Chapter 3. Facebook and the Commercialisation of Personal Information: Some Questions of Provider-to-User Privacy

Jennifer Hendry* & Kay Goodall‡
*School of Law, University of Leeds; ‡School of Law, University of Stirling

Abstract

Most of the debate about online social networking sites, such as Facebook, has thus far revolved around questions of privacy and access to personal information. Users of such services, should they choose to exercise them, have a myriad of privacy options that allow them to restrict access to their own personal information posted online, and the privacy policies of such sites are abundantly clear that the making of such choices is the responsibility of the users themselves. However, due to the focus resting upon these peer-to-peer privacy questions, those relating to the service provider-to-user relationship have been overlooked. This paper seeks to highlight some of the more subtle privacy issues of (what we will call) the 'Facebook debate' in terms of two main considerations: the access to and the control of personal information on the part of the provider.

3.1. Introduction[1]

Online social networking sites have been around since the mid-to-late 1990s,[2] but only in the past few years has the 'craze' really entered the mainstream[3] in the shape of MySpace, Friendster, Bebo, Hi5 and, particularly, Facebook.[4] Some sites have a specific intended purpose, such as dating or job searches, but all of them have online communication and social interaction as their basic aim, and most share certain core features: users create a 'profile', which takes the form of a template that can be completed with personal information, including photographs, videos, preferences and opinions, and this profile can be perused or linked to by other users on the network, be they friends, former classmates, colleagues, or even perfect strangers. The personal information on a user's profile is all voluntarily 'uploaded', usually in terms of category-based representations of general interests, such as a person's musical or sporting preferences, but also personal details such as sexual orientation, religious and political views, and personal data like birthdates, phone numbers and addresses.

Due to the personal nature of this information, concerns have been raised regarding privacy, and many of the online social networking (OSN) sites listed above provide privacy controls so that users can choose both who can see their profile[5] and how much any category of 'friend' can access within that profile. However, although these privacy controls are useful in terms of restricting the access to a personal profile by other users of the social network sites (i.e. peer-to-peer access), there are few, if any, restrictions upon the service provider, namely the sites themselves, regarding the private information of the service users. Much of the literature on this topic revolves around questions of peer-to-peer privacy and attempts to understand certain behavioural forms of information revelation, and it is not our intention here to enter into either of those debates. Rather, our focus is on the frequently overlooked issue of the service provider-to-user relationship, and the privacy questions arising from it. Instead of being purely about access to

---

[1] This paper was presented at the *Perspectives on Regulating Technologies* conference, hosted by the Tilburg Institute for Law, Technology & Society, University of Tilburg, Netherlands, in December 2008.An earlier version of this paper was presented at the BILETA Annual Conference on 'Law Shaping Technology, Technology Shaping the Law', held at Glasgow's Caledonian University in March 2008. Our thanks go to Elaine Sutherland, Fraser Davidson, Rosa Greaves, Alison Green, Richard Jones, Elizabeth Crawford and Janeen Carruthers for their suggestions and comments. Any errors, of course, remain our own.

[2] Early examples include Classmates.com, which started in 1995 and focused on connecting former school friends, and SixDegrees.com, which started in 1997 but closed in 2000 after 'struggling to find a purpose for its concept' of forming indirect ties. See Janelle Brown, 'Six degrees to nowhere', 21 September 1998, http://archive.salon.com/21st/reviews/1998/09/21review.html.

[3] Nicole Martin, 'Debrett's guide to online etiquette', *Telegraph*, 13 June 2008, http://www.telegraph.co.uk/digitallife/main.jhtml?xml=/connected/2008/06/12/dldebretts.xml.

[4] See http://www.myspace.com; http://www.friendster.com; http://www.bebo.com; http://www.Hi5.com; http://www.facebook.com.

[5] Such as the 'request' and 'confirm' functions – a user wishing to be 'friends' with another user, i.e. wishing to be granted access to that individual's profile, must first request it and wait for confirmation. The recipient must either confirm or ignore this request, with access only being granted in the event of the former. Obviously this system depends upon the personal privacy settings of each user – requesting access is only an issue if it has been previously restricted in some way.

personal information, therefore, we look at the subsequent use and control of the information posted on a social networking site such as Facebook[6] by the site provider itself.

3.2. Access and Control

The two issues of access and control are closely interrelated, especially in today's digital age, when duplicates are often a simple mouse-click away and dissemination of these is equally straightforward. The Internet, more than any other medium, provides a means of putting information directly into the public domain: instead of students and young people setting up pirate radio stations and crying 'reclaim the airwaves' in an attempt to be heard, the current youth generation are able, like no other before them, to disseminate information by means of social networking sites, blogs, and personal homepages. However, once information has been posted online and thus made public, it then becomes difficult for the owner or poster to control – a situation that has resulted in such Internet phenomena as the Star Wars Kid[7] and the 'Numa Numa' Dance's Gary Brolsma,[8] neither of whom were particularly happy about their unexpected infamy.

Although such phenomena are rare, and neither of the abovementioned examples had any privacy restrictions on these videos, it is evidently important to consider how and to what extent information being posted can be controlled by the owner and/or poster, and that questions relating to controlling the dissemination of information will inevitably involve considerations of access to that information. This intertwining of access and control means that concerns quickly shift from being purely about privacy to also being about (i) property, specifically intellectual property, and (ii) exploitation of private information, personal preferences and online activities by, for example, highly-targeted advertising.[9] This paper will, firstly, look at both of these examples of commoditisation of essentially private user-content and information, then outline some of the legal problems that exist as a result of the broad licence signed by each user on joining Facebook, before finally suggesting some possible solutions.

3.3. User Content and Intellectual Property

What does the Facebook privacy policy and its terms and conditions have to do with considerations of intellectual property? Before attempting to answer this question, it is necessary, first of all, to establish what an intellectual property right means, and in what relevant situations such a right will arise.

