CHAPTER TEN: LAW AND THE FUTURE OF DATA CONTROL

# Data Control and Social Networking: Irreconcilable Ideas?

Lilian Edwards[1] and Ian Brown[2]

## I. Introduction

The future of both law and technology will require reconciling users' desire to self-disclose information with their simultaneous desire that this information be protected. Security of personal information and user privacy are potentially irreconcilable with the conflicting set of user preferences regarding information sharing behaviours and the convenience of using technology to do so. Social networking sites (SNSs) provide the latest and perhaps most complicated case study to date of these technologies where consumers' desire for data security and control conflict with their desire to self-disclose. Although the law may provide some data control protections, aspects of the code itself provide equally important means of achieving a delicate balance between users' expectations of data security and privacy and their desire to share information.

## II. The rise of social networking

### A. What are SNSs?

SNS's were the Internet phenomenon of 2007 and show no sign of losing impetus. Sites like MySpace, Facebook, Orkut, LinkedIn, Bebo and Club Penguin have attracted students and seniors, adults and children, business users and entertainment seekers, Americans and Europeans in ever increasing numbers. Social networking sites (or "services", as that sometimes unreliable font of all wisdom Wikipedia, describes them[3]) can be characterised as "*online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software*[4]". SNSs differ enormously in their intended audience, Unique Selling Points and interfaces, but all tend to share some points of similarity, such as

- "friends" or "buddy" lists;
- disclosure of personal information via pre-structured "user profiles" including items such as name, nickname, address, email address, birthdate, phone number, home city or town, school or college, pets, relatives etc;
- some form of intra-site messaging or "bulletin posting", which encourages further disclosures of information by users to other users;
- a profit-making mechanism for the site owner, usually at least partly derived from adverts served up to users when they view their own or other users' profiles.

---

[1] Professor of Internet Law and Director of ILAWS, the Institute for Law and the Web at Southampton, University of Southampton. We would like to thank Chris Marsden, University of Essex, for engagement with work preliminary to this paper, and Judith Rauhofer, University of Central Lancashire, for helpful comments in draft.
[2] Research Fellow, Oxford Internet Institute.
[3] http://en.wikipedia.org/wiki/Social_network_service .
[4] Ibid.

- governance by terms and conditions of the site user, or "end user license agreement" or EULA.

As will be seen below, all of these common features which enable and enhance social networking (or in the fourth and fifth examplex, allow the site to survive financially and practically), can unfortunately also be seen in practice as sources of concern when we look at user privacy. Other features which are beginning to appear on some SNSs, and which also have serious privacy implications include:

- organisation of users into groups or "networks" by some schema eg country, region, town , college, school, colour, sexuality
- integration of the SNS as website with mobile phone communications so, eg, an SNS member can be notified or made known to another SNS user when within the same locational area – using mobile phone cell or GPS technology
- the allowing of access by site owner of third party "apps" or applications to the SNS. This brings into play issues of control of, and access to, the personal data of users by parties other than the SNS site owner which as we shall see below can be disquieting.
- mining of personal data placed on SNS profiles together with non-explicit "traffic" data generated by users to produce profiled, context sensitive advertising.

Finally, many, though not all, SNS specifically target children and young persons as a key audience. Early social networking websites, for excample, included Classmates.com ( founded 1995), focusing on ties with former school mates, and Facebook (founded 2004) originally built its audience by "capturing" entire school or undergraduate student years as a kind of digital class yearbook. In recent years sites aimed at a younger age group such as Bebo and Club Penguin have been big commercial successes. Given the perceived vulnerability of young people in the online environment and their general lack of life experience, this raises further concerns. Note however the UK statistics cited above which demonstrate that even SNS s originally rooted in a youth demographic have the capacity to outgrow this stage and reach a wider audience.

## B. How prevalent are SNSs?

According to the Pew/Internet Survey of 2007, 55% of US online teenagers have an SNS presence[5] while in Europe, 32% of 18-24 year olds use an SNS at least monthly[6]. Global SNS user figures are staggering for such a recent innovation; MySpace reports having 217 million users worldwide while competitors Bebo and Facebook claim 40 and 62 million global users respectively, while "business user" SNS, LinkedIn, has 17 million global users[7]. As well as the current "big three" SNSs, MySpace, Facebook and Bebo, SNSs exist for every social, cultural , racial and ethnic niche: Jews, blacks, Asians, Swedes, football fans, environmentalists, photo-bloggers, etc etc[8].

[5]

[6] Livingstone

[7] http://en.wikipedia.org/wiki/List_of_social_networking_websites

[8] Ibid.

In the UK, which bears perhaps the greatest resemblance to US Internet culture in Europe, the SNS site, Facebook, has become both the market leader in SNS in 2007 and omnipresent in conversation and press headlines. Facebook grew exponentially in the UK in August 2006- September 2007 according to a major survey carried out in 2007 by analysts Human Control, increasing its audience capture by 1800%[9], overtaking MySpace to become the market leader, and reaching around 23% of the active Internet user population of the UK. Over the same survey period Internet "reach" itself only increased by 11% in the UK. Audience numbers rose by 20% per month throughout 2006-2007, although this had slowed to 15% per month by September 2007. Facebook had 7.5 million unique users in the UK by September 2007, while MySpace had only 5.2 million users and Bebo (aimed at younger children) 2.7 million users[10]. Based on number of unique users, Facebook was the 13th most popular website in the UK in 2007, beaten out by numerous other Web 2.0 sites such as You Tube, eBay and Wikipedia. based on number of web pages viewed however, Facebook was the third most popular site, with over 3,000 million page views per year, beaten only by Google and eBay.

