicited (refer to the discussion earlier in this article). Under the APPs, however, unsolicited information is specifically covered and retention of personal information that has not been solicited is only permitted if the organisation could have collected it in accordance with the information collection principle or where it is unlawful or unreasonable to de-identify it or destroy it: *Privacy Amendment Act* sch 1 [APP 4].

127 *Privacy Amendment Act* sch 1 [APP 3.7].

128 *Privacy Amendment Act* sch 1 item 44.

129 While on the one hand a decision of the Administrative Decisions Tribunal, referred to by the NSW Law Reform Commission (NSWLRC), suggests that virtually all complaints received by investigative agencies will be considered to be unsolicited for the purposes of privacy legislation, the NSWLRC nevertheless refers to conflicting advice issued by Privacy NSW to the effect that agencies holding themselves out as being the appropriate body to receive complaints should not treat complaints received as unsolicited: see NSWLRC, *Privacy Legislation in New South Wales*, Consultation Paper No 3 (2008), 87 [5.58].

open and connected'[130] and it has been noted that 'Facebook's business model depends on the promiscuity of its members.'[131] Indeed, in some cases Facebook has actively encouraged users to share information about others, such as by providing the tag suggest feature for users.[132]

It seems clear that the creation of biometric templates will not fall within the collection principle given that templates are not in any sense solicited, but are created by Facebook from other information in their possession.[133] To adopt the words of the ALRC, Facebook has 'done nothing to cause the information to be sent to it.'[134] Accordingly, the creation of biometric templates, as well as summary information, will not be considered under the collection principle, but may fall to be considered as unsolicited information which is received by an APP Entity: this is discussed further below.

Although an organisation does not ordinarily require the consent of the individual to whom the personal information relates before collection occurs, the collection should be reasonably necessary for one or more of the organisation's functions or purposes.[135] Facebook could almost certainly argue that the collection of photographs and associated information (such as tags) of users and non-users alike is necessary, given that the sharing of personal information by members about themselves is the very reason users open a Facebook account.

It will be recalled that photographs and associated information (such as tags) may be treated as sensitive information in some cases, and will be regarded as sensitive information when used in connection with automated biometric identification. In relation to the collection of sensitive information, compliance with the APPs requires Facebook to have the consent of those to whom the information relates.[136] The

---

130 Facebook, *Product/Service* <www.facebook.com/facebook>.

131 Johnston and Wilson, above n 61, 63.

132 EPIC, above n 17, 19, 25. However, note that the Facebook Terms of Use specifically require users to refrain from tagging others without having first received consent to do so: Facebook, *Statement of Rights and Responsibilities,* above n 15; Facebook, *Data Use Policy*, above n 15.

133 By analogy, Privacy NSW has, according to the NSWLRC, been warning agencies against treating complaints made to them as unsolicited, where the agency has held themselves out as being the appropriate point of contact for complaints: NSWLRC, above n 129, 5 [5.58].

134 *ALRC Report*, above n 6, vol 1, 725 [21.51].

135 *Privacy Amendment Act* sch 1 [APP 3].

136 Ibid sch 1; *Privacy Act* sch 3 [NPP 1]. [APP 3]. However, when the new APPs come into effect and in the event that information is unsolicited and consent to the receipt of the

question of whether Facebook users have consented to the collection of sensitive personal information is a complex one, the answer to which depends on the nature of the sensitive information in question as well as the construction and application of Facebook Terms of Use to information.

Although Facebook users, when opening an account, agree to be bound by Facebook's terms and the Data Use Policy, and although agreement to these terms is possibly sufficient to constitute consent to the collection and use of sensitive information, such as photographs, there are still questions around whether that consent is effective for ensuring compliance with the amended *Privacy Act*.[137] The *Privacy Act* currently defines consent to include express or implied consent and this definition remains unchanged by the new legislation. As noted by the ALRC, the meaning of consent as used in the *Privacy Act* does not disturb the requisite general law elements of consent: namely that consent must be given voluntarily, and the person providing the consent must have the capacity to understand and communicate their consent.[138] In determining whether consent has been provided voluntarily, the ALRC notes that this will depend, inter alia, on whether an individual has a clear option not to consent, and whether the consent is given specifically and not bundled with other purposes.[139]

---

information is not obtained, the organisation may still be able to hold the information without de-identifying it, although the information must then be dealt with in accordance with the remaining privacy principles: *Privacy Amendment Act* sch 1 [APP 4].