An intellectual property right can be defined as a right: (i) that can be treated as property; (ii) to control particular uses; (iii) of a specific type of intangible asset; and are normally characterised by (i) only being granted when the intangible asset can be attributed to an individual creator or group of creators, and (ii) being enforceable by both the civil and criminal law.[10] The legal right created gives the owner of the intellectual property 'an open-ended set of use-privileges, control powers and powers of transmission'.[11] It is this notion of control of the asset that is so important in the instance of online posting, mainly due to the fact that a Facebook user *relinquishes control* of information and 'content' posted on their profile or on the site in general (i.e. on the profile pages of others, on group pages, and on various applications[12]). The next

---

[6] There are differences across the various sites and so, for the sake of clarity, this chapter will take the Facebook site as its main focus.

[7] The Star Wars Kid, otherwise known as Ghyslain Raza, earned his moniker when a 2002 video he had filmed of himself swinging a golf club around his head as if it were a lightsabre(in the style of Darth Maul from the Star Wars movie) was 'shared' by a friend of his on the Kazaa peer-to-peer network. It was then adapted to include music and sound effects and, as of November 27, 2006, it was estimated to have been viewed 900 million times, making it the most popular viral video on the Internet. See http://news.bbc.co.uk/1/hi/entertainment/6187554.stm.

[8] In 2004, Brolsma filmed himself on a webcam although dancing exuberantly to the pop song 'Dragostea din tei' as performed by Moldovan pop band O-Zone. With 700 million views, it comes second only to the Star Wars Kid (above). See reference ibid.

[9] This distinction follows that discussed by Corien Prins, who suggests that the two are conceptually separate: "At first sight, privacy and property seem mutually exclusive concepts. [...] Some, however, argue that privacy protection on the one hand and personal data protection on the other have evolved into two highly distinct concepts..." See C. Prins, "When Personal Data, Behaviour & Virtual Identities Become A Commodity: Would A Property Rights Approach Matter?" in *SCRIPT-ed* (June 2006) 3(4) 270-303 at 275

[10] M. Spence, (2007) *Intellectual Property*, Clarendon, OUP: Oxford, 12-13.

[11] Ibid, 15.

[12] The term 'application' applies to additional, normally (third-party) user-created, programmes that run off the site platform. At the time of writing, there were over 500,000 applications available on the Facebook website, ranging from ones that allow

section will explore in detail what can probably be referred to as the most commonly experienced and widely recognised issue relating to controlling personal information posted online – specifically, photographs.[13]

3.4. Facebook Photos: Why All the Fuss?[14]

A friend of ours is camera-shy, and constantly protests that he does not want any pictures of himself 'posted' online,[15] no matter they are only accessible by friends and friends of friends. Justifications for posting photos tend to follow along the lines of 'relax, it's only friends who can see it', or 'it's a group picture, I can't take you out of it', and even 'well, I won't tag you and then it won't show up on your profile page, only on mine'.[16] Our dissatisfied and increasingly disgruntled friend points out that he is not a Facebook user and thus is not aware of pictures of him being posted, let alone which ones and by whom, and also that it matters little whether they are on one person's profile page or another – they are available and accessible online either way. That he has never given any permission for either his name or image to be used is a source of frustration for him, as he feels that he has no control of either. Imagine his horror, then, if he were to read the 'Statement of Rights and Responsibilities' that his friends are agreeing to when they post pictures on the Facebook site. According to these, by posting their 'Content' to any part of the site, users effectively grant to Facebook:

> a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License").[17]

'Use' is far from the mere hosting that the uninformed reader might foresee. Only near the very end of the Statement might the reader discover that it means 'use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of' and as we will see it would be an unusually unsociable user if all their content was kept so close to their chest that Facebook alone would have the right of 'use'. In response to complaints in an earlier version of these terms which stated that the licence was 'perpetual' and 'irrevocable'[18], Facebook adds that the 'IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.' This sounds comforting if the reader is unaware that the default option they will be given, of 'deactivating' their account, is not the same as deleting it. The reader is likely also to be unaware that 'sharing with others' does not refer only to the information they thought they had made publicly available – of which again, more later.

Furthermore, Facebook's previous Terms of Use stated that:

> [Facebook reserves] the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice. If we do this, we will post the changes to these Terms of Use on this page and will indicate at the top of this page the date these terms were last revised. Your continued use of the Service or the Site after any such changes constitutes your acceptance of the new Terms of Use.

This last part was particularly interesting given the US decision in *Douglas* v *US District Court*[19] that a service provider cannot change the terms of its service contract merely by posting a revised contract on its

---

users to add music, videos, literary and popular culture preferences to their profiles, to ones that pinpoint a user's geographical location, allow filesharing or promote certain causes. The specific privacy implications of 'adding' an application to your profile are also not straightforward – a user must deliberately re-set their privacy options, as the default setting is to 'public' access.

[13] Groups existing within the Facebook network, such as 'My photos are MINE! NOT Facebook's! Change the Terms and conditions!' and 'Facebook: Do not sell my private pictures! Change your terms of use, NOW!' show that users are well aware of the implications of the Terms & Conditions. See: http://www.facebook.com/group.php?gid=5606823556 and http://www.facebook.com/group.php?gid=5841663547.

[14] Photographs are by far the clearest example, which is why it has been selected here. However, text-based content such as poems, short stories, academic work – in short, anything 'post-able' to which copyright could apply – would also come under this ambit.

[15] 'Posted online' means uploaded to the internet.

[16] To 'tag' someone is to put their name on their image in a photograph, which has the effect of creating a direct link between the photograph and that person's profile page, assuming that they are a user of the site.

[17] Facebook's Statement of Rights and Responsibilities, version last revised 21 December 2009.

[18] Facebook's previous Terms of Use, accessed June 7, 2008.

[19] *Douglas* v *US District Court*, 495 F.3d. 1062 (9th Cir. 2007). Following appeal to the US Supreme Court, certiorari was denied: *Talk America, Inc.* v *Douglas*, 128 S.Ct. 1472 (2008).

website. It may be that *Douglas* can be distinguished on the grounds that the core activity of Facebook users involves accessing the website; however, the Court of Appeals did observe that '[p]arties to a contract have no obligation to check the terms on a periodic basis to learn whether they have been changed by the other side.'[20] Furthermore, Lemley has argued that US courts have tended not to enforce similarly restrictive 'browse-wrap' licences (in software marketing) against the consumer unless that consumer is a 'sophisticated economic entity'.[21]

The new version seems not much better for the user, though:

> We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and become a fan.
> [but it bafflingly adds:]
> We can make changes for legal or administrative reasons upon notice without opportunity to comment.

