

# SalingerPrivacy

**We know privacy inside out.**

## **MORE TROUBLE WITH FACEBOOK**

Stephen Wilson, Principal of Lockstep Consulting and Anna Johnston, Director of Salinger Privacy.

*This article does not constitute legal advice, and should not be relied upon as legal advice by any party.*

*This article was originally published by LexisNexis in the Privacy Law Bulletin, (2010) 7(2) Priv LB.*

### **Introduction**

The last edition of *Privacy Law Bulletin* included an article by John Kell and Phillip Ng titled "Privacy and Facebook – the trouble with Facebook". The authors of that article identified two significant privacy risk areas in relation to Facebook's activities: data retention and the disclosure of users' personal information to third parties.

In relation to the latter risk area, the authors concluded that Facebook was complying with Australian privacy law, on the basis that "Facebook can probably infer consent to its use and disclosure of personal information to the extent that such use and disclosure is adequately described in its privacy policy".<sup>1</sup> We respectfully disagree with that conclusion.

In this article, we outline why we believe users have not necessarily consented to the disclosure of their personal information by Facebook to third parties, and we also identify a third major area of compliance risk for Facebook, namely their collection practices.

### **The ease of registration**

As Kell and Ng point out, registering for Facebook is very easy. We contend it is rather too easy, with the site providing only oblique references to the privacy implications of serious collection events such as the importing of contacts, and scant explanation of the default privacy settings.

A brand new Facebook user registers by completing a short web form, providing their first and last name, e-mail address, a "new" password, their sex and birthdate. The password entry is very unusual for you are only called upon to

enter your password once; it is universal practice for registration forms to capture the password twice, to help save the user from typing errors.

The Facebook server then does a simple password quality check (rejecting suggestions that are too short or insecure, like the word "password" itself) and verifies that the user's e-mail address hasn't already been used. Next the user is shown a challenge-response security phrase which they must re-enter; this is a standard web site technique for differentiating a robot attempting to sign up instead of a human. The final step is to click a "Sign up" button, noting the fine print beneath "By clicking Sign Up, you are indicating that you have read and agree to the [Terms of Use](#) and [Privacy Policy](#)", with hyperlinks to the relevant documents where underlined.

The Terms of Use and the Privacy Policy are dense documents, running to approximately 3,900 words and 5,800 words respectively. Crucially, the Privacy Policy only provides a partial account of the all-important Privacy Settings feature. Given the furore over Facebook's default settings and allegations that they tend to serve the interests of the company and not the user<sup>ii</sup>, it is surprising that the Privacy Policy is not more accessible in this area. In particular, the Settings feature is not available to the user during registration, but can only be reviewed after they have completed the sign up. Further, there is no information at all in the Policy's Section 3. *Sharing information on Facebook* about "friend information" or "relationships" (i.e. imported contacts), matters which we discuss further below.

After signing up, the new user is directed to a three step process to set up their Facebook profile. On their face, these steps offer a handy way to populate one's profile and quickly establish a social network, which is after all what will attract most members to the service. Sadly however, we fear that new users may be drawn unwittingly into connecting Facebook to rich veins of personal information about themselves and moreover their external friends.

The first of these steps is to *Find friends*. The new member is invited to enter their email address *and password* in order for Facebook to facilitate introductions. What is barely apparent at this point is that Facebook imports the address book from the user's external e-mail account via an automated API.<sup>iii</sup> The primary purpose mentioned on the Facebook site is to facilitate introductions. That is, Facebook looks through the new user's contacts for e-mail addresses in common with other existing members, and then offers up those members as instant friends. We discuss the implications of this below.

The next two steps prompt the new user to enter their initial profile information (comprising High School, College/University, and Employer) and finally to upload a profile picture. The user is then presented with their initial home page, which at first is dominated by invitations to again "find friends" if you haven't elected to do so already. At the very bottom of the home page is a prompt to visit the privacy settings.

## **Indirect collection of a member's contacts**

One of the most significant express Collections by Facebook (that is, a collection where the user is purportedly aware that something is going on) is surely the e-mail address book of those members that elect to have the site help "find friends". This facility provides Facebook with a copy of all contacts from the address book of the member's nominated e-mail account. It's the very first thing that a new user is invited to do as they register.

We are not in a position to judge how the typical or "average" Facebook member will understand the "find friends" feature. It is very briefly described as "Search your email for friends already on Facebook" and without any further elaboration, new users are invited to enter their e-mail address and password for an external mail account. A link labelled "Learn more" in fine print leads to the following additional explanation:

*We will not store your password after we import your friends' information. We may use the email addresses you upload through this importer to help you connect with friends, including using this information to generate Suggestions for you and your contacts on Facebook. If you don't want us to store this information, visit [remove uploads page].*

It is entirely possible that casual users will not fully comprehend what is happening when they opt in to have Facebook 'find friends'. Further, there is no indication that by default, imported contact details are shared with *Everyone* and are therefore visible to anyone on the Internet.