137 The *Privacy Act* currently defines consent as including express or implied consent: at s 6. This definition remains unchanged by the *Privacy Amendment Act*. As noted by the ALRC, the meaning of consent as used in the *Privacy Act* does not disturb the requisite general law elements of consent: namely that consent must be given voluntarily, and the person providing the consent must have the capacity to understand and communicate their consent: *ALRC Report*, above n 7, vol 1, 669 [19.9]. In determining whether consent has been provided voluntarily, the ALRC notes that this will depend, inter alia, on whether an individual has a clear option not to consent, and whether the consent is given specifically and not bundled with other purposes: vol 1, 669 [19.10]. At the initial stage of opening a new account with Facebook users are informed as follows: '[b]y clicking Sign Up you agree to our terms and that you have *read* our Data Use Policy, including our Cookie Use.' Facebook <https://www.facebook.com> [emphasis added]. Later in the sign-up process new Facebook users do indicate their agreement to the Data Use Policy: Europe v Facebook, *Legal Procedure against "Facebook Ireland Limited"*, Complaint No 8, Attachment 8 <http://www.europe-v-facebook.org/EN/Complaints/complaints.html>.

138 *ALRC Report*, above n 6, vol 1, 669 [19.9].

139 Ibid vol 1, 669 [19.10].

In the context of complaints made about Facebook to the Irish DPC, it has been argued that the means of gaining user consent to the provisions of the data use policy is deliberately ambiguous. This is said to be the case because users indicate consent to the Data Use Policy indirectly (by entering a code given as part of the security check process on signing up).[140] Arguably consent to the Data Use Policy is therefore bundled with other purposes (the security check) and the other purposes take prominence over the consent.[141] If this is so then users may not be considered to have effectively consented to the collection and use of their sensitive information for the purpose of ensuring compliance with the data collection principle.

In relation to sensitive information about those who are not registered users of Facebook, the consent of those individuals has clearly been neither sought nor given. Although the Facebook terms are available to non-users and are stated to apply to users and 'others who interact with Facebook' they are unlikely to apply to those who have not registered with the site (or who have not otherwise entered into a contract with Facebook). Even if a person who is not a registered Facebook user does interact with the Facebook site,[142] the Terms of Use are not specifically drawn to their attention as a condition of using the site and they are not required to indicate consent to those terms in any way. Of course, many individuals who have photographs or other personal information about them posted on Facebook will not interact with Facebook and may not be aware of the existence of their information on the site. It must also be remembered that many of those whose photographs and other personal information are posted on Facebook will also be minors who might not be considered to possess sufficient capacity for giving consent in any event.[143] Indeed, one aspect of EPIC's complaint to the US Federal Trade Commission was that Facebook users are encouraged to tag a child in photographs, even if that child is not a Facebook

140 Europe v Facebook, above n 137, Complaint no 8, 4 and Attachment 8. In the Irish DPC's audit of Facebook, the office did not make any specific findings as to whether the Data Use Policy was sufficient for the purpose of obtaining users' consent to the collection of their information per se. However, the office did recommend that the Data Use Policy be made more accessible and given greater prominence during the registration process: Data Protection Commissioner (Ireland), above n 25, 5. The office also noted that 'reliance upon the Facebook Data Use Policy as the sole means for capturing user consent for the use of their information may not always be considered acceptable…for all possible uses of data': at 14.

141 Europe v Facebook, above n 137, Complaint no 8, attachment 8(b).

142 As is possible when a non-registered person visits a corporate page on Facebook.

143 See generally *ALRC Report*, above n 6, vol 3, Chapter 68 [Decision Making by and for Individuals Under the Age of 18].

member.[144] Accordingly, if sensitive information in the form of photographs or associated information about individuals who are not registered users of Facebook is considered to be collected and solicited by Facebook, the organisation will not be in compliance with the new data collection principle.