Douglas aside, though, the implication of the Statement is that user Content, be it photographs, pictures, written notes, stories or any other personal information, is available to Facebook or its application developers to use in any way they choose, even for commercial purposes. As we will show, exercising a supposed privacy option does not fully protect against this. To put this in the strongest light, there is the very real (albeit unlikely) possibility that our camera-shy friend could be walking down the high street one day and discover his own face staring back at him from an advertising billboard.[22] His first post-tantrum reaction would certainly be to confront the friend whose photograph it was, but to no avail – under this Statement, Facebook does not even have to ask the user's permission before making use of any posted Content which has not specifically been protected by means of the user manually overriding the publicity default. Indeed, the above-quoted licence is so comprehensive that it effectively undermines the following assertion in the Statement, which provides that:

> You own all of the content and information you post on Facebook, and you can control how it is shared ...[23]

This provision regarding ownership is, in essence, almost entirely worthless due to the scope of the licence – although the user may own all of the Content they post on the site, Facebook does not, in fact, need to own the information because they are licensed to utilise it in whichever way they choose, regardless of ownership. It is like borrowing your parents' car – at no point do you ever claim to own it, but that does not really matter when you are driving around town.

There are two separate issues relating to both privacy and property that should be considered here. These are probably best distinguished in terms of active and passive posting; the former being when a user posts a picture that they (alone) own, the latter being when a picture is posted that shows another person or group of people, to which the user does not have exclusive rights. In the Intellectual Property help section, a Facebook user is told that they 'may only upload content to the Facebook website if you are certain that you have the legal right to do so. If you are not certain that you are legally authorized to use the content you have uploaded to our website, you should remove it immediately.'.[24]

This gives rise to considerations of copyright, for who owns and has the right to distribute photos? Is it the photographer? The subject or subjects? What about the artist, designer, or employer? All of the above? The answer is not especially straightforward, even leaving jurisdictional concerns aside for the moment.[25]

---

[20] *Douglas* v *US District court,* ibid., 1066.

[21] Mark A. Lemley 'Terms of Use' 91 *Minnesota Law Review* (2006-2007), 460, 462-463. See also Dale Clapperton and Stephen Corones 'Unfair terms in 'clickwrap' and other electronic contracts' 35 *Australian Business Law Review* (2007), 152 and Clapperton's blog at http://defendingscoundrels.com/2007/10/dissecting-the-facebook-terms.html.

[22] This may sound farfetched, but cases such as that of Alison Chang, a 15-year-old who saw a photo of herself, initially posted on Flickr, on an Australian Virgin Mobile advertisement, suggest that 'corporate photonapping' is a very real danger. See Monica Hesse 'Hey, Isn't That…' (9 January 2008) *Washington Post* and also: http://www.theregister.co.uk/2007/09/24/creative_commons_deception/.

[23] Statement of Rights and Responsibilities, supra note 17.

[24] http://www.facebook.com/album.php?aid=14347&id=635057322&saved#!/help/?page=439

[25] A notoriously complex area of law, the international copyright system can nonetheless be said to have three main rules of thumb: (i) the law of the country of origin of the work is likely to be relevant when determining ownership of copyright or

In the UK and in terms of photographs[26] taken after 1 August 1989, generally the 'author' of a photograph is the first owner of copyright,[27] meaning that you are the owner of the copyright of any photos you take. However, this may not be the case if someone else decided on the specifics of the photograph, such as the exposure or angle, for example, or even if the people either taking or designing the photo were simply employed to do so – in this situation the employer would be the first owner. If there happens to be more than one person involved in taking, making and designing the photo, and those contributions are indistinct, then each person will be both a joint author and thus a joint owner of copyright, meaning that any usage must be unanimously agreed to.[28] This is complicated all the more by provisions on 'fair dealing',[29] which allow photographs to be used without permission providing that they are being used for specific purposes, including: non-commercial research and private study,[30] criticism and review, and where there is sufficient acknowledgement.
These copyright concerns appear to be moot, however, considering that the approach taken by Facebook here is one that, first of all and as noted above, never makes any claim to having ownership and thus any restricted rights over the photograph but rather relies upon the licence granted by the user and, secondly, rests all responsibility of actually ascertaining copyright ownership with the user.[31] The user is told on the Intellectual Property page:

> '[j]ust because you have recorded content onto your own recording device, this does not necessarily mean that you own the copyright to that material or that you are authorized to use it. Disclaiming ownership of that content cannot protect you from infringing on the true owner's copyright. If you have any question whatsoever as to whether you are legally authorized to post any content, consult an attorney before uploading it to the Facebook website'.

A later question-and-answer states:

> 'How does Facebook prevent users from uploading material that is copyright infringing?
> The material uploaded to the Facebook website is uploaded by our users. Our Terms of Use prohibit users from posting content that violates another party's intellectual property rights. We encourage our users to report instances of copyright infringement using the procedures outlined in our How to Report Claims of Intellectual Property Infringement page, and we terminate the accounts of repeat infringers in appropriate circumstances.'

By requiring the user to accept their right to post the photograph in advance of doing so, Facebook thus effectively side-step any potential liability for copyright violations, although, as third party rights in copyright are not affected by the Statement, if the user is not the copyright owner then their implicit licensing of Facebook would mean little were the *true* copyright owner to bring suit.[32] Nevertheless, a peeved 'friend' whose picture has been posted by another user (passive posting) appears to have no direct recourse

---

authorship; (ii) the law where the infringement takes place is likely to be relevant to questions regarding the infringement, and; (iii) which courts will deal with the resolution of any international dispute will be determined with reference to international conventions on jurisdiction. As yet there are no dedicated rules governing cyberspace. See S. Stokes, *Digital Copyright: Law & Practice* (Oxford, Portland: Hart Publishing 2005), 7 and, for more detail, P. Goldstein, *International Copyright: Principles, Law & Practice* (New York: OUP 2007).

[26] The Copyright, Designs & Patents Act (CDPA) 1988, s. 4(2) defines a photograph as 'a recording of light or other radiation on any medium on which an image is produced or from which an image may by any means be produced, and which is not part of a film'.