While it is important that Facebook promises not to retain a copy of the user's e-mail password, this may be the least of the privacy problems. What concerns us more is that the importing of contacts represents an indirect collection by Facebook of personal information without the authorisation (or even knowledge) of the individuals concerned. Furthermore, the "disclosure" quoted above leaves the door open for Facebook to use imported contacts for other purposes unspecified.

Imported contacts are vaguely described in the Privacy Policy as "Friend information" or even more ambiguously as "relationships". In any case, the Privacy Policy says very little about this information; in particular, Facebook imposes no limitations on itself as to how it may make use of imported contacts.

On the all-important Privacy Settings page, imported contacts appear to be described as "relationships" and are lumped together with "family". The recommended and default setting is that this information is shared with *Everyone*.

## **A fundamental clash with the Collection Principle**

Whether you apply the current National Privacy Principles (NPPs), the draft Australian Privacy Principles, or some other standard, the most basic information privacy principle is the Collection Principle. This requires that an organisation refrain from collecting personal information unless (a) there is a clear need to

collect that information, (b) the collection is done by fair means, and (c) the individual concerned is made aware of the collection and the reasons for it.

In accordance with the Collection Principle and others besides, a conventional privacy notice and/or Privacy Policy must give a full account of what personal information an organisation collects (including that which it creates internally) and for what purposes. And herein lies a fundamental challenge for most online social networks.

The main mission of Facebook and its ilk is to exploit personal information, in many and varied ways. From the outset, Facebook founder Mark Zuckerberg appears to have been enthusiastic for information built up in his system to be used by others. In 2004, he told a colleague "if you ever need info about anyone at Harvard, just ask".<sup>iv</sup> Since then, Facebook has experienced a string of privacy controversies, including Beacon in 2007 which automatically imported and posted members' activities on external web sites. Facebook's missteps are characterised by the company using the information it collects in unforseen and undisclosed ways.

Yet this is surely what Facebook's investors expect the company to be doing: exploiting personal information in new and innovative ways. The company's gargantuan market valuation<sup>v</sup> speaks of a widespread faith in the business community that Facebook will eventually generate huge revenues. Only a proportion of this can come from advertising on the site. It is worth remembering that Facebook is a pure play information company: its major asset is the information it holds about its members. There is a market expectation that this asset will be "monetised" and anything that impedes the network's flux in personal information – such as the restraints that come from privacy protection – must affect the company's futures.

It's best to remember that Facebook's business model depends on the promiscuity of its members, so there is an apparent conflict of interest in their privacy posture. The more information its members are willing to divulge, the greater is Facebook's power. Facebook and its founder Mark Zuckerberg are far from passive bystanders in this; we argue that they're actively training their constituents to abandon privacy norms, in order to generate ever more information flux upon which the site depends.

Zuckerberg is quick to judge what he sees as broader societal shifts. He told an interviewer in January 2010:

*"[In] the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time. We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are".<sup>vi</sup>*

We believe it is too early draw this sort of sweeping generalisation from the behaviours of a specially self-selected cohort of socially hyper active users. Online social networking is a unique sort of activity, and has not yet been subjected to much serious study by social scientists. Without underestimating

the empirical importance of Facebook to hundreds of millions of people, we nevertheless suggest that one of the over-riding characteristics of the online social networking pastime is simply fun. There is a sort of suspension of disbelief when people act in this digital world, divorced from normal social cues. And as we've seen, Facebook users are not fully briefed on the consequences of their actions, and so their behaviour to some extent is being *directed* by the site designers; it has not evolved naturally as Zuckerberg would have us believe.

## **Compliance with privacy principles**

As noted above, the Collection Principle requires that an organisation refrain from collecting personal information unless (a) there is a clear need to collect that information, (b) the collection is done by fair means, and (c) the individual concerned is made aware of the collection and the reasons for it.

NPP 1.1 says that an organisation can only collect personal information if it is "necessary for one or more of its functions or activities". We argue that until Facebook's mode of operations and business model has been settled and clarified, it is difficult to see how Facebook's collection of some information, like a user's existing address book, is justified as "necessary", with reference to a clear purpose. This is especially true of information which is collected by default, rather than at the active instigation of users who might wish to actually use the feature on offer.

NPP 1.2 says personal information can only be collected "by lawful and fair means and not in an unreasonably intrusive way". Furthermore, NPP 1.4 requires an organisation to only collect personal information directly from an individual "if it is reasonable and practicable to do so". We suggest that practices such as importing contact details of non-users presents an example of collection practices which are unfair and intrusive, and thus likely in breach of NPP 1.2. Furthermore, we would argue that allowing for this indirect collection without an individual's authorisation is likely in breach of NPP 1.4.