Although it has been submitted here that photographs and associated information such as tags might be considered to be personal information that has been collected and solicited by Facebook, this is not beyond doubt. If such information is not considered to be solicited, it will fall to be considered under the principle relating to receipt of unsolicited information.[145] Assuming that photographs and associated information fall within the receipt of unsolicited information principle, one consequence is that Facebook may be able to retain and use even sensitive personal information about individuals who are not registered Facebook users, even where those users have not consented to the retention of that information. This is because, although the receipt principle requires an entity to destroy or de-identify information which it could not have collected in accordance with the collection principle (APP 3), an exception to that requirement is where it would not be lawful or reasonable to destroy or de-identify the information in question.[146] As noted above, in accordance with the collection principle (APP 3), those who are not registered users of Facebook have not consented to the collection of sensitive information (which may include photographs and other associated information, such as tags or geolocation data). However, Facebook may be able to mount an argument that the destruction or de-identification of that information, even so, would be unreasonable. Although Facebook has the right to remove any content which violates its terms or policies (and one of those terms is that users have obtained consent to the collection of information from others[147]) this does not amount to an obligation to remove such content.[148] Facebook may be able to argue that removal of material in this way constitutes an unjustified interference with a Facebook user's freedom of expression,[149] and would also be technically difficult and expensive to police.[150]

---

144 EPIC, above n 17, 25. According to EPIC, Facebook also has a large number of registered users who are under the age of 13: at 24.

145 *Privacy Amendment Act* sch 1 [APP 4].

146 Ibid.

147 Facebook, Statement of Rights and Responsibilities, above n 15, term 2.

148 See, eg, *Roadshow Films Pty Ltd v iiNET Limited (No 3)* [2010] FCA 24, [427].

149 In Australia there is no general right to freedom of expression, though freedom of communication on government and political matters is recognised as being implied under the Constitution of Australia: *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520. However, Australia has ratified the International Covenant on Civil and Political Rights and art 19(2) provides that everyone shall have the right to freedom of

In relation to summary information and biometric templates (face prints), these are certainly unsolicited information but there is doubt about whether the information can be said to have been 'received', given that it is not obtained from a third party.[151] Although the word 'received' is not defined in the amended *Privacy Act* it can be defined to include acquisition (of something).[152] In line with the dictionary definition of 'receive', information created by an organisation will have been acquired, and thus received, by the organisation. On the other hand the wording of this principle does not easily apply to information that is internally generated: indeed it would make little sense for an organisation to create personal information before making a decision as to whether or not it was entitled to retain it.

Conversely, taking into consideration that one of the stated objects of the *Privacy Act*, as inserted by the recent amending legislation, is to promote the protection of the privacy of individuals, [153] the principle relating to the receipt of unsolicited information should probably be interpreted broadly to include within the meaning of 'receipt' internally generated information. Certainly the ALRC, in recommending changes to the *Privacy Act*, intended that information obtained by surveillance and

---

expression. This right, in turn, may be subject to lawful restrictions to protect, inter alia, the rights and reputations of others (art 19(3)): *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23 (entered into force on 23 March 1976).

150 In *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16, the High Court considered, inter alia, what constituted 'reasonable steps' on the part of an Internet Service Provider (ISP) to prevent or avoid copyright infringements on the part of its users. Although the circumstances of an ISP are quite different from those of a site host with the contractual ability to remove content, and although the iiNET case related to allegations of copyright infringement and not to the *Privacy Act*, comments made in that judgment are nevertheless insightful and reveal that practical considerations relating to the nature of the internet were taken into account in considering what is 'reasonable': see, eg, [138] (French CJ, Crennan and Kiefel JJ) noting that 'iiNET had many thousands of account holders. Was it a reasonable step to require of iiNET that it monitor continually the activities of IP addresses?'

151 The word 'receive' is not defined in the Act but could be interpreted as being limited to information that comes into the possession of an entity from another party, rather than including information that is 'created' or generated by the entity itself. The receipt principle was inserted following the ALRC's recommendation to this effect and to deal with the problem they saw that related to the fact that entities often received information from others without having taken any active steps to collect the information. *ALRC Report*, above n 7, vol 1, 720 [21.36].