[27] Copyright, it should be noted here, simply protects against copying and dealing in illegal copies.

[28] Intellectual Property Office, http://www.ipo.gov.uk/copy/c-applies/c-photo/c-photo-ownpost89.htm, accessed 30/01/08.

[29] These 'fair dealing' provisions are a UK exception (Art. 5) from EC Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society of 22 May 2001. The US defence of 'fair use' is much broader in scope, as it is not limited to specific purposes; see s. 107, US Copyright Act 1976.

[30] S. 29, CDPA.

[31] The Facebook Statement further says: 'If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim.'

[32] An important issue in this respect is whether the User in fact has the right to grant that licence – despite the requirement of 'ticking the box' it is evident that many Users simply do this as a matter of course, regardless of whether they have this right or not. If it transpires that the User does not have the authority, then any subsequent use of the material by Facebook may constitute an infringement, with the possibility of the User being secondarily liable for Facebook's infringement.

against Facebook, even if they subsequently have used, copied, publicly displayed or distributed it – the only option for the aggrieved party would be to take up the matter at the source, namely the original infringement. What remains unclear is whether or not 'corporate photonapping' as in the case of Alison Chang[33] would be actionable if the photograph used had been posted on Facebook, although the outcome of this hypothetical situation would surely turn on the extent of Facebook's own involvement in the transaction: if the corporation had unilaterally copied and then used a posted photograph for commercial purposes without the express permission of either Facebook or the copyright owner, then this would appear to be an infringement.

Perhaps the most interesting observation here is that it is the users and the bloggers – 'communit[ies] typically associated with piracy' – who are now 'rallying in support of copyright'.[34] As Lawrence Lessig observes, 'average individuals are increasingly thinking of themselves as artists, whose work has value – or at least deserves respect'[35] and, although we would agree with this assertion, we would also argue that the Facebook debate is still less a commercial than a privacy concern in this respect. Commercial considerations come much more to the fore when the focus shifts from questions of (intellectual) property to those of personal information and private data.

3.5. 'Facebook Ads' – The Conundrum of Targeted Advertising

Targeted advertising is not a new phenomenon and is, indeed, one of the reasons that free-to-use websites such as Facebook, Google and MSN's Hotmail have become so lucrative. Users of Google's web-based Gmail service may have had the rather creepy experience of noticing that the little adverts beside their email seem coincidentally similar to the content of their emails. This is not coincidental: Google actually scans the text of all emails and links it to commercial advertisements, which in turn have text links displayed beside the user's inbox. This process takes place automatically and no data – not even aggregate data on the number of advertisements shown in Gmail – is relayed back to the advertiser.[36]

Facebook takes a similar approach with the imaginatively-named 'Facebook Ads', a facility launched in November 2007,[37] and whose tripartite approach provides businesses with a simply staggering insight into what users and their 'friends' are interested in and are buying.

The sort of personal data provided freely by users is a hugely valuable resource for commercial profiling. Facebook's standard page layout encourages users to upload details of their favourite books, music, hobbies and interests, their political and religious affiliations, their family and relationship status, their employment circumstances, date of birth, address and other contact details, their connections with other Facebook users (who are also profiled in this manner), and much else; the structure of the pages even facilitates this self-categorising by providing a pre-set selection of categories. The value of this pre-categorised data for marketing analysis is obvious, and Facebook allows marketers to access much of it so they can create 'SocialAds'[38] targeted to the individual user.

This situation is made even more intriguing when we consider that one of Facebook's core 'principles' is 'ownership and control of information'.[39] Its introductory 'guide to privacy on Facebook' announces that 'You should have control over what you share. … Your privacy settings should be simple and easy to understand.'[40] Its Privacy Policy begins by avowing that 'We want to earn your trust by being transparent about Facebook works.[41] The underlying message here is that you, the user, should be able to control who has access to your information, which in turn suggests that you control what will be done with said information. These controls take the form of optional privacy restrictions that each user can set to their own desired levels: for example, a user can opt to have their profile completely visible to all other users (standing somewhere in the region of 300 million worldwide visiting the Site each month[42]), to those who

---

[33] As discussed above, see supra note 22.
[34] Lawrence Lessig, quoted by Monica Hesse, see supra note 22.
[35] Ibid.
[36] http://mail.google.com/mail/help/about_privacy.html.
[37] http://www.facebook.com/press/releases.php?p=9176.
[38] http://www.facebook.com/business/?socialads.
[39] Facebook Principles, accessed 25 February 2010.
[40] http://www.facebook.com/privacy/explanation.php.
[41] Facebook's Privacy Policy, version 9 December 2009.
[42] Eric Eldon, http://www.insidefacebook.com/2009/09/15/facebook-reaches-300-million-monthly-active-users/. Note that by this Facebook means 'monthly uniques', that is, individuals distinguished by unique identifiers such as IP code.

are in the same networks, or to just their 'friends' (although note that even this is not full cloaking[43]), with the further option of hiding certain information from some friends by only granting them access to your 'limited profile'.

However, and this appears to be the crucial point, these privacy controls *only apply to other users and not to Facebook itself*. Any control that the user has only relates to the access they grant (or do not grant) to other users in a peer-to-peer relationship, although the relationship of service provider-to-user stays out of the limelight. The conscious frame is the individual 'other'. Indeed, when Facebook rolled out its Social Ads, what it was telling its potential advertisers reads rather differently from what it was telling its users – for example:

> With Facebook Insights, you have access to data on activity, fan demographics, ad performance, and trends. With this information, you are better equipped to improve your custom content on Facebook and adjust your ad targeting. (...) Facebook's robust database of authentic demographic information provides you with a deep understanding of exactly who is engaging with your business and how. (...) Facebook Insights helps you learn more about your target audience.[44]