Furthermore, and contrary to popular belief (and unlike many other SNSs), Facebook is not used exclusively by undergraduate students and school kids. In fact, the age of the average Facebook user by September 2007 was almost 34 with most of the user growth coming from the 25-34 year old age bracket. Even among over 65s, hardly the typical imagined users of SNSs, Facebook had an audience in September 2007 of 131,000 men and 49,000 women. Furthermore, like many SNSs and unlike many more traditional Internet sites, Facebook does not have a male bias. Instead, it has distinct gender skew with 22% more females using it than males, the bias being greatest among young females in the 18-24 age group.

These figures demonstrate provocatively the staggering and sudden rise in popularity of SNSs, the diversity of the age and gender groups engaging, and in particular the current victory over the UK market by one site, Facebook.

## III. Social Network Sites and Personal Data Disclosed

A Typical Facebook user profiles frequently include large amounts of personal, and even, in the terminology of the European Data Protection Directive (DPD)[11], "*sensitive*" personal data[12]. For example, one real Facebook profile revealed through

[9] All figures about Facebook in this paragraph are taken from Broughton T and Popk H *The Facebook Faceoff: A Survey by Human Capital*, based on Nielsen Net Ratings survey panel of approximately 40,000 persons in the UK only; survey released at *Poke 1.0*, London, November 15, 2007, accessible at http://www.scribd.com/doc/513941/The-Facebook-Faceoff-An-Empirical-Analysis-by-Human-Capital.

[10] See Sonia Livingstone presentation, *Taking Risky Opportunities in Youthful Content Creation*, Media@LSE, presented at Poke 1.0, London, November 15 2007, accessible at http://www.scribd.com/doc/513946/sonia-livingstone-social-networking-presentation-Poke-symposium.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[12] Defined below.

self-disclosed information and network affiliations that a certain male member of the Communication Workers' Union living in Illford, England, was a liberal Catholic in an open relationship with a woman named Jeanette and infected with the HIV virus. In this profile, therefore, we find sensitive information of several kinds – union affiliation, political and religious affiliation, interpersonal lifestyle information, including information naming another individual, and health information.

Privacy in the context of the information society is usually viewed as being about control by a living person over the processing of one's "personal data", defined in the DPD as "*any information relating to an identified or identifiable natural person ("data subject")*" where an identifiable person is "*one who can be identified , directly or indirectly, in particular by reference to a identification number or to one or more factors specific to his physical, physiological , mental, economic, cultural or social identity*".[13] The DPD then goes on to prescribe a regime based on eight principles for the processing of personal data which include but also expands upon the familiar OECD Privacy Principles[14]. Key elements of the European DPD regime include that :

- processing is to be fair and lawful, with consent of the data subject as the primary means of establishing that processing meets these conditions;
- processing is only to be undertaken for known and specified purposes;
- no more personal data is to be gathered than necessary and relevant to these purposes
- data is to be kept accurately and if necessary updated
- data is not to be held longer than necessary to fulfil these purposes
- data is to be held securely
- rights of data subjects, eg to access and correct their data, and prevent its use for direct marketing, are to be respected
- data is not to be exported without consent to countries outside the EU where privacy protection is not "adequate".

"Sensitive personal data" is defined in the DPD as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life*.[15]" . The DPD states that particular conditions and safeguards must be observed when particularly "sensitive" personal data is processed.

If we look at many Facebook profiles they contain, or appears to contain, almost every category of data deemed especially "sensitive" by EU law. Facebook profiles typically reveal sexual details ("looking for man/woman/both"); religious details ("Jewish/atheist"); and political details ("very liberal"). Group memberships and events may also reveal significant information (eg member of "Gay Pride London 2008"; "attending "Vote for Obama" "; member "HIV Survivors Support New Jersey" ). Empirical research suggests the view that this revelation of sensitive data is typical of user profiles. Gross and Aquisti found in 2005 that, looking at a sample of 4,500 Facebook profiles of Carnegie Mellon students they had spidered, 80%

[13] Art 2(a), DPD.

[14]

[15] Art 8, DPD.

contained an image of the user; 87% contained a date of birth; 39% listed a phone number; and over 50% listed a current residence. Turning to "sensitive data", the majority of users in the study also listed sexual preferences ("Men", "Women"), current relationship status, and political views[16].

This simple example demonstrates both the potential of SNSs to disperse highly personal data, possibly to the detriment of the data subject; while at the same time introducing the conundrum of whether traditional privacy legislation may over-regulate in a new era where disclosure rather than secrecy may be becoming the norm. EU DPD law demands, for example, that a user gives *explicit* consent to the processing of sensitive personal data, while in relation to "ordinary" personal data implied consent will suffice. Is it reasonable or practical to demand a higher standard of privacy protection in relation to one piece of data on a user SNS profile and not the rest of the profile? Arguably the DPD provide an exception that may negate the special rules on "sensitive data" in the SNS context, namely that "special treatment" is not required where "the data are manifestly made public by the data subject"[17] but this merely pushes the question one stage back: should a vulnerable young person, say, lose protection over their sensitive data simply because social networking sites are by default public? Are these particular types of data really more "sensitive" in the eyes of the average SNS user? Certainly standard industry practice does not seem to show a difference in practice in relation to different types of data disclosed and it is questionable how such distinctions would be implemented.

Below we will examine a number of problems which have arisen in relation to privacy and personal data on SNSs through the lens of a number of widely covered recent incidents in the SNS world, and ask if these apparent or potential threats to personal privacy demand reconsideration of either or both of the *detail* or the *application* of existing informational privacy laws to SNSs.