152 Concise Oxford Dictionary, above n 94.

153 *Privacy Amendment Act* sch 4 item 2A.

other means should be included within the collection principle.[154] Given that information obtained by surveillance cannot be considered to have been 'solicited' it will only be caught by principles relating to collection by virtue of falling within the receipt of unsolicited information principle.[155]

Assuming, then, that the principle relating to the receipt of unsolicited information will apply to information that has been internally generated, sensitive information – such as biometric templates and summary information – that has been created without the permission of the person to whom it relates will have to be destroyed or de-identified unless it is not lawful or reasonable to do so. In relation to biometric templates, users may be said to have consented to the creation of these if they have actively enabled the tag suggest feature. Where the tag suggest feature is enabled as a default setting, however, the position is less clear. In relation to the creation of summary information, it will be recalled that this information exists unless and until users remove any tags from photographs of themselves posted to Facebook. There is no opportunity for users to prevent themselves being tagged in photographs. Whether inaction - a failure to remove tags - is sufficient to constitute consent must be doubtful. Assuming that a Facebook user does not consent to the creation of a biometric template about himself or herself, nor to the creation of summary information, is it reasonable for Facebook to destroy or de-identify the information? Facebook could argue it is not reasonable to do so, in that the information enables the site to provide important features (such as tag suggest) to its users and that users have the ability to self-police and ensure the removal of this information should they so wish.[156]

It is not clear whether Facebook creates biometric templates or summary information about those who are not registered users of Facebook – though this has been alleged.[157] If it does, it would be more difficult for Facebook to argue that it is unreasonable to destroy or de-identify this information: the information does not appear on a user's page, so there can be no argument that it interferes with freedom of expression or 'consumer choice'. Equally, the information is not used to provide services to Facebook users; and those who are not registered users of Facebook have no ability to control whether or not this information is created. Accordingly, if the creation of biometric templates and the internal generation of other information about those who are not registered users of Facebook is regarded as being the

154 *ALRC Report*, above n 7, vol 1, 732 [21.81].
155 *Privacy Amendment Act* sch 1 [APP 4].
156 Data Protection Commissioner (Ireland), above n 25, 47-48.
157 Lynch, above n 1, 2.

'receipt' of information under the APPs, it is also likely that the retention of this information would be a breach of the APPs.

There are a number of other privacy principles which apply to the collection, use and disclosure of personal information and which may present compliance risks for Facebook. A consideration of each of those principles is beyond the scope of this article. However, of note is a requirement in the new APPs for an entity's privacy policy to contain information regarding how complaints about a breach of the APPs (or a registered privacy code) should be made and how such complaints will be dealt with.[158] Facebook's privacy code (also referred to as the Data Use Policy) does inform users of the place to which complaints concerning the data use policy should be addressed, but there is no information in the code about how complaints are dealt with. In addition, if the new principles are interpreted so as to impose a requirement that an entity make specific reference to the APPs in its privacy code, this could prove problematic for organisations, such as Facebook, which have a generic privacy code for users in various jurisdictions all over the world.

IV Facebook: Compliance or Complacency?

Despite the ambiguities around the scope of the application of the amended *Privacy Act*, this article has highlighted a number of compliance risks that may apply to Facebook in relation to its collection or creation of photographs, summary information and biometric face prints.[159] One of the most significant risks for Facebook in terms of compliance with Australian information privacy laws concerns its collection (or creation) of sensitive information, particularly where this information relates to individuals who are not Facebook users and who cannot be said to have consented to the collection or use of this information. Although it is not clear whether Facebook has ever created (or ever will create) biometric templates of individuals who are not registered Facebook users, the organisation is in possession of vast amounts of information about individuals who may never have interacted with the site: this includes photographs and associated information, and possibly summary information. Some of this information will, in turn, be sensitive information: such as where a photograph reveals particular information about an identifiable individual, or where summary information is to be used for creating a biometric template. Compliance risks for the organisation also relate to the creation of summary information and face prints of its own users, at least while there exist

158 *Privacy Amendment Act* sch 1 [APP 1.4], [APP 5.2].