Much more disturbing from a privacy perspective, however, are the third-party applications that are given access to user data through the Facebook platform. A host of quirky and humorous applications are available to Facebook users and are part of the charm of socialising on the site. Users can display clips of their favourite films to friends, send imaginary drinks, take part in jokey quizzes, place virtual bets – the options are as wide as the developers' imaginations, and the applications are hugely popular. The default for signing up, however, is that users often give the application access to all their personal data, even if the individual's profile is otherwise set as 'private'. They may not be able to add the application if they refuse. In a 2007 survey of the top 150 applications, researcher Adrienne Felt found that 90.7% were being given more access to information than they needed to provide their service.[45] For a chilling list of what information the user gives away without explicitly being asked, see Facebook's own page giving some insight into the security gaping hole of its Platform 'service'.[46]

It comes as no surprise that in 2008 Facebook announced plans to develop an e-commerce facility to allow financial transactions to take place through the applications.[47] The site now enables apparently trivial financial transactions through a virtual currency called 'Facebook credits' such as the buying of virtual flowers for a nominal sum as 'gifts' for friends. These credits can be bought in the real currency of dollars and can for instance be paid for by being added to a mobile phone bill. Thus there already exists the (code) facility to enable companies with access to target information such as this, to sell easily to users *at the point of* use.[48]

As we mentioned above, the casual reader of the Facebook Statement and guide to privacy may gain the misleading impression that their privacy is secure. The reader must turn to the full privacy policy to uncover the disturbing news that '[t]his privacy policy covers all of Facebook. It does not, however, apply to entities that Facebook does not own or control, such as Facebook-enhanced applications and websites' and it is only on more in-depth perusal of these documents that the reader can discover that Facebook may draw on any information in their user profile for the use of third parties; that Facebook may also use user information that it has gleaned from other sources, such as newspapers, blogs or instant messaging programs; and that Facebook may share the user's 'customer information' with other companies in connection with the user's use of a store or service that the company also happens to provide on Facebook. The Privacy Policy maintains that 'sensitive' information is encrypted; however, by this it means data such as credit card details, and not date of birth, sexual orientation or religious beliefs, which,

---

[43] Facebook's Privacy Policy, note 41 above: 'Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, and networks you belong to are considered publicly available, and therefore do not have privacy settings.'

[44] See cached page at: http://web.archive.org/web/20080213223005/http://www.facebook.com/business/?insights, stored on 13 February 2008.

[45] http://www.cs.virginia.edu/felt/privacy/.

[46] http://developers.facebook.com/about_platform.php

[47] http://blog.washingtonpost.com/posttech/2008/06/ecommerce_on_facebook.html?nav=rss_blog.

[48] The much-criticised Beacon application, which was applied to some accounts without the users' explicit consent, and which advertised to their Friends what purchases they had made on partner sites such as Amazon, was an obvious precursor of this sort of data-mining and marketing. It is now being discontinued following settlement of a legal action against Facebook: see *Lane et al* v *Facebook, Inc. et al*, Case No. 5:08-CV-03845-RS.

although more mundane, are most certainly deemed 'sensitive' under the UK Data Protection Act 1998 and the European data protection directive (95/46/EC).[49]
Facebook's approach to privacy last year became the subject of a complaint to the Canadian Privacy Commissioner,[50] much of which was upheld.[51] A Canadian legal clinic based at the University of Ottawa argued that Facebook is violating several principles of the Personal Information Protection and Electronic Documents Act. Although not singling out Facebook as the sole miscreant among social networking sites, the clinic chose it for this first complaint because of its popularity.[52] The Canadian Internet Policy and Public Interest Clinic (CIPPIC) focused among other things on the typical defaults in user agreements for downloading third-party applications. CIPPIC also maintained that Facebook 'misrepresents itself as solely a social networking site',[53] failing to make it clear to users the purposes for which Facebook allows third-party developers to access personal information.

The report from the Canadian Office of the Privacy Commissioner[54] made many criticisms of Facebook's policies, but one criticism is worth quoting in full:

> 'Another consent-related concern that I have is the fact that no specific consent is sought from users for the disclosure of their personal information to applications when their friends and fellow network members add applications. Facebook maintains that, through its privacy settings, users have an extensive ability to choose whether or not they will interact with any particular Facebook application and to block any particular application and opt-out of all Facebook applications in a simple way. However true this statement may be in theory, I would note that users' "ability to choose" would depend on their being knowledgeable about developers' practice of accessing and using third-party information when friends add applications. I would also note that the only way users can control the exposure of their personal information to application developers when their friends and fellow network members add applications is either to opt out of all applications altogether or to block specific applications. Moreover, the latter option would effectively require them to guess which of the more than 350,000 applications their friends and fellow network members are likely to add.
>
> I do not consider it appropriate for Facebook to put on users the onus of informing themselves and opting out of the disclosure of their personal information when friends and fellow network members add applications. Nor do I believe that the practice meets the reasonable expectations of users.'[55]

3.6. Cyberspace and Problems of Legal Challenge

In the early days of Facebook the legal reader might have wondered whether there really was an enforceable contract, particularly under English law. What economic exchange was taking place? With the advent of e-commerce on Facebook allied to the dispersal of personal data to third-party developers, the value of the licence of the user's intellectual property rights has become more obvious. Perhaps, then, such legal protections as the Unfair Contract Terms Act 1977, the Unfair Contract Terms Directive,[56] the Data Protection Act 1998 (the 1998 Act) or the data protection directives[57] will come into play at this point. A standard form contract that leads users into a relationship from which it is extremely difficult to extract themselves may be in practice both unreasonable and in breach of the fifth data protection principle on keeping data longer than is necessary[58] – indeed, the UK Information Commissioner investigated just such

[49] See s. 2 and Schedule 3 Data Protection Act 1998; also see the Data Protection (Processing of Sensitive Personal Data) Order 2000, SI 2000/417.
[50] http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.
[51] http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm
[52] http://www.cippic.ca/uploads/NewsRelease_30May08.pdf.
[53] See p. 31 of the complaint, above, note 50. See also pp. 19-20.
[54] Elizabeth Denham, Assistant Privacy Commissioner of Canada, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the *Personal Information Protection and Electronic Documents Act*, 2009.
[55] Paragraphs 308-309, above.
[56] Implemented in the UK by the Unfair Terms in Consumer Contracts Regulations 1999.
[57] See the Data Protection Directive (95/46/EC) and the Directive on privacy and electronic communications (2002/58/EC).
[58] 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.' Part I of Schedule 1, Data Protection Act 1998.

