Privacy 2.0: Online Privacy in a User-generated World Wide Web

Andrew Ailwood and Chris Govey look at the difference between younger and older Web users when it comes to privacy.

Web 2.0 was spawned from a change in attitude amongst software developers rather than any single technical revolution.[1] The resulting proliferation of user generated content on social media sites such as Wikipedia, YouTube and personal blogs, and increased user interaction through social networking sites such as Facebook, MySpace and Bebo, has led to a rethink of many key regulatory axioms.

In particular, Web 2.0 has fostered a change in users' attitudes towards their privacy.[2] According to Chris Kelly, Facebook's chief privacy officer, the classic notion of the right to privacy as the user's right 'to be left alone' has been replaced by a focus on users' ability to control their personal information.[3] In essence, users are resigned to the inevitability of, and indeed facilitate, the release of their personal information into the public domain; however, they expect that release to be accompanied by a right to privacy that controls how that personal information may be used.

On 30 May 2008, the Australian Law Reform Commission (the ***ALRC***) was due to deliver its eagerly awaited final report and recommendations to the Federal Attorney-General (the ***ALRC Report***) following the ALRC's *Review of Australian Privacy Law*.[4] While the content of the ALRC Report is not yet publicly available,[5] it is expected to address the growing gap between the technicalities of the law of privacy in Australia and the technologies utilised by the private citizens of Australia.[6]

In this expectant period leading up to the release of the ALRC Report, this article discusses the shift in (particularly young) users' attitudes towards privacy that has given Australia the phenomenon of 'Privacy 2.0'. We give particular attention to the use of personal information by advertisers and the possible enforcement options that might be included in amendments to the *Privacy Act 1988* (Cth) (the ***Privacy Act***). Ultimately, regulators must join users in recognising that, as there is no way to guarantee absolute privacy online, the focus of privacy laws must be ***controlling*** the use of personal information, rather than ***preventing*** its use and disclosure outright.

Targeting Advertising

The increasing prevalence and penetration of Web 2.0 is perhaps best reflected in the amounts recently paid by:

- News Corporation to purchase MySpace (US$580 million in July 2005);[7]
- Google Inc to become the exclusive advertisement provider for News Corporation owned sites (including MySpace) for three years (US$900 million in August 2006);[8]
- Microsoft Corporation to purchase a 1.6% stake in Facebook (US$240 million in October 2007);[9] and
- AOL to purchase Bebo (US$850 million in March 2008).[10]

These figures reveal the commercial value of sites that are constantly collecting personal information. Web 2.0's advertising potential resides in the approximately 115 million 'unique' viewers that, for example, MySpace and Facebook each attract to their respective sites every month.[11] Indeed, a study published in March 2007 by Pali Research analyst Richard Greenfield estimated that MySpace generates over US$70 million a month in advertising revenue.[12]

This advertising potential is being extended by developing marketing techniques. Modern sites hyper-target advertisements to users based on their self professed demographic information and the content of a page that they are viewing. For example, where the user is male and using a Sydney IP address to search for information on cricket, it is reasonable to assume that they might be interested in purchasing tickets to a match at the Sydney Cricket Ground. Therefore, an advertisement server using hyper-targeting would advertise an upcoming game at the Sydney Cricket Ground.

More interesting is when advertisers use Web 2.0 to extrapolate users' interests, demographics and use history to classify them into market segments and serve up advertisements accordingly. For example, where the user is male and using a Sydney IP address to look for information on cricket, it is reasonable to assume that they might be susceptible to an advertisement for beer based on the generalised market segment that their details classify them in.

Each of these advertising techniques relies on unidentified information which, as disclosed to advertisers in an aggregate form, is arguably outside the scope of the Privacy Act definition of 'personal information'. However, the next advance in targeted marketing involves selecting those users whose network of friends (as indicated by the structure of their Facebook or MySpace account) reveals them to be a leader or influential personality type, with a correspondingly strong influence on the (purchasing) behaviour of their social circle (or, more likely, circles). Such information is inherently sensitive but arguably (without being attached to traditional identifying detail) falls outside the ambit of the protection of the National Privacy Principles (***NPPs***) in the Privacy Act[13] as it is not 'information or an opinion… about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion'.[14] The question of policy then becomes whether such use of behavioural and psychological data should be subject to a regulatory regime which facilitates rights of access and security and limits the use and disclosure of such data.