159 In addition to those APPs that are considered, there are a number of other APPs that apply to personal information and sensitive information but which are not discussed in this paper: *Privacy Amendment Act* sch 1.

ongoing questions as to whether those users can be said to have properly consented to the creation of that information. This may be a particular risk where (despite the Facebook Data Use Policy) features are enabled as a default setting (for example, where tag suggest is enabled as a default setting, requiring users to opt-out rather than opt-in) or where users have no ability to opt-out of a feature (for example, users are unable to opt-out of manual tagging of themselves by others.)[160]

Even to the extent that the *Privacy Act* might not have direct application to certain practices of Facebook, the APPs nevertheless provide a benchmark by which any organisation's practices can be measured. Indeed, the Irish DPC reported on Facebook's practices not in terms of whether or not they contravened the Irish Data Protection laws, but rather to the extent that they represented or fell short of best practice.[161] Facebook has also shown itself to be responsive to public sentiment in relation to user control of information,[162] and its decision to disable the tag suggest feature in the US – although explained by the organisation as an opportunity to enhance efficiency of the tool[163] – could also be seen as a response to privacy concerns raised in relation to the technology. What is more, it does seem likely that as and when the tag suggest feature is re-introduced, at least for users outside of the US, it will allow users to opt-in rather than require them to opt-out.[164]

Even so, significant concerns must remain for those who are not registered users of Facebook and whose personal information is posted and possibly used without their consent, or even knowledge. Concerns must also remain about the use of face recognition technology generally, particularly in the private sphere. This is so even where consent to creation of biometric templates and summary information is given. Questions as to security of the information, the way in which it is used, and the potential applications of the technology and the massive databases of personal information it generates must continue to be asked.

Furthermore, the Australian *Privacy Act* should be considered, at best, a blunt instrument by which to enhance the level of control that individuals have over their

---

160 Facebook, *Tagging Photos* above n 23; Data Protection Commissioner (Ireland), above n 25, 48.

161 Data Protection Commissioner (Ireland), above n 25, 3.

162 See, eg, 'Facebook Backs Down, Reverses on User Information Policy', *CNN* (online), 18 February 2009 <http://edition.cnn.com/2009/TECH/02/18/facebook.reversal/index.html>.

163 Above p 3 and n 14.

164 Anita Ramasastry, 'The Right to be Untagged: As Facebook Disables Facial Recognition for EU Consumers, US Consumers are Left Wondering What's Next for Them', *Verdict* (online), 25 September 2012, <http://verdict.justia.com/2012/09/25/the-right-to-be-untagged>.

personal information. Individuals who are concerned about possible non-compliance with Australian's information privacy laws do not have standing to bring legal action for breach of those principles.[165] Instead users must address unresolved complaints to the OAIC who may decide to investigate them. There is also the problem of enforcement. Under the newly amended *Privacy Act*, the Commissioner will have the power to make a number of orders against agencies and organisations who are found not to have complied with the privacy principles, including a civil penalty order up to a maximum of $1.1 million in relation to serious and repeated interference with the privacy of an individual.[166] Timothy Pilgrim, the current Australian Privacy Commissioner, has been quoted as saying that 'fines will send a clear message that the community expects better legal protection.'[167]

Whether the imposition of fines will be anything more than a message about what the community expects must be questionable given the significant challenges involved in trying to enforce Australian laws against an organisation that is not incorporated in Australia and has no presence here.[168] Moreover, while Facebook has previously shown itself to be susceptible to public pressure in relation to decisions perceived as impinging on individual control of their information,[169] it is increasingly

---

165 Recommendations made by the ALRC for the introduction of a cause of action for serious invasion of privacy are still some way off from being implemented: ALRC, above n 7, vol 3, 2584-2585. As to the status of these recommendations, see Department of the Prime Minister and Cabinet, *Privacy Reforms,* Australian Government <http://www.dpmc.gov.au/privacy/reforms.cfm>. Even if the ALRC's recommendations are implemented an action for invasion of privacy will only lie if a person shows they had a reasonable expectation of privacy, and that the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

166 *Privacy Amendment Act* sch 4 item 50; Explanatory Memorandum, Privacy Amendments (Enhancing Privacy Protection) Bill 2012 (Cth) 62, 226-227.

167 Andrew Colley, 'Big Firms Face Fines and Hefty Sanctions Over Privacy Breaches', *The Australian* (online), 3 July 2012 <http://www.theaustralian.com.au/australian-it/it-business/big-firms-face-fines-and-hefty-sanctions-over-privacy-breaches/story-e6frganx-1226415040657>.