### A. Case study one: the Oxford Facebook case and the dangers of default privacy settings

In July 2007, Oxford proctors in charge of university discipline at the ancient university used Facebook to find evidence of students breaking university disciplinary rules. Students, who, in post-exam hilarity, had held wild parties, sprayed each other with champagne or shaving foam, or thrown flour bombs at each other, often posted photos of these incidents on Facebook. Proctors combed Facebook for evidence of such incidents and caught a number of students *in flagrante*. As a result, a number of students received disciplinary emails or more vigorous sanctions. The response from students was dismay and shock. The student union claimed that the incident was a "disgraceful" intrusion into the privacy of the students concerned. One caught perpetrator complained that she was "outraged":

> "Alex Hill, 21, a maths and philosophy student, received an e-mail stating that three of her photos provided evidence that she had engaged in "disorderly" conduct. "I don't know how the proctors

[16] Gross R and Acquisti A "Information Revelation and Privacy in Online Social Networks (the Facebook case)", ACM Workshop on Privacy in the Electronic Society, *WPES* '05, November 7 2005, Alexandra, Virginia, USA, available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf .
[17] DPD, Art 8(2)(e).

> got access to it," the St Hugh's College student said. "I thought my privacy settings were such that only students could see my pictures.
>
> "They cited three links to pictures on my Facebook profile where I've got shaving foam all over me. They must just do it randomly because it would take hours and hours to go through every profile. I'm outraged. It's truly bizarre that they're paying staff to sit and go through Facebook. It must be extremely time-consuming.[18]"

A number of points are worth making here. First, Ms Hill displays a common misperception that her posts on Facebook were "private" or at least restricted in access to her perceived "friends" group, namely fellow Oxford students. In fact, on Facebook, the default site setting is that profiles, including photos of events posted, are visible to everyone in the user's default "network". For Ms Hill, an Oxford student with, one assumes, an *oxford.ac.uk* email address, her posts and photos would have been visible in their entirety to every member of the Oxford university network (unless she had deliberately altered the default settings – see further below). While, from press reports, Ms Hill seems to have been aware that she belonged to a network and that this had disclosure implications, what she failed to anticipate is that not only students but also staff on the Oxford University payroll (including proctors) might have *oxford.ac.uk* email addresses, and thus also have access by default to her profile and photos[19].

While one might argue that an Oxford student who failed to work out something as obvious as the possibility of surveillance when committing illegal acts deserved to get caught, the "network default" issue is an important one. The London Facebook Network has 2.1 million people in it as of January 2008: those who join that network in good, albeit ignorant, faith (perhaps because they want to see what events are on in their area, or want to track down a friend in the area) are disclosing their personal data by default to those millions of people, some of whom have every chance of being ID thieves, spammers or worse. Furthermore while university networks on Facebook are in theory "policed" by the need to have a relevant email address (eg an *ed.ac.uk* address to join the Edinburgh University network), non-university networks eg London, Oxford, Edinburgh have no such requirements – this writer might , for example, join the Portsmouth network to stalk a Portsmouth resident without having any connection to that city[20].

Privacy defaults on SNSs can of course generally be altered by users, and Facebook in fact has a relatively sophisticated and granular set of privacy controls[21]. However both

---

18 See "Caught on camera- and found on Facebook", *Times* July 17 2007 at http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2087306.ece .

19 Another "lurking" set of persons with access to a university "network" on Facebook are those who once had legitimate university email addresses but have since moved on. The writer of this chapter, now at Southampton University, is still a member in good faith of the Edinburgh University network on Facebook, on the basis of a now expired email address acquired from her former employers.

20 Although Facebook does restrict a user from belonging to more than one geographical network at a time. This would not one imagines deter the determined stalker.

21 By "granular" I mean that user X can choose, for example, to disclose his friends list to everyone, his picture and biographical details only to friends and his email address to nobody. Compare the SNS Live Journal where a user can only choose to display the whole of a post or none of it certain groups of "Friends".

anecdotal and survey evidence show that few users are aware these controls can be "tweaked" (or even that they exist) and even fewer then take the time and energy to make these changes[22]. Gross and Acquisti, for example, found that only 1.2% of Carnegie Mellon students in their survey changed their default settings to make their profile more private, and concluded that "*only a vanishingly small number of users change the (permissive) default privacy preferences*[23]." Default settings are not consistent across different SNSs so there is little or no "learning from experience" as users move from today's hot SNS to the next flavour of the month. Even within a single site such as Facebook, privacy defaults may not be consistent. For example, consider A, who is a member of two Facebook networks, Oxford University and London. A may alter his privacy defaults so that only his "friends" list and not every member of the Oxford University network has access to his biographical details, photos etc. However, possibly unknown to A, his choice will not have altered the settings for his London network and so all 2.1 million London members will continue to have access to all of his personal data. Even a determined privacy-conscious user might struggle to control access to their data given such inconsistencies, let alone the inexperienced, time-poor and disclosure-prone users of SNSs.

The fundamental issue here is that privacy on SNSs is primarily regulated not by law (whether it is EC data protection law or US rules such as COPPA[24]) nor by informed user choice as the OECD principles might demand, but, as Lessig famously put it, by *code*[25]. Privacy rights in the examples above are determined by the default settings coded into the software, and they in their turn are determined by the writers of the SNS code. What incentive does the SNS have to code a "reasonable expectation" of privacy into its system as a default? There is no guarantee that the SNS has the privacy interests of its users as first priority when setting privacy defaults - indeed the converse is more likely to be true. As SNSs derive their income streams at least partly from data disclosed by users, their financial incentive is arguably to maximise disclosure and minimise privacy[26].

A second key point raised by the Oxford case is the recurring question of whether Facebook and similar SNSs are indeed a "private" space where the user has reasonable expectations of privacy, or a "public" space where such expectations do not or should not exist. Ms Hill's "outrage" at being stalked in an "underhand" fashion by Oxford proctors seems to show an honest (if unreasonable?) belief that she was operating in a friendly private space. Should such attitudes be taken into account and reified by the law or by code?

