From IEEE Technology and Society Magazine, V31.2, 2012

Privacy compliance problems for Facebook

Anna Johnston & Stephen Wilson

Abstract

Facebook is an Internet and societal phenomenon. In just a few years it has claimed a significant proportion of the world's population as regular users, becoming by far the most dominant Online Social Network (OSN). With its success has come a good deal of controversy, especially over privacy. Does Facebook and its kin herald a true shift in privacy values, or despite occasional reckless revelations, are most users actually as reserved as ever? We argue it's too early to draw conclusions about society as a whole from the OSN experience to date, However, Facebook in particular brings a number of compliance risks in jurisdictions that have enacted modern Information Privacy Law.

Over 70 jurisdictions worldwide now have enacted data privacy laws[1] around half of which are based on privacy principles articulated by the Organisation for Economic Cooperation and Development (OECD). Amongst these are the *Collection Limitation Principle* which requires data custodians to not gather more personal information than they need for the tasks at hand, and the *Use Limitation Principle* which dictates that personal information collected for one purpose not be arbitrarily used for others without consent.

In many jurisdictions, Facebook may not be complying with local data privacy laws. This article examines a number of areas of privacy compliance risk for Facebook. We focus on several ways in which Facebook collects personal information indirectly, through the import of members' email address books for 'finding friends', and the tagging of friends as being in one's company when using the 'places' feature. The ease of registration as a new member, combined with a lack of transparency about collection practices and permissive default privacy settings, lead to many opportunities for misadventure. Taking the National Privacy Principles from the *Privacy Act 1988* (Cth) as our guide, we identify a number of potential breaches of privacy law, arising in part because Facebook administrators appear not to avail themselves of alternative means for managing personal information.

OECD Privacy Principles and Australian law

The Organisation for Economic Cooperation and Development (OECD) has articulated eight privacy principles for helping to protect personal information.[2] These principles have been enacted in over 30 countries. The principles are listed as follows:

1. *Collection Limitation Principle*
2. *Data Quality Principle*
3. *Purpose Specification Principle*
4. *Use Limitation Principle*
5. *Security Safeguards Principle*
6. *Openness Principle*
7. *Individual Participation Principle*
8. *Accountability Principle*

Of most interest to us here are principles 1 and 4:

> **1. Collection Limitation Principle**: *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*
>
> **4. Use Limitation Principle**: *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification] except with the consent of the data subject, or by the authority of law.*

Australia's *Privacy Act 1988* regulates private sector organisations carrying on business in Australia. The Act sets out ten National Privacy Principles (NPPs), which govern the way 'personal information' must be collected, stored, made accessible, used, disclosed and disposed of. We will use Australia's NPPs as our terms of reference for analysing some of Facebook's systemic privacy issues. In Australia, Personal Information is defined 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.*

The ease of registration

Registering for Facebook is very easy—arguably 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, email address, a 'new' password,

their sex and birthdate. The password entry is very unusual, as you are asked to enter your password only once; it is universal practice for registration forms to capture the password twice, to help avoid 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 email 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 website technique to distinguish a robot's attempt to sign up from a human's. 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[3] and the Privacy Policy[4] are dense documents, running to approximately 3,900 words and 5,800 words respectively. Crucially, the Privacy Policy provides only a partial account of the all-important Privacy Settings feature. Given the furore over Facebook's default settings, and allegations that it tends to serve the interests of the company and not the user,[5] it is surprising that the Privacy Policy is not more accessible in this area. In particular, the Settings feature is not available to users during registration, but can be reviewed only 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' (that is, imported contacts), matters discussed below.

After signing up, the new user is directed to a three-step process to set up their Facebook profile. On the face of it, these steps offer a handy way to populate one's profile and quickly establish a social network, which is after all what attracts 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 email account via an automated API.[i] The primary purpose mentioned on the Facebook site is to facilitate introductions. That is, Facebook looks through the new user's contacts for email 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 email 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 email account. It's the very first thing that a new user is invited to do when 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 email 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,

[i] 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.

there is no indication that, by default, imported contact details are shared with e*veryone*.