a complaint against Facebook as regards the difficulty (at the time of complaint) of removing personal data from an established account.[59]
One can also question the very need for Facebook to retain in-depth user data for any length of time. Under the second and third data protection principles, personal data can be obtained only for specified purposes and should not exceed what is needed for those purposes.[60] Although the Regulation of Investigatory Powers Act 2000 mandates that communications data be retained, it only requires this of the Internet Service Provider (ISP) and not of a social network provider.[61] In addition, a 'data subject' under the 1998 Act (which would certainly cover a Facebook user)[62] has the right under s. 10 to object to and prevent the processing of information held about them if it is likely to cause them substantial damage or distress. They also have the right under s. 7 to know what data is held on them, which would mean that, if a user leaves Facebook, they would have the right to be informed as to exactly what data remained, even in archives. In a similar vein, and considering that the right to share sensitive data requires explicit and informed consent, the default opt-out system provided by Facebook would fall short of this requirement, especially where subsequent actions by the user can have the effect of overriding the user's prior selection of an overall 'privacy' setting. However, a platform site such as Facebook is able to upload all user data onto servers in the United States, thus bypassing British and EU data protection provisions (although we should emphasise that Facebook itself does in fact have a London office at present and has signed up to both the EU Safe Harbor Privacy Framework and TRUSTe dispute resolution).[63] And although a user may assume that they are governed by the law of their local jurisdiction, including rules regarding parity and fairness in contract, Facebook's Statement requires them to consent to quite another arrangement:

> You will resolve any claim, cause of action or dispute ("claim") you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.

This in practice is a significant improvement on the previous Terms of Use, which bound the User to the laws of Delaware, a much less amenable jurisdiction. However, it nonetheless raises several questions, the foremost of which relates to the very validity of such a licence.[64] In the UK, Regulation 9 of the Unfair Terms in Consumer Contracts Regulations 1999[65] prohibits exclusion by choice of law clause. Regulation 5(1) provides that '[a] contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.' The Regulations cover a wider range of unfair clauses than the Unfair Contract Terms Act 1977 does and although Facebook's service is not typical of those envisaged by the drafters, it is a service with commercial implications and, as we later discuss, Facebook has recently announced plans to develop e-commerce through its third-party applications.[66] Schedule 2 provides a non-exhaustive list of terms which may be regarded as unfair; among

---

[59] http://news.bbc.co.uk/1/hi/technology/7196803.stm. See also 3.7, below.
[60] '2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.' Part I of Schedule 1, Data Protection Act 1998.
[61] Facebook only really need to keep records that meet the standards required to serve the normal purposes of the ordinary criminal law. The licence will be discussed in the next section.
[62] See s. 1(1) of the 1998 Act, which defines a 'data subject' as simply 'an individual who is the subject of personal data'.
[63] The 'Safe Harbour' agreement between the US and the UK was intended to provide a framework for firms in the face of different private sector data protection standards between the two areas. For more on this see, for example, A. Busch, "From Safe Harbour to the Rough Sea? Privacy Disputes Across the Atlantic" in (2006) *SCRIPTed* 3(4)
[64] Compulsory arbitration clauses are always treated as unfair, and exclusive jurisdiction clauses are likely to be treated as unfair, where they are governed by the Unfair Terms in Consumer Contracts Regulations 1999. For discussion of US case law on the question of mandatory arbitration clauses and exclusive choice of law in electronic contracts, see Dale Clapperton and Stephen Corones, 'Unfair terms in 'clickwrap' and other electronic contracts', 35 *Australian Business Law Review* (2007), 152.
[65] SI 1999/2083.
[66] Also consider here the Consumer Protection (Distance Selling) Regulations 2000 and the Electronic Commerce (EC Directive) Regulations 2002.

these at paragraph 1(q) is 'excluding or hindering the consumer's right to take legal action or exercise any other legal remedy'.
The Rome I Regulation[67] came into force across the EU at the end of 2009. If a case is raised in the UK or another member state of the European Union, Rome I applies. Again, there may be a question over whether the user's agreement with Facebook can in fact be regarded as a 'consumer contract' within the scope of the Regulation,[68] but the future of e-commerce makes this matter critical. Article 3 provides that the parties may choose the law applying to the contract. Article 8 provides that the existence and validity of the contract or any term of it is to be decided by the law which would govern it if it were valid. However, under Article 3(2),'[t]he fact that the parties have chosen a foreign law, whether or not accompanied by the choice of a foreign tribunal, shall not, where all the other elements relevant to the situation at the time of the choice are connected with one country only, prejudice the application of rules of the law at the country which cannot be derogated from by contract'. It could however be difficult for a typical Facebook user to show that all the other elements relevant were 'connected with one country only.'
It is also unclear as to whether the Facebook 'agreement' overrides protection given in other jurisdictions, even to the extent of also overriding constitutional protections.[69] Similarly, is it also applicable to those who are below the age at which they can give irrevocable consent? This question is pertinent because Facebook explicitly permits persons of 13 or over to register as users. In the UK full capacity to contract is not attained till the age of 16 in Scotland and 18 in most of the rest of the UK,[70] and majority as regards contract is not attained before 18 in California, thus making it unclear how minors can make a binding assignation licensing their intellectual property rights (some in perpetuity) to Facebook and its developers in this way, even setting aside the conflict of laws question. As yet there is no definitive answer to any of these questions of jurisdiction; there has been speculation that Facebook's broad licence is an underhand way of bypassing EU and UK legislation, but there is no clear evidence of this. What is obvious, however, is that Facebook adds to the already lengthy jurisdictional challenges posed by cyberspace.

3.7. Limiting the Licence?

As has been illustrated so far, many of the concerns raised and legal questions posed by Facebook stem from the breadth of the licence agreed to by users at the point they join the social network. In this section we question whether such an expansive licence is, in fact, required and consider this in terms of both the lasting effects and scope of the licence.