Livingstone, researching attitudes of young persons in the UK to privacy on Facebook in 2006, found that young people had both a conflicted attitude to privacy and often were either ignorant or confused as to how far they could alter privacy settings[27]. One of her respondents, Nina, complained that "*they should really do something about*

[22] Partly because of the approved social value of "openness" and its perceived advantages on SNSs – see further below.
[23] Gross and Acquisti, supra, n XX.
[24]
[25]
[26] See "Do social network sites genuinely care about privacy?", *The Guardian*, September 13 2007, available at http://www.guardian.co.uk/technology/2007/sep/13/guardianweeklytechnologysection.news1 .
[27] See Livingstone, supra n. XX.

*making it more like private, because you can't really set your profile to private"*. Another, Ellie struggles with trying to leave her school area network when she moves away. "*I probably can, but I'm not quite, I'm not so great at that, I haven't learned all the tricks to it yet*."

Barnes, working in the US, notes that there is an apparent disconnect – which she names the "privacy paradox" - between "*the way users say they feel about the privacy settings of their blogs and how they react once the they experience unanticipated consequences from a breach of privacy*"[28]. She cites a student in one of her own surveys who explicitly reported her concern at revealing personal information online, but meanwhile had a Facebook page which nonetheless gave away her home address, phone numbers and pictures of her young son. The Internet abounds with such contradictory evidence.

Barnes' conclusion is that "*on the Internet , the illusion of privacy creates boundary problems*" with new users, and those engaged exclusively in recreational pursuits are most convinced by the illusion[29]. Students and young persons clearly wanted to keep information private from some persons, eg parents and teachers, but did not seem to realise Facebook was a public space. Such pervasive assumptions seem to go beyond mere ignorance to something more rooted about perceptions of social network and virtual community spaces, especially given so many students of today are tech-savvy and (by definition?) well educated and familiar with information technology.

Privacy jurisprudence itself is conflicted about whether "privacy in public" exists and should be protected. The European Court of Human Rights, for example, has been in the process for some years of recognising that privacy rights do exist even in public spaces, and even where celebrities, the archetypal "public property", make themselves accessible to press attention in public - most noticeably in the celebrated recent ECHR case of *von Hannover*[30]. In the UK, the Press Complaints Commission has given spectacularly contradictory decisions concerning celebrity privacy in quasi-public spaces such as beaches[31]. On social networking sites, where the whole purpose for

---

[28] Barnes S "A privacy paradox: social networking in the US" , *First Monday*, Issue 11/9, September 2006, available at http://www.firstmonday.org/ISSUES/issue11_9/barnes/ , citing Viegas FB "Blogger's expectations of privacy and accountability; An initial survey", (2005) Journal of Computer-Mediated Communications, volume 10, number 3, at http://jcmc.indiana.edu/vol10/issue3/viegas.html .

[29] See also Katz JE and Rice RE *Social consequences of Internet use – Access, involvement and interaction* (2002, Cambridge, MIT Press).

[30] von Hannover case.

[31] See Anna Ford complaint about paparazzi taking photos of family beach holiday, not upheld at , http://www.pcc.org.uk/news/index.html?article=MjAyNA and Gail Sheridan, complaint re use of long lens to photograph her in her own back garden, at http://www.pcc.org.uk/news/iondex.html?article=NDUzNw== - both privacy complaints not upheld; cf JK Rowling, complaining of press photos taken while on a Mauritius beach as family holiday, upheld, at http://www.pcc.org.uk/news/index.html?article=MjA0NQ==, despite very similar circumstances to Ford. (Contrast Rolwling's treatment in the courts in *Murray (by his litigation friends Neil Murray and Joanne Murray) v Express Newspapers plc and Big Pictures (UK) Limited [2007] ) EWHC 1908 (Ch)* *(http://www.bailii.org/ew/cases/EWHC/Ch/2007/1908.html)* .
The PPC is not a court and asserted in the Rowling complaint that it did not have to follow its prior decisions, especially Ford, though it would have regard to them. See also apology to Sara Cox, equivalent of "settlement") at http://www.pcc.org.uk/news/index.html?article=Mjg2MQ== .
Interestingly, following a number of complaints, the PCC has recently commissioned a report into whether use by newspapers of information found on SNSs is abusive of privacy and should be a breach

users is to network and to expose parts of themselves so as to engender trust and communication, the discourse is hopelessly confused. Trust and disclosure, arguably, depend on users perceiving their surroundings as quasi-private or at least "gated"; as a "social club" of some kind. Yet Dwyer, Hiltz and Passerini found in 2007 that SNS users were prepared to disclose remarkable amounts of personal information on a number of SNS sites even if they had relatively little trust in fellow users[32]. This would seem to argue that a high level of disclosure by users does not imply a reasonable expectation of privacy.

A final obvious point raised by the Oxford case and the many, many similar cases[33], is that SNSs are simply a stalker's[34] – and a voyeur's - charter. Many groups have incentives to surveille SNS users for a variety of less or more dubious purposes. These range from surveillance for legitimate law or norm enforcement purposes (as in the Oxford case itself), to curious investigation by current or former friends, to less savoury stalking by strangers or perhaps ex-partners, to collection of data without consent for economic exploitation by *inter alia* spammers, direct marketers, data miners and identity thieves[35]. It is extraordinarily difficult to measure or prescribe the quantity of privacy protection that users should expect or be able to demand as default or option, given this extensive range of possible watchers and data collectors, legitimate and illegitimate.

It should also not be forgotten that data disclosed on SNSs may persist for an unknown length of time. What if the harmless pranks of children today, which once would have vanished into faded memory but are now enshrined on an SNS, become part of a juvenile delinquent's profile tomorrow, and a reason to be denied employment or admission to university in ten years' time? One of the most worrying aspects of the SNS phenomenon is the generally acknowledged surge in their use by employers and other institutions as a means to screen applicants[36].