168 A consideration of cross-border enforcement issues and challenges is beyond the scope of this paper, but see generally Dan Svantesson, 'Protecting Privacy on the "Borderless" Internet – Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168. See also OAIC, Submission no 16 to Senate Standing Committee on Environment, Communications and the Arts, Parliament of Australia, *The Adequacy of Protections for the Privacy of Australians Online,* August 2010, 19-21.

169 As at December 2011, Facebook had 845 million monthly active users: Facebook Inc., 'Prospectus: Subject to Completion', Registration Statement under the Securities Act 1933

subject to countervailing pressures brought to bear by other stakeholders, notably its investors and advertising partners.[170] What is more, the extent to which public disapproval of Facebook's practices poses any real threat to the organisation may decrease in direct proportion to the growth in size of the Facebook community: the more people use Facebook to connect with each other, the more they are likely to feel that there is no 'viable and popular alternative' to the site.[171] Perhaps, as one commentator has suggested, Australians are prepared to trade privacy with free services, this trade being 'the Faustian pact into which we have entered in order to survive in this age of constant connectivity, where the tentacles of Facebook … are extending to every corner of the internet '.[172]

As noted by the ALRC in its 2008 report, 'effective law reform must respond not only to current problems and gaps in the law, but also anticipate where there are likely to be significant problems in the future that will require some kind of regulation.'[173] It is unfortunate then that, in the era of Web 2.0 and the growth of social media platforms which are often owned and operated from outside of Australia, amendments to the *Privacy Act* still do not adequately clarify the threshold issue of the extent to which the Act regulates the practices of overseas organisations. Even if the *Privacy Act* does apply to acts and practices of an organisation in relation to information (such as summary information and biometric templates) that is internally generated by an organisation outside of Australia, the extent to which the collection and receipt principles in the APPs (namely APP 3 and APP 4) apply to that type of information is unclear. Whilst the recent amendments to the *Privacy Act* were intended to preserve the principle of technological neutrality,[174] the ALRC has also noted the importance of legislation that is technologically aware.[175] Unfortunately there are a number of respects in which the legislation appears to be technologically blind, particularly in so far as little or no proper consideration has been given to ensuring that fundamental definitions, such as the definition of 'collect', do not exclude certain means of information acquisition.

(Form S-1), 1 February 2012, <http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm>.

170 See, eg, Chander, above n 19, 1841; Johnston and Wilson, above n 61.

171 Chander, above n 19, 1841.

172 Julian Lee, 'Facebook's Power Should Worry Us All', *The Sydney Morning Herald* (online), 10 October 2011 <http://www.smh.com.au/opinion/society-and-culture/facebooks-power-should-worry-us-all-20111009-1lfu0.html>.

173 *ALRC Report*, above n 6, vol 3, 2571 [74.141].

174 *ALRC Report*, above n 6, vol 1, 422 [10.9].

175 Ibid vol 1, 421 [10.5].

According to Hamburg's DPC, face recognition technology is already moving faster than the public debate, and data protection laws are generally unable to keep pace.[176] In the meantime, what is clear is that Facebook's tentacles are extending not only to every corner of the internet but, increasingly, into every corner of our lives. Given the amount of personal information, photographic and otherwise, that is uploaded to Facebook every day, and given our seemingly insatiable appetite to share more and more of our own lives, as well as those of others, Facebook may know more about us than our governments, or even our closest friends. Throw into the information mix the use of face recognition technology and it is possible that there will be, quite literally, nowhere to hide. In an interview with the Wall Street Journal, Google CEO Eric Schmidt was quoted as saying: 'I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time,' and went on to predict that young people may in the future automatically be entitled to change their name to 'disown youthful hijinks stored on their friends' social media sites'.[177] Changing one's name is drastic, but at least feasible. Changing one's face, on the other hand, is quite another thing altogether.[178]

176 Günther Birkenstock, 'Face Recognition Threatens Anonymity in Public', *Deutsche Welle* (online), 11 December 2012 <http://www.dw.de/face-recognition-threatens-anonymity-in-public/a-16431905>.

177 Bianca Bosker, 'Google CEO Eric Schmidt Advises You to Change Your Name to Escape Online Shame,' *The Huffington Post* (online), 17 August 2010 <http://www. huffington post.com/2010/08/16/google-ceo-eric-schmidt-s_n_684031.html>.

178 Acquisti, Gross and Stutzman, above n 31.