3.7.1. 'You can check out any time you like…'

As if a ' non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence' was not enough, Facebook's Statement also announces that deleted content will be kept in back-up copies for a reasonable period of time.[71] This means, essentially, that even if a user chooses to leave Facebook, there is no guarantee that their information will be deleted; on the contrary, this implies that it will be deliberately kept, with 'reasonable' left undefined. Even with this considered, leaving Facebook was until recently much easier said than done. Before February 2008, if a user did opt for the drastic solution of trying to reassert full control over their property and ending the licence, they found that they had simply 'deactivated' the account, which, in fact, deletes nothing: all the information is archived in case the user decides to

[67] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). Thanks to Elizabeth Crawford and Janeen Carruthers for drawing our attention to this instrument.
[68] This is defined in Art. 5(1) as 'a contract the object of which is the supply of goods or services to a person ('the consumer') for a purpose which can be regarded as being outside his trade or profession, or a contract for the provision of credit for that object'.
[69] Given that most constitutional protections exist vis-a-vis the state rather than private corporations, in most circumstances these rights will be inapplicable anyway, but consider here, for example, the protection of the visual image under German intellectual property law and the constitutional law governing the dignity of the person.
[70] See the Age of Legal Capacity Act 1991, s. 1, in Scotland; and the Family Law Reform Act 1969, s. 1, in England. Below that age, the position is governed by common law and incidentally the Minors Contract Act 1987; minors can only contract in limited circumstances. These include contracting for 'necessaries' (*Nash* v *Inman* [1908] 2 KB 1), which is a concept broader than the ordinary meaning of the words would imply. See also the Age of Majority Act 1969 (Northern Ireland) as regards reaching full age in Northern Ireland.
[71] Statement of Rights and Responsibilities, supra note 17.

reactivate the account in future. A user who wanted all their data to be destroyed had to delete it themselves, every last bit of it, item by item. This can be no easy task for a previously active user, who may have thousands of items on their own and others' pages, and even then there was no guarantee that all contact details had finally been removed. For example, a Facebook user called Nipon Das went through this painstaking process and removed all the data on his profile, but then reported that a journalist was nevertheless able to contact him through his empty profile.[72] The UK Information Commissioner negotiated with Facebook following a complaint about a similar case in which a British user had to contact the press before Facebook finally deleted his account.[73] Somewhat ironically one user, Steven Mansour, set up a Facebook group on 'How to leave Facebook'.[74] The company has now simplified the process,[75] but information on the procedure is only accessible through its help pages and the default - which is all that appears to be on offer, unless one searches for the alternative - is 'deactivating'. Many will not realise that this leaves all their data where it was - indefinitely. Facebook states that the data will then be inaccessible to other Facebook users[76] but as we have seen, other individual users are only one hole in the leaky tub. Meanwhile, all the data posted by other users – such as photographs, for example – of course remains in place.[77]

Why make it so difficult for users to leave and to delete their information? It is reasonable to build in some delay for the protection of the user against ill-considered deletion of an account, or malicious deletion by others. This does not however justify the extent of the barriers Facebook had erected and have only reluctantly begun to remove. Rather, Facebook can make the case that they need comprehensive licences and exemptions – even at the point at which the contract otherwise ends – because the commercial value of the sites rests in their number of users. If the owners of Facebook wish to sell, the site is worth little unless all the users and all of their personal data can be transferred to the buyer without the need to obtain the individual consent of millions of users. No doubt it also helps if inactive 'deactivated' accounts can remain part of the user tally, thus inflating the value of the enterprise.[78] Certainly, a broad licence is a potentially immense asset, but it is arguable that Facebook would be able to provide a similar service without it; it is the fact that it chooses not to that, more than anything, marks Facebook out as a fundamentally commercial enterprise.

3.7.2. Possible Alternatives

We argue that Facebook would be able to provide the service it does without such a broad licence, without such broad sharing of data with marketers, and without lengthy retention of sensitive personal data after a person has requested that their account and all record of it be deleted. The issues raised here are both technical and commercial.

From a technical perspective, it should certainly be possible for all data uploaded by an individual to be tagged with a unique identifier so that there could be saturation deletion of all a user's content (live and archive copy) when they delete the account, with the exception of material that was never theirs, such as any photos uploaded by another user. Even here however, if the picture has been tagged with the first user's Facebook ID, it should not be difficult to monitor this and include it in a total deletion.[79] Users could also be given the facility to 'lock' data so that it cannot be electronically copied by other users (one only

[72] http://www.iht.com/articles/2008/02/11/business/11facebook.php.

[73] House of Lords Select Committee on the Constitution, 2nd Report of Session 2008–09, *Surveillance: Citizens and the State* Volume I: Report, London: Stationery Office 2009, para.42.

[74] http://www.stevenmansour.com; see also the link to the group: 'How to permanently delete your facebook account', run by Magnus Wallin.

[75] https://ssl.facebook.com/help/contact.php?show_form=delete_account

[76] http://www.facebook.com/help/?page=842

[77] Facebook were not alone in placing obstacles in the path of those who wish to leave: MySpace and Friendster were notorious for their practice of requiring users to confirm repeatedly that they want to leave permanently before they were offered an opportunity to delete the account. It is more straightforward to close a Bebo account, although we experimented with this and found that it took several days for the profile to become inaccessible through a search.

[78] Personal data changes ownership by means of company activities such as merger-acquisitions and reorganisations. See S. Gauthronet, "The Future of Personal Data in the Framework of Company Reorganisations", conference publication, 23rd International Conference of Data Protection Commissioners, Paris - September 2001.

[79] Such as the 'random number system' proposed by Phorm – in that case it is designed to facilitate anonymity, but it could arguably be utilised in the opposite way. For more on Phorm see section 8 below or www.phorm.com.

need think of Acrobat Reader, where information can be read but not edited).[80] It would, of course, be difficult to prevent copying through print-screen options, but this would nevertheless make it more difficult for users to cut, paste and print another user's personal information as they choose. Furthermore, although Facebook may argue that it needs the broad licence for commercial purposes, in order to maximise the value of the site, this fails to justify the relative lack of partial opt-outs. Under an opt-out system, users could offer a broad licence to sell, but not to use, all of their personal data or just some – again, this would return a great deal of control to the user.