NPP 1.3 obliges organisations to notify individuals about "(c) the purposes for which the information is collected; and (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind". That notification must be given "(a)t or before the time (or, if that is not practicable, as soon as practicable after)" the collection of the information. However the explanation of Facebook's Privacy Settings is only available to users after they have registered for an account. We argue there is no "practicable" reason why Facebook could not offer greater clarity and transparency about their use and disclosure of personal information before the new user registers, and therefore they are likely in breach of NPP 1.3.

We then turn to Facebook's use and, more controversially, its disclosure of users' personal information. As Kell and Ng pointed out, the only exemption on which Facebook could rely in order to justify its many and varied disclosures of users' personal information (whether to other users, third parties such as

application developers or Facebook's advertising business partners, or to the world at large via the internet), is a user's "consent".

However we do not believe that Facebook can so easily infer consent simply on the basis that a user "agrees with" a privacy policy at the time they first register for an account. We see three problems with the 'users have consented' argument.

First, there are inherent problems with a bundled consent model. Kell and Ng themselves noted a recent case in which a "catch-all" clause could not be relied upon to provide the necessary consent to a disclosure; there are other cases and comments from other Privacy Commissioners suggesting the same problem.<sup>vii</sup> We would suggest that the only evidence of consent to a disclosure is once a user has actively arranged or confirmed some clear privacy settings, prior to a disclosure taking place. (The capacity of some users such as younger teenagers and children to understand what they are agreeing to is a substantial but separate issue.)

Second, Facebook's Privacy Policy, and the default Privacy Settings, have changed multiple times over the past few years, with each change allowing more disclosures.<sup>viii</sup> A user who ticked a box in 2005 saying they "agreed with" Facebook's Privacy Policy is now subject to a vastly different regime. We do not believe that their consent to a later version of the policy can be so easily inferred.

Third, some users' personal information is disclosed without their involvement at all. The collection, use and disclosure of the email addresses of a user's contacts represents the use of personal information of third parties who may not be Facebook users themselves. We do not see how consent can be inferred in these kinds of situations.

We suggest that Facebook's compliance with NPP 2.1(b) is not as evident or straight-forward as our fellow authors had concluded.

## **Conclusion**

We argue that Facebook's current practices pose a risk of non-compliance with NPPs 1.1, 1.2, 1.3, 1.4 and 2.1. Changes to introduce much greater transparency prior to sign-up would assist, as would re-setting the default Privacy Settings to non-disclosure settings. However until the business model for "monetising" Facebook is settled and clarified, we argue that Facebook will continue to face problems complying with the most basic privacy principle of all, which is to not collect personal information in the first place, unless it is necessary.

---

<sup>i</sup> Kell, John and Ng Phillip, "Privacy and Facebook – the trouble with Facebook", *Privacy Law Bulletin*, Vol 6 (10), September 2010, p.89.

---

ii See for example Nussbaum, Bruce, "Facebook's Culture Problem May Be Fatal", *Harvard Business Review*, 24 May 2010;  
[http://blogs.hbr.org/cs/2010/05/facebooks\\_culture\\_problem\\_may.html](http://blogs.hbr.org/cs/2010/05/facebooks_culture_problem_may.html) (access 6 October 2010).

iii An API or "Application Programming Interface" is a programmatic means for software applications to communicate directly with the Facebook server, in order to import or export information, and perform other sophisticated automatic tasks. Facebook as a software platform has led the way in providing and supporting a rich library of APIs, which their business partners use to interact with the system and its members.

iv "CEO confirms 'embarrassing' IMs are his" Business Insider 9/13/2010;  
[http://www.msnbc.msn.com/id/39149294/ns/technology\\_and\\_science-tech\\_and\\_gadgets](http://www.msnbc.msn.com/id/39149294/ns/technology_and_science-tech_and_gadgets)  
(accessed 5 October 2010).

v Valuing Facebook is much complicated by the fact that it is not publicly traded. In March 2010, a new index for private companies was created by SharesPost Inc., which valued Facebook at US\$11.5 billion. See Bloomberg <http://www.businessweek.com/news/2010-03-03/facebook-valued-at-11-5-billion-in-debut-of-sharespost-index.html> (accessed 5 October 2010).

vi TechCrunch, 8 Jan 2010 <http://www.ustream.tv/recorded/3848950> (accessed 5 Oct 2010).

vii See *Own Motion Investigation v Insurance Company* [2010] PrivCmrA 1, May 2010, [www.privacy.gov.au](http://www.privacy.gov.au); and *KJ v Wentworth Area Health Service* [2004] NSWADT 84; *JK v Department of Transport Infrastructure Development* [2009] NSWADT 307; Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004.

viii See for example the graphical representation of the changes to the default privacy settings from 2005 to 2010 at Matt McKeon's "The Evolution of Privacy on Facebook"; <http://mattmckeon.com/facebook-privacy/> (accessed 6 October 2010).