While it is important that Facebook promises not to retain a copy of the user's email 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, unspecified purposes.

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 be to described as 'relationships' and are lumped together with 'family'. The recommended and default setting is that this information is shared with *everyone*.

Privacy harms are possible in social networking if members blur the distinction between work and private lives. Recent research has pointed to the risky use of Facebook by young doctors,[6] involving inappropriate discussion of patients. Even if doctors are discreet in their online chat, we are concerned that they may run foul of the Find Friends feature exposing their relation to patients. Doctors on Facebook who happen to have patients in their webmail address books can have associations between individuals and their doctors become public. For doctors working in mental health, sexual health, family planning, substance abuse and so on, naming their patients could have significantly harmful consequences for those patients.

Usually, healthcare professionals will use a specific workplace email account, yet some don't have that option. Many allied health professionals, counsellors, specialists and the like run their sole practices as small businesses, and naturally some will use low cost or free webmail to communicate with patients. Note that the substance of a doctor's communications with their patients over webmail is not at issue here. The problem of exposing associations between patients and doctors arises simply from the presence of a name in an address book, even if the email was only ever used for non clinical purposes such as appointments or marketing.

Location-based social networking

'Places' is a feature introduced by Facebook to compete with specialist social media newcomers, Gowalla (http://gowalla.com) and Foursquare (http://foursquare.com). The basic idea is that individuals' social networking is augmented by linking their actual location in real time to their profile. This allows friends or interesting potential contacts to locate one another and potentially meet face-to-face. Other uses for location are rapidly emerging. It enhances the way social media users can comment on bars, restaurants, clubs, tourist attractions and the like; it also connects users to greater location- and behaviour-based advertising, such as special deals at nearby stores, or loyalty discounts in return for having 'checked in' multiple times at a given premises. Businesses stand to benefit from location based social networking by free promotion every time a customer broadcasts to the network they have checked in there, as well as the 'buzz' generated by having networking sub-groups emerge around them. Businesses may garner more information about their customers and prospects, either directly (by being Facebook members themselves) or indirectly.

As with Facebook's collection of personal information in general, it is far from clear how Facebook will use location data, let alone how it might disclose it to others. The Facebook Privacy Policy, in fact, does not expressly mention the Places feature at all, instead it cursorily refers to places and location in a generic sense and at only a few points. The Policy declares that in addition to 'general information' (which includes your name, your friends' names, profile pictures, gender, connections, and 'user IDs'), Facebook 'may also make information about the location of your computer or access device and your age available to applications and websites'.

Location-related personal information is disclosed by Facebook in many ways. One side-effect of using Places is that most users will be led to enable location services on their mobile device, which inevitably adds to the volume and detail of personal information that is disclosed by Facebook *as a matter of course*, as declared in their policy. There is also significant indirect collection of the location data of others through 'tagging'. When a user checks in to a location, Facebook invites them to tag friends who are claimed to be in the user's company. After tagging, the named individual is

automatically alerted (as are many other people in the network), and they have the opportunity to remove the tag. Users are also able to disable all tagging in their privacy settings, but it is enabled by default.

In our view, disclosing a person's location without their permission, even when they have a chance to retract the tag, represents a potentially serious privacy invasion. Some locations (such as doctors' surgeries and certain entertainment venues) have sensitive connotations that an individual may well desire to keep secret. It is also worth noting that even if a tag is erroneous, it may still represent an important technical breach, because under Australian law, the definition of 'personal information' includes information or an opinion *whether true or not.*

A fundamental clash with the Collection Principle

In Australian privacy law as with the OECD privacy framework, the first privacy principle, NPP 1, concerns *Collection*. NPP 1 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".[7] Since then, Facebook has experienced a string of privacy controversies, including Beacon in 2007, which automatically imported and posted members' activities on external websites. With the introduction of 'places' in 2010, Facebook is inviting further opposition, by making user-location data routinely available to others, including Facebook business partners, and allowing users to 'tag' the location of others without their consent.