Rather than rebelling against this increasing use of users' personal information, Web 2.0 users in a Privacy 2.0 Australia are more likely to prefer to receive advertisements that are targeted to their interests. The ALRC notes that: '[y]oung people appear much more willing to share personal details, post images and interact with others on internet chat sites'.[15] Users are happy to trade their personal information for a perceived benefit; whether it be pure pleasure, a chance at winning the latest computer hardware to facilitate their future browsing or merely so that the unavoidable online advertisements they view are at least tailored to their interests. Indeed, the growing prevalence of such targeted advertisements must be supported by a growth in 'hits' on such advertisements, which is in turn indicative of users' preference for targeted advertising material.

Take-down Notices or Statutory Cause of Action for Privacy Breaches

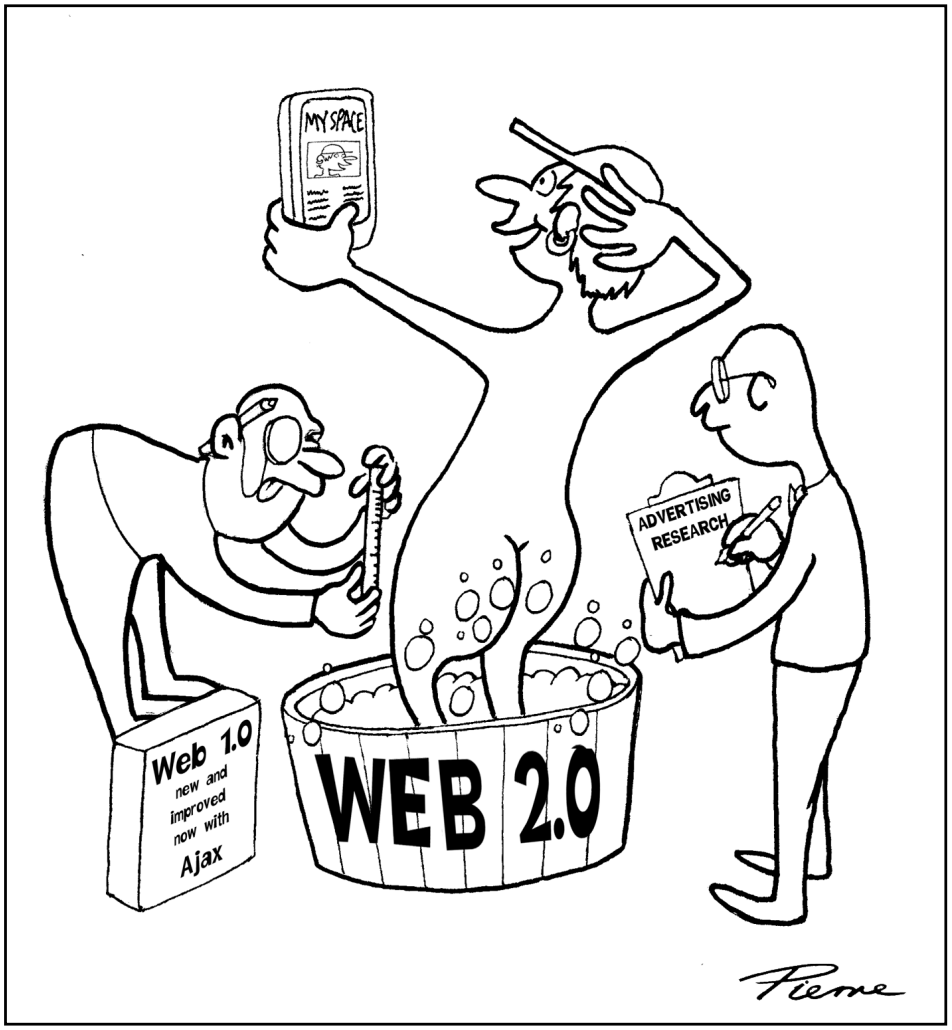
Despite the positive aspects of increased access to Web 2.0 users' personal information discussed above, there are clearly instances where users desire greater con-

trol. One popular feature of social networking sites such as Facebook and MySpace is that they permit users to post photos. As Duncan Watts (a sociologist at Columbia) opined in an interview with The New Yorker in 2006: '[i]f I had to guess why sites like Facebook are so popular, I would say it doesn't have anything to do with networking at all. It's voyeurism and exhibitionism. People like to express themselves, and they are curious about other people.'[16]