As we have seen, then, several avenues of legal complaint could be pursued, and Facebook could be persuaded to offer better, more flexible privacy opt-outs. Perhaps, though, offering such options provides a fanciful protection rather than a real one. At the very simplest, the privacy option would have to be the default, but this would not reflect the variety of privacy choices different users would wish to make. Chris Peterson has argued instead that the solution lies in a more intuitive privacy architecture in which the way users' information is dispersed resembles the way in which they would protect their privacy among real-life, visible audiences.[81] In a prescient study published in 2005, Alessandro Acquisti and Ralph Gross [82] found that student Facebook users at their own university, Carnegie Mellon, permitted an astonishing amount of sensitive personal data to be made public. Whether this was due to Facebook's misleading references to its 'core principle' of privacy, simply because of a lack of awareness, or because they did not much care,[83] students at the university actually used very few of the privacy options that Facebook already provides. The authors, simply by dint of being in that university 'network' on Facebook, were able to download 4540 profiles of the network's users, the vast majority of whom had concealed none of their data from the network. The findings of this study suggest that, even were Facebook to offer greater service provider-to-user or third-party-to-user protection, it is unlikely that such opt-out would be widely used.

3.8. Online Social Networking in the Future

It has been our intention in this paper to draw attention to some of the issues associated with online social networking and, particularly, the Facebook platform. Two main issues have been identified as regards the provider-to-user relationship, namely the 'privacy policy' issues of individuals' personal information in terms of the broad licence, and those relating to advertising targeted at potential consumers on the strength of information gleaned from uploaded personal information. While the fundamental concern of each of these issues is one of privacy, it would appear, however, that the both social attitudes towards and the legal treatment of these issues is very different, much of which could be said to stem from the position Facebook has in the wider context of online and technological advances.

Targeted advertising, for example, is not something that is specific to Facebook alone – on the contrary, Facebook is merely one locus out of many, and not even the largest one at that – the corollary of which is that they are simply part of the wider continuum of commercial digital data capture and use. This 'continuum' is becoming increasingly subject to regulation: the recently announced Internet Advertising Bureau UK (IABUK) Good Practice Principles of online behavioural advertising (OBA) can be cited as an example of industry self-regulation[84], while another interesting development is the arrival on the scene of

[80] For more on technological means of upholding property rights, see, for example, the discussion of 'technologies of identity' in P.E. Agre's article "Beyond The Mirror World: Privacy & the Representational Practices of Computing" in P.E. Agre & M. Rotenberg (eds) *Technology & Privacy: The New Landscape* (2007, MIT Press: Cambridge).

[81] 'Saving Face: The Privacy Architecture of Facebook', 2009, http://works.bepress.com/cpeterson/1/.

[82] Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, 2006, http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

[83] Acquisti and Gross speculate that people tend to give truthful answers on Facebook because they are interacting with their friends, namely people who already know their name, birth date, sexual preferences and so on. This is very different from other, open-access sites such as MySpace, where there is much more incentive to create a fictional self or multiple identities.

[84] The drafting of these principles has been undertaken in collaboration with the American Association of Advertising Agencies (AAAA) and the Direct Marketing Association (DMA), along with many of the bigger players in the industry, although this list does not, it should be noted, include Facebook. These Good Practice Principles, which are due to come into force in the UK on September 4, 2009 are intended to be used by 'businesses that collect and use data for behavioural advertising' and are '[t]hey are based upon offering users notice about data collection, choice as to whether to participate and education about behavioural advertising and its benefits.' For further details see http://www.iabuk.net/en/1/behaviouraladvertisinggoodpractice.html

companies such as NebuAd in the US and Phorm in the UK, who are respectively promoting an alternative to what they term the recognised 'orthodoxy' of 'store and retrieve'.

On the other hand, the privacy policy issues are far less well-developed in terms of, specifically, their *legal* character, not least to the extent that it is actually still unclear whether or not this is an area that should be covered by legal provisions as such. For example, should the law *force* Facebook and other OSN sites to improve upon or even simply clarify their privacy policies, and – if so – how could this be effected? Would a mere display of a clear notice on the behalf of the provider be sufficient in providing the users with this information? Also, and perhaps most controversially, is the question of whether or not the users actually *care* about this to any real extent? While the users and the Bloggers are 'rallying in support of copyright' in order to protect their work, as was discussed above, can it really be said that there is the same attachment to one's personal data? Is its 'gathering' and storage perceived as being a simple consequence of participation in OSN communities, a price that users are willing to pay for the privilege?[85] If there were to exist some form of legal recourse for a complaint of this nature, would such a complaint be forthcoming?

With online social networking still being in its comparative infancy, it is impossible to provide answers to these and similar questions with any degree of certainty, although we would tentatively suggest that much of the development of the law in this area will be dependent upon which of the many differing social attitudes towards online privacy ends up eventually prevailing. With these different attitudes being spread across various sectors of society (most notably age-group)[86], however, it is far from clear whether it is possible that a genuine consensus be achieved. Indeed, in terms of access and control of personal information posted online, it appears that an exploration into what is in fact considered to be *private* is required before the law can make much of an attempt to regulate OSN providers such as Facebook.

[85] One possible 'sweetener' could be that the individual gleans some benefit from inputting their personal data and related online practices, over and above that of simple utilisation of the platform; as Corien Prins states: "Individuals make deals for the disclosure, collection, use and re-use of their personal data [and] in certain situations receive some form of compensation [...] and thus 'exploit' and 'sell' their habits, user-profile and individual data'. See C. Prins, *supra* note viii at 275

[86] 'In the past ten years a new set of values has sneaked in..., erecting another barrier between young and old. [... T]he older generation has responded with a disgusted, dismissive squawk: Kids today. They have no sense of shame. They have no sense of privacy. They are show-offs, fame whores, pornographic little loons who post their diaries, their phone numbers, their stupid poetry – for God's sake, their dirty photos! – online.' And the opposite perspective: 'More young people are putting more personal information out in public than any older person ever would – and yet they seem mysteriously healthy and normal, save for an entirely different definition of privacy. From their perspective, it's the extreme caution of the earlier generation that's the narcissistic thing.' See Emily Nussbaum's New Yorker Magazine article, February 12, 2007: http://nymag.com/news/features/27341/ and Vicky Allan's related article in Sunday Herald, April 4, 2009: www.sundayherald.com/search/display.var.2499891.0.meet_the_bebo_generation.php