Facebook's privacy missteps are characterised by the company using the information it collects in an unforseen and barely disclosed manner. 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[ii] 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'. 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 is also 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 five or six 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."*[8]

We believe that it is too early to draw this sort of sweeping generalisation from the behaviours of a specially self-selected cohort of socially hyperactive 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

[ii] 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. Since then, valuations as high as US$50 billion have been cited, but also disputed.

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 or their geographical location, is justified as 'necessary', with reference to a clear purpose. This is especially true of information that 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 be collected only '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 are examples of collection practices that are unfair and intrusive, and thus likely in breach of NPP 1.2. Furthermore, we argue that allowing for this indirect collection without an individual's authorisation is probably in breach of NPP 1.4.

We also suggest that practices such as 'tagging', which allows User A to provide location data on User B to Facebook (and the broader network community) without User B's consent, present an example of collection practices that are unfair and intrusive, and thus likely in breach of NPP 1.2. Furthermore, because it is reasonable and practicable for Facebook to collect User B's location directly from User B (should they actually want their location broadcast to others), we would argue that 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 'at or before (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 available to users only after they have registered for an account. We argue that 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 it is likely in breach of NPP 1.3.

We then turn to Facebook's use and, more controversially, its disclosure, of users' personal information. 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. A number of cases have suggested that a 'catch-all' clause cannot be replied upon to provide the necessary consent to a disclosure; there are other cases and comments from Privacy Commissioners suggesting the same problem.[9,10,11,12] 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.[13] 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 by third parties who may not be Facebook users themselves. The geographical 'tagging' feature can lead to the disclosure of a user's location before they realise it and have the chance to remove the tag. We do not see how consent can be inferred in these kinds of situations.

Conclusion

We argue that Facebook's current practices pose a risk of non-compliance with NPPs 1.1, 1.2, 1.3 and 1.4. Changes to introduce much greater transparency prior to sign-up would assist, as would re-thinking features such as Places, and resetting the default Privacy Settings to non-disclosure. 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.

About the authors

Anna Johnston is a director of Salinger Privacy, Sydney, Australia, and Stephen Wilson is principal of Lockstep Consulting, Sydney, Australia.

Acknowledgement

An earlier version of this article was originally published by LexisNexis in the *Privacy Law Bulletin* (2010) 7(2) Priv LB.

[1] G. Greenleaf, "76 global data privacy laws," Privacy Laws & Business, Sept. 2011.

[2] B. Gerber, OECD Privacy Principles, 2009, 2010; http://oecdprivacy.org.

[3] Facebook, Statement of Rights and Responsibilities, Oct. 4, 2011; http://www.facebook.com/#!/terms.php, accessed Jan. 15, 2012.

[4] Facebook, Data Use Policy, Dec. 22, 2010; http://www.facebook.com/#!/policy.php, accessed Jan. 15, 2012.

[5] B. Nussbaum, "Facebook's culture problem may be fatal," Harvard Bus. Rev., vol. 24, May 2010; http://blogs.hbr.org/cs/2010/05/facebooks_culture_problem_may.html, accessed Oct. 6, 2010.

[6] G. Moubarak et al., "Facebook activity of residents and fellows and its impact on the doctor–patient relationship," J. Med Ethics, vol. 15, Dec. 2010.

[7] "CEO confirms embarrassing IMs are his" Business Insider, Sept. 13, 2010; http://www.msnbc.msn.com/id/39149294/ns/technology_and_science-tech_and_gadgets, accessed Oct. 5, 2010.

[8] TechCrunch, 8 Jan 2010; http://www.ustream.tv/recorded/3848950 (accessed 5 October 2010).

[9] *Own Motion Investigation v Insurance Company*, 2010, PrivCmrA 1, May 2010, www.privacy.gov.au.

[10] *KJ v Wentworth Area Health Service*, 2004, NSWADT 84.

[11] *JK v Department of Transport Infrastructure Development*, 2009, NSWADT 307.

[12] Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004.

[13] M. McKeon, "The evolution of privacy on Facebook;" http://mattmckeon.com/facebookprivacy, accessed Oct. 6, 2010.