The risk is that there will come a time when the user feels it is necessary to restrict the use of their personal information. Just as David Hicks probably regrets posing with a bazooka on his shoulder, and Trevor Flugge no doubt would have preferred that the photo of him shirtless with a revolver in his hand had remained private, how many Web 2.0 users wake up on Saturday morning fearful of the personal information their friends might be about to post online? Perhaps it is fair to say, as the founder and current CEO of Facebook Mark Zuckerberg did in 2006 (regarding students who had been expelled from school as a result of photos of them taking illicit drugs being posted on Facebook): 'I think that that's just the sort of deviant behaviour on the very far end of the distribution'.[17] But at what point does a photo that is damaging to one's reputation, and uncontrollable once released, foster a legitimate privacy concern?[18]

In the internet's infancy, users operated under a screen name or pseudonym, but as the internet pervades the offline, real lives of users, those users have shown an increasing willingness to utilise their real name (in exchange for otherwise unattainable benefits, such as online shopping deliveries or online job applications).

However, with this departure from anonymity comes the risk of real damage to users' reputations and their ability to control their public information. Currently, the law does not provide for an effective, let alone timely, solution. Beyond a desperate appeal to the 'friend' that posted the offending photo, the user has no obvious legal recourse. Although an image is personal information so long as an individual's identity is apparent or can be reasonably ascertained from that image,[19] it will not be regulated by the Privacy Act if it was taken by an individual who is acting in their private capacity,[20] or by someone acting on behalf of a small business which is exempted from the Privacy Act.[21] Even if the Federal Privacy Commissioner (the ***FPC***) investigated the organisation hosting the personal information, a subsequent court order (from the Federal Court or the Federal Magistrates Court) would be required to enforce any determination by the FPC that there has been a breach of privacy.[22]



It is in this context that the ALRC has discussed introducing a take-down scheme similar to that governed by the Australian Communications and Media Authority regulations in the context of online adult content.[23] This could be extended to material that interferes with a user's privacy. While many Web 2.0 sites have developed terms of use that provide for a voluntary take down scheme following notice by users of the existence of offensive content, or even proactively moderate content, a legislated take-down scheme may provide a 'practical, cost-effective remedy for individuals faced with publication of offensive material, including images, relating to themselves. It would enable individuals to exercise some control over how images of themselves are published when they are taken without consent.'[24]

Additionally, the ALRC has considered a statutory cause of action for invasion of privacy, describing it as 'the most effective way to regulate the issue'.[25] This would also give a user direct recourse against the individual posting the photo. Such recourse would be particularly pertinent to Australian users faced with the prospect of having personal information removed from a site hosted by an organisation that is not incorporated or otherwise formed in Australia. Generally speaking, the Privacy Act only applies to such organisations if they are carrying on business in Australia and, even then, only applies in relation to the organisation's acts and practices in Australia.[26] If the relevant personal information was never collected or held in Australia then it may not be covered by the Privacy Act.

Not only might a take-down notice scheme or a statutory cause of action overcome this jurisdictional obstacle; such measures would also provide a pragmatic solution to privacy enforcement between the extremes of an outright ban on cameras in public on the one hand and the arguably toothless provisions of the current Privacy Act on the other. Moreover, a take-down notice scheme or a statutory cause of action would bring Australian law into line with Privacy 2.0 by providing users themselves with the tools to control their personal information.

Conclusion

As the increasingly commercial use of personal information by advertisers and the potential viability of a take-down notice scheme (or even a statutory cause of action for privacy breaches) suggest, there has been a significant shift in users' attitudes

towards privacy since the inception of the internet. Although the ALRC recognises that 'individual control is a more viable regulatory option than technical legal solutions',[27] and that 'young people think of privacy differently from older generations',[28] it seems likely that the ALRC Report will not capitalise on this change in Web 2.0 users' attitudes towards privacy to update Australian privacy law in line with Privacy 2.0. The ALRC believes that '[w]hile young people have slightly different privacy concerns and experiences when compared to older Australians, the differences are not so great as to warrant a reconsideration of the basic framework of the Privacy Act...'.[29]

Regardless of the recommendations encapsulated in the ALRC Report once released, and irrespective of the precise amendments (if any) passed by the Federal parliament, it is undeniable that the shift in users' attitudes that underscores Privacy 2.0 will only gain momentum as the generations of young people that take technology for granted grow older.

Andrew Ailwood is a Senior Associate and Chris Govey a Law Graduate in the Sydney office of Allens Arthur Robinson.