Recent reports in the UK have also suggested that while, in theory, data on Facebook can be deleted, Facebook does not guarantee this in terms and conditions, and in

---

of the PCC Code: see http://blogs.guardian.co.uk/greenslade/2008/02/pcc_faces_up_to_facebook_intru.html . In this context, the PCC may be viewed as being in advance of the courts.

[32] Dwyer C, Hiltz SR and Passerini K "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", Proceedings of the 13th Americas Conference on Information Systems, Keystone, Colorado, August 8-12 2007, available at http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf .

[33] See n XX below.

[34] The first UK prosecution for harassment explicitly involving Facebook has been initiated in March 2008. See http://www.out-law.com/page-8913 .

[35] See "Cyber thieves target social sites", BBC News, 3 January 2008, suggesting that in 2008 SNSs would become "an attack vector for the hi-tech gangs who are behind the vast majority of cybercrime", available at http://news.bbc.co.uk/1/hi/technology/7156541.stm .

[36] See eg "Would be students checked on Facebook", *Guardian* January 11 2008 (Cambridge University tutor admits to screening students via Facebook), available at http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html; Yeoman A "Facing up to facebook", Magazine of the Society for Computers and Law, 2007, Vol 18, issue 4, October/November, p 31 (citing the growth of Facebook "sucks" sites by disgruntled employees and what employers should do to curb them) available to members at www.scl.org; "Caught on camera", *The Times*, supra n XX (survey of 600 UK companies revealed that one in five employers had used Facebook and other SNSs to screen applicants).

practice profiles have a bad habit of persisting[37]. Even where the site co-operates in providing effective deletion mechanisms, it is more than likely that disclosed data may still be available via Google cache[38] or archiving sites such as the Way Back Machine[39]. Such concerns, yet again, do not seem to have communicated themselves to younger users. A study by the UK Information Commissioner's office (ICO) in 2007 found that almost 60% of UK 14-21 year olds did not realise the data they were putting online could be permanently linked to them, and reactions were generally horrified when this was suggested [40]. Just as users' perception that SNS's are a safe and private space is faulty, so apparently is their perception of the risk of long term unintended consequences arising from their disclosures.

### B. Case study two: the "Compare Me" application and the role of third party applications, third party tagging and loss of data control

One feature of Facebook which may have helped it become SNS market leader in several countries has been the opening up of the site to applications written by third parties who have entered licensing agreements – the so-called "apps". Popular apps include, for example, Scrabulous – an obvious clone of Scrabble which is currently subject to threat of suit for trademark infringement by Mattel and Hambro[41] - which allows users of facebook to play Scrabble online. Similarly apps have been written to allow users to send kises, flowers, virtual fish and virtual gifts to their friends list; to engage in tribal "warfare" games in which friends are either attacked or recruited to ranks of vampires, werewolves, slayers etc; and to interface with other popular sites such as LifeJournal , Flickr and Blogger. What all these apps have in common is that when the user attempts to use the application they are required to consent to a license which invariably requires the user to share his or her own personal data, and sometime to share the personal data of friends.

By way of example, one third party application on Facebook is called "You are Gay." It is impossible to opt out of allowing this application to access all the data Facebook holds about you and to still gain access to the application. This data would include full real name, friends, phone number et al, even though the only purpose of the

---

[37] See eg "Facebook faces privacy probe", *PC World*, 22 January 2008 (reporting a UK Information Commisioner investigation in January 2008 into persistence of Facebook profiles even after users tried to accomplish deletion) available at http://www.pcworld.com/article/id,141607-page,1/article.html . Facebook are now reported to have bowed to ICO and other pressure and guaranteed that total deletion of profiles will in future be possible – see http://www.out-law.com/default.aspx?page=8882 . See also Anita Ramasastry's editorial at http://writ.news.findlaw.com/ramasastry/20080229.html , who opines that Facebook's lack of deletion facilities prior to this change, may have been legal in the US but not the EU.

[38] Facebook profiles were originally not made available to Google spiders. However Facebook took a decision to make profiles available to Google and other search engines in September 2007. Users were given an opportunity to opt-out of (rather than to opt *in* to) having their profiles indexed. See discussion in this writer's blog, "Facebook and privacy returns", *Pangloss*, September 05 2007, available at http://blogscript.blogspot.com/2007/09/facebook-and-privacy-returns.html.

[39]

[40] See full report at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/research_results_topline_report.pdf . One respondent to the survey (female, age 14) replied "*Initial thoughts – who cares? Subsequent thoughts – omg*!".

[41] See "Facebook asked to pull Scrabulous", BBC News, 16 January 2008, available at http://news.bbc.co.uk/2/low/technology/7191264.stm .

application is to send a message to a specified other Facebook user saying "You Are Gay!" (too?). Almost all Facebook Apps are similar in demanding access to all the information the user has given to Facebook, and yet making little or no use of it for the purpose of the app itself[42]. This pattern is replicated throughout every Facebook app this writer has seen, and it must therefore be assumed it is the standard access license template offered by Facebook to app developers. The impression of choice for the user is therefore illusory: it is take the app *and* give away personal data (*all* personal data), or nothing.

Why this is problematic for privacy? Consider the "Compare Me" incident of September 2007. Compare Me is an app created by Ivko Maksimovic which allows a user to compare two friends on random questions, "everything from "who is more tech-savvy" to "who would you rather sleep with"[43]. As a result, anonymised rankings are produced in which a user might learn that he was 3rd "hottest" in his group of friends but only 18th the "person they would most like to go shopping with". No details would be available of who the user had defeated or lost to in the various comparisons made, nor who had voted for the user to win or lose. Naturally, such information if available could be highly embarrassing. The app claimed that:

> *"Your friends cannot find out how you compared them except when it's an innocuous compliment. For example, if someone loses a comparison, they will not know that they lost. If you rate compare someone on a dating question, they won't know how you chose. There is no way for someone to look at the rank lists and see who said what about them. "*

However, despite this promise, a "premium" Compare Me service was then offered for a small payment, which allowed subscribers to find out some details both of "voters" and who had been beaten or won in the various "Compare Me" challenges[44]. Despite publicity on various blogs of this breach of privacy (and promise), the app continues to be available on Facebook, as of January 2008.