(Endnotes)

1 Wikipedia, 'Web 2.0', http://en.wikipedia.org/wiki/Web_2 (last accessed 25 June 2008).

2 This article, in line with the Australian Government Law Reform Commission's '*Review of Australian Privacy Law: Discussion Paper*' (September 2007, Discussion Paper 72 (the ***ALRC Discussion Paper***), focuses on information privacy, that is the 'establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records' (known as 'data protection'), as opposed to bodily privacy ('the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches'), privacy of communications (that is the 'security [and prevention of interception] of mail, telephones, email and other forms of communication') and territorial privacy ('the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes trespass, searches, video surveillance and ID checks') – see the 'defining privacy' section of the ALRC Discussion Paper (page 114).

3 ALRC Discussion Paper, pages 1730-31.

4 ALRC Discussion Paper.

5 The ALRC Report will not be publicly available until it is tabled in Parliament; the ALRC believes this will occur in August 2008.

6 To this end, '[i]mportant definitions in the Privacy Act—such as the definition of 'personal information', 'sensitive information' and 'record'—should be updated to deal with new technologies and new methods of collecting and storing personal information' (ALRC Discussion Paper, page 105); in particular, the ALRC recognises that reliance on the *Acts Interpretation Act 1901* (Cth) to extend the definition of 'record' to computer data is inadequate (see page 218 of the ALRC Discussion Paper). Similar recognition should be given to the possibility of a users' IP address constituting personal information as other information accretes around it (see page 205 of the ALRC Discussion Paper).

7 News Corporation, 'News Corporation to Acquire Intermix Media, Inc', (18 July 2005), http://www.newscorp.com/news/news_251.html (last accessed 25 June 2008).

8 News Corporation, 'Fox Interactive Media enters into Landmark Agreement with Google Inc', (7 August 2006), http://www.newscorp.com/news/news_309.html (last accessed 25 June 2008).

9 Jay Greene, 'Microsoft and Facebook Hook Up' (25 October 2007) http://www.businessweek.com/technology/content/oct2007/tc20071024_654439.htm (last accessed 25 June 2008).

10 Allen Stern, 'Bebo To AOL for $850 Million', (13 March 2008), http://www.centernetworks.com/aol-acquires-bebo-850-million (last accessed 25 June 2008).

11 Michael Arrington, 'Facebook No Longer The Second Largest Social Network', (12 June 2008), http://www.techcrunch.com/2008/06/12/facebook-no-longer-the-second-largest-social-network/ (last accessed 25 June 2008).

12 Diane Mermigas, citing Richard Greenfield, 'Make Social Networks Pay: Recast Ads', (18 April 2008), http://blogs.mediapost.com/on_media/?p=151 (last accessed 25 June 2008).

13 The NPPs are contained in Schedule 3 of the Privacy Act. The breach of an NPP by an organisation, such as a web hosting site, is a contravention of section 13A(1)(b)(i) of the Privacy Act).

14 See section 6(1) of the Privacy Act for the definition of 'personal information'.

15 ALRC Discussion Paper page 122, citing L Weeks, 'See Me, Click Me: The Publizen's Life? It's an Open Blog. The Idea He May be Overexposed? LOL', *Washington Post (online)* (23 July 2006) <www.washingtonpost.com>.

16 John Cassidy, 'The Online Life: Me Media: How hanging out on the internet became big business' (15 May 2006) The New Yorker, page 50, 55.

17 Id, page 50, 59.

18 Pertinently, the ALRC Discussion Paper notes (at page 119) that '[r]ecently enacted domestic human rights legislation also recognises privacy as a basic human right. For example, s 13 [privacy and reputation] of the *Charter of Human Rights and Responsibilities Act 2006* (Vic)' and the *Human Rights Act 2004* (ACT).

19 See the definition of 'personal information' in section 6(1) of the Privacy Act.

20 Sections 7B(1) and 16 of the Privacy Act.

21 ALRC Discussion Paper, page 1735.

22 ALRC Discussion Paper, page 180.

23 Currently set out in the *Broadcasting Services Act 1992* (Cth) schedules 5 and 7.

24 ALRC Discussion Paper, page 1747.

25 ALRC Discussion Paper, page 1747.

26 In relation to any act or practice outside Australia the organisation must also comply with the rules on transborder data flow in NPP 9.

27 ALRC Discussion Paper, page 1744.

28 ALRC Discussion Paper, page 1715.

29 ALRC Discussion Paper, page 1744.