The example is trivial, but it illustrates vividly the difficulty of controlling personal data spread and enforcing privacy guarantees against third party application writers. While an SNS in its nature encourages the disclosure of personal data, at least that information may be relatively safe if the SNS itself can be trusted, and the user takes sensible safeguards, such as changing privacy defaults to hide sensitive parts of profiles from all comers. However once data has been divulged to third parties via an app, that data is beyond the control of both user and the SNS site itself. It is possible that the SNS may contractually require the third party app developer to take reasonable security precautions and accord with local privacy laws – but the user will not usually see that contract nor be party to it nor have title to enforce it. Neither does

---

[42] See survey referenced at http://www.cs.virginia.edu/felt/privacy/ by Adrienne Felt and David Evans. In October 2007, they performed a systematic review of the top 150 applications on Facebook. 8.7% needed no data at all to work; 82% used public data (eg name, list of friends) and only 9.3% needed acess to private-by-default data (eg birthdate). They concluded: "Since *all* of the applications are given full access to private data, this means that **90.7% of applications are being given more privileges than they need.**"

[43] See "Compare Me Facebook App Pulls A Bait and Switch?", 7/9/07, available at http://www.sugarrae.com/compare-people-facebook-app-pulls-a-bait-and-switch/ .

[44] See "More on the Compare Me Premium Service", 11/0/07, available at http://www.sugarrae.com/more-on-the-compare-people-premium-service/ .

the law in either Europe or the US appear to demand that an SNS ask for such contractual assurances.

SNSs as currently constructed typically give the average user little or no chance to find out if an app is really a front for, or selling information to, third parties such as marketers, spammers or stalkers. Obtaining information about app developers in advance is difficult to impossible. In many cases, a full terms and conditions or license agreement can only be viewed (if at all) after consent has been given and the app has been loaded – equivalent to locking the stable door after the personal data has bolted.

To make matters worse, many apps are "viral", in the sense that a user cannot sign up to them, or get results out of them, unless they pass the app on to 10 or 15 other friends on the same SNS first. What this boils down to is that the price of entry is not only giving away your own details but also supplying the email addresses or other personal data of friends. Being viral, such apps spread rapidly. And being, on the whole, trivial applications, users rarely stop to think whether sharing data with unknown third parties is wise or in their best interests. All in all, it might be suggested that the easiest way to become an ID thief in the SNS world is to simply write a popular app, sit back, and gather all the personal information you want[45].

In fact, it is not even necessary to write an app to collect data from strangers. Many users, as we have already discussed, will leave their privacy defaults undisturbed and broadcast all their personal details to the world. Even those who restrict some or all of their data to "friends", however, can fall prey to illicit surveillance and data collection. Above, we mentioned the "illusion" that an SNS is a private or a "friendly" space, not a "public" space. Another problem with this "illusion" as to SNSs is that "friendship" seems to be a far thinner construct on SNSs than in real life. Millions of people inhabit SNSs and friends lists of 100s or even 1000s of people are not uncommon. By contrast, anthropological research has often shown that in "real life" a viable friends group usually has a maximum of around 50 people[46]. Social competition and peer pressure seems to lead users, especially young people to engage in competition to collect "friends" – "friends whoring" as it is sometimes called. In such an environment, it is not hard for a stranger to ask to become someone's "friend" and have his or her request accepted, even if they are completely unknown to the user in question. In one famous experiment, Sophos the anti-virus company created a frog character on Facebook, who requested to become Friends with 200 users[47]. 41% of users approached agreed to befriend the frog, thereby divulging in most cases data such as email address, data of birth, phone number, current address and education or occupation[48].

Loss of control of personal data to third parties is a pervasive theme on SNSs. On Facebook, photographs and "tagging" present a particular problem. Photographs can be "tagged" with the names of the Facebook users who appear in them, and this tagging can be done not only by the data subject – the person in the photograph – but

[45] See further *Macafee Virtual Criminology Report 2007,* November 2007, available at
[46] ref
[47] In a nice touch, the frog was named Freddi Staur, an anagram of "ID Fraudster".
[48] See Sophos press release at http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html
.

by any other Facebook user. It is quite possible that the students caught in the Oxford Facebook case (above) had not been so foolish as to tag themselves in photos depicting illegal acts, but that "friends" had done it for them. Photo-tagging is seen as one of the "killer app" features of Facebook and there is no community norm discouraging the tagging of other people's photos. Again, it is possible on Facebook to amend the code defaults so that tagging can not be done by third parties – but this option is buried in the privacy section and almost certainly entirely ignored by most users. We will return to the issue of the setting of privacy defaults below.

Photographs, and photos used as icons (characteristic pictures which head up the user's profile) are of particular importance in a privacy context because they can act as an index to connect a user profile of A on one site to A's activities on another site. For example, a user might have the same photograph on herself on two websites, Live Journal and Facebook. Live Journal is a blogging site where pseudonyms are used and privacy is on the whole prized and respected. Meanwhile, Facebook is a site whose contractual terms and code both attempt to enforce the use of real names. It is not hard to imagine how a photo tagged with a name can be used as a "key" or unique identifier to link anonymised personal data to real world nymic data, with predictable privacy-invasion consequences. The ENISA Report on security issues for online social networks[49] recognised "face recognition issues" as one of the key problems for SNSs. Face recognition software has improved extraordinarily over the last decade so that automated correlation of user pictures across different sites has become increasingly plausible both for law enforcement agencies and more dubious entities. According to ENISA, Facebook had a database of around 1.7 billion user photos as of May 2007, growing at more than 60 million per week. In work by Gross and Aquisti in 2007 and 2005[50], it was shown that above 60% of images on Facebook were good enough for direct identification of users using commercial face recognition software. Re-identification – the connection of a user via their photo to other data anonymised but bearing the same image – was therefore eminently possible. In a world of ubiquitous CCTV surveillance and post 9/11 paranoia, the privacy consequences of this beggar the imagination.

A final threat related to loss of control over data is the threat to security. It is well known that apps can be used to introduce malware such as spyware and adware onto user's desktops. One recent example was the "Secret Crush" app, which ostensibly allowed users to find out of which of their friends "had the hots for them"[51] – but in fact was a conduit for adware. Facebook disabled the application for violation of its terms of service, but only after around 4% of Facebook users had installed it[52].

### C. Case study three: the Facebook Beacon, data collection and targeted ads

Facebook is a free service to users. It makes money, it appears, primarily via third party advertising served to its users. Since Facebook's value has been put at some $15

[49] ref , Threat SN.3 .
[50] Gross and Acquisti, supra n XX; Gross R "Re-identifying facial images", Carnegie Mellon University Technical Report, Institute for Software Research International, 2005.
[51] "Facebook Blocks Secret Crush over Adware row", *The Register*, 8 January 2008, available at http://www.theregister.co.uk/2008/01/08/facebook_blocks_secret_crush/ .
[52] Ibid.

billion[53] , it is clear these adverts must be a valuable income stream. (It is also clear that some revenue is accrued via extra services offered by Facebook, merchandising, sale of anonymised aggregate personal data, and allowing of access to the site to third party app developers, but these are probably not the main revenue-generators.)

Facebook's privacy policy[54] governs its self-imposed rules on collection and disclosure of user personal data. Facebook's policy, as of February 2008, says that : "*We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you.*" This leaves open the question of when exactly Facebook "believe" that you wish to share your information. However in practice Facebook, while allowing third party advertisers access to their site and to users, do not appear to date to be selling user information on in a non-anonymised form[55].

In late 2007, Facebook announced that it had formed a partnership with certain third party retailers in an enterprise called "Facebook Beacon". Facebook took information about user's activities on these partner businesses, and published the details on Facebook for everyone to see. So, for example, some users found a line on their profiles saying "X went to Amazon and bought *The Story of O*" (say) – something they might not want everyone to know, and certainly, in many cases, an embarrassing surprise. Some users were horrified at connections being made between their private purchasing habits and the "public" world of their SNS profile. Many users complained. 50,000 signed a petition asking Facebook to "stop invading my privacy". Facebook succumbed to user pressure in December 2007 and changed the system so that users had to explicitly "opt in" to having their details published by the Beacon system[56].

Were Facebook doing anything illicit here? According to both their own terms and conditions, and European data protection law, arguably they were in the right even before adopting "opt-in". Facebook had already apparently gained tacit user consent to collection of both explicit user personal data and user traffic data on its own site,

---

[53] See http://www.nypost.com/seven/10262007/business/myspace_love_facebook_value.htm. See also a fascinating discussion of Facebook's value and putative political values resulting, at http://www.guardian.co.uk/technology/2008/jan/14/facebook .

[54] See policy at http://www.facebook.com/policy.php, last visited 14 February 2008.

[55] Anonymised aggregate data clearly can be sold according to the policy. "Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are."

[56] See policy as noted at n 47 above : "Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collect certain information from that site and present it to you after you have completed an action on that site. You have the choice to have Facebook discard that information, or to share it with your friends."

via the blanket assertion that *"By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.*" These practices include:

"*When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us…When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies.*"

The policy of course only covers data revealed to Facebook not to the third party retailers. However it is likely those third parties had very similar policies in place.

Yet Facebook Beacon had apparently, again, violated the "reasonable expectation" of privacy of users. In DPD terms, although consent had been given to the collection of data, for what *purposes* had that consent been given? DPD (as the OECD principles do) rests on the notion of notice and choice: users are given notice not only as to what data is being colected but how it is to be processed, and it is this whole package to which they give consent. Would users who had given consent, say on both Facebook and Amazon have expected a result to be explict revelations on their profile about what they had been buying for the world to see?

Furthermore, even if legal consent *had* been obtained from users to any and every purpose or use, can such "consent" truly be regarded as informed and freely given, as the European DPD requires[57]? Consent as we noted above is meant to be a gate-keeping condition signifying agreement to terms and conditions. But here, consent is the price of access to Facebook itself.

It is well known that on many Internet sites, including SNSs, consent to terms and conditions is habitually obtained via an entry page tick box, which may often be already ticked. The EC Article 29 Data Protection Working Party has already strongly criticised such practices in its report in 2002: "*using pre-ticked boxes fails to fulfil the condition that consent must be a clear and unambiguous indication of wishes*[58]". Yet having to proactively tick a box is not much better. How many young people are likely to turn down the opportunity of entry to Facebook because of fears about a privacy policy they are unlikely to have read or understand? Research has showed repeatedly that small print online is rarely read and even more rarely understood. And as with employment contracts, such terms and policies are take it or leave it: never negotiable.

Regardless of these legal quibbles, however, Facebook, in the end, caved and instituted "opt in", not because they were threatened with legal action, but because Beacon was a public relations disaster, and users were prepared to leave the site if the worst excesses of Beacon were not curbed.

Beacon is, however, only the beginning of the story for imaginative use of personal data disclosed online via SNSs. Both MySpace and Facebook have announced plans

[57] Ref Art 2 DPD I think
[58] WP 114, 2002 at XXXX.

to use the large amount of personal data disclosed on their site, possibly combined with other personal databases, to allow advertisers to serve finely targeted ads to their users[59]. So, for example, a user who describes himself as male, single, living in London and 25 might find himself served with ads for local dating agencies rather than baby nappies. The idea of targeted context-sensitive ads is not new: indeed it has long been the basis of Google's successful AdWords programme where ads are served up alongside matched to the search term the user entered. A similar protocol has been adopted, with rather more privacy-activist resistance, on Google's Gmail[60]. SNSs however give advertisers unprecedented access to personal data, often highly sensitive, in a context where that data has been made visible for a quite different purposes than seeking advertised services – unlike on Google. In European and OECD terms, the data was disclosed and thus made available for collection for one purpose (networking) and has now been used for another (ads). Businessmen might argue that Facebook et al are merely adopting the obvious route to make money out of the service they offer for free. According to the Center for Digital Democracy and the US Public Interest Research Group , however, this "*sheer betrayal of trust, as youth-driven communities are effectively sold to the highest advertising bidders, threatens to undermine the shared culture of the Internet*[61]*."*

Striking an academic balance, again the main problem here seems to be the illusory quality of the consent collected by Facebook. Going back to the concept of "reasonable expectations of privacy", a user may well expect when they sign up for a free service like Facebook that they may have to receive ads of some kind to make it worthwhile for the site owner. (A similar expectation might apply to Gmail.) However they almost certainly do not fully understand or expect their personal data to be collected, mined, combined and sold to third parties to produce user profile data that may then be retained and distributed near indefinitely, and used to serve them with publicly visible adverts which they may find intrusive of their privacy. Interestingly, in the US the FTC has recently backed a tightening of the use of personal information regarding user behaviour to produce targeted ads in guidelines proposed in January 2008[62]. They suggest that "*every web site where data is collected for behavioural advertising should provide a clear, consumer friendly and prominent statement that data is being collected to provide ads targeted to the consumer, and give consumers the ability to choose whether or not to have their information collected for such purposes"*. If implemented, these guidelines might mean that in practice if not in theory US consumer law was more protective of the privacy of users on SNSs than currently implemented EC DP law. As we have noted throughout however, notice is of little value if users do not have a real marketplace of choices where there is an alternative to consenting to such disclosure for such purposes (or if regulation does not impose limits on the consequence of "choice").

The FTC proposals also suggest that where particularly "sensitive data" is collected for use in "behavioural advertising", such as medical details, then "explicit consent" should be required from the user. As noted above, this is in line with the letter of current EC DP law, but in practice, little or no distinction seems to be drawn between

[59] See eg http://www.itnews.com.au/News/64502,facebook-and-myspace-monetize-frienship-with-targeted-ads.aspx .
[60] refs
[61] Ibid.
[62] See

"ordinary" and "sensitive" personal data when consent is sought in the SNS world. (The definition of what is sensitive data has not yet been settled – the FTC proposals contemplate children's data being "sensitive" which is not one of the current EC catgories of sensitive data.[63]) Explicit "opt-in" consent was implemented by Facebook to deal with the Facebook Beacon problem, but when similar concerns were raised some months earlier about the opening up of Facebook profiles to Google and other search engine spiders, Facebook chose only to implement an "opt-out" regime[64]. In general, the level of actual or potential public dissatisfaction seems to be the determining factor in the type of consent obtained by an SNS site in relation to collecting or disclosing particular data, as opposed to any legally-driven taxonomy of the sensitivity of the particular information collected[65].

## IV. Data control issues on SNSs and possible solutions

The examples studied above illustrate that major problems exist in reconciling reasonable user expectations of data security and privacy with the "disclosure by design" paradigm concerning personal data on SNSs. Example 1 demonstrated that users tend to misperceive SNSs as a private rather than public space, leading to unfortunate and unintended disclosures of personal and sometimes sensitive data. Users are also often mislead as to what their "reasonable expectations of privacy" are on an SNS by the way the code has been written and defaults set. This makes SNSs a paradise for stalkers, ID thieves and marketers, just as much as law enforcement officials. Example 2 showed how even users who choose to disclose data carefully on SNSs tend to lose control of it and find it misused by third parties. Third party "apps" and photographs in particular are almost wholly not under the control of users. Finally, example 3 showed how the advertising model of "behavioural advertising" which is likely to be adopted on SNSs in the future is also worryingly out of the control of users. Users may be asked to give individual consents to collection of data on individual sites but need not be given an opportunity to allow or veto the processing of the digital dossiers of primary and secondary data which are generated, both from explicit revealed information but also from traffic data collected on SNS and other sites. The ENISA report on security names the aggregation of digital dossiers, and secondary (traffic) data collection, as the two main privacy related threats on SNSs today[66].

Examples 2 and 3 also illustrate how, underlying the obvious problems of privacy and disclosure on SNSs, is a more subtle issue: that of governance. SNSs are governed, like private spaces, primarily by contract in the form of EULAs, terms and conditions or privacy policies. They are not regulated as public spaces, by public regulation, with the public interest in mind. When we turn to *privacy* issues on SNSs, a policy choice presents itself starkly. If privacy is viewed as an aggregate social benefit, as

63

64 See discussion at http://impact.freethcartwright.com/2007/09/lets-not-forget.html .

65 See Wong R "Data Protection Online: Alternative Approaches to Sensitive Data?" Journal of International Commercial Law and Technology, Vol. 2, No. 1, 2007 Available at SSRN: http://ssrn.com/abstract=936391, which calls for a rethink on how "sensitive data" is categorised and regulated, especially in the context of the Internet.

66 ENISA Report, supra n X, p 8.

the likes of Regan[67] and Bennett and Raab[68] assert, then the a case for public regulation of SNSs to preserve societal privacy, even where individuals do not take proactive steps themselves, can surely be made. On the other hand if privacy is viewed purely as an individualistic right, for solely that individual's benefit, then it can arguably be legitimately left to the individual to assert and protect that right. A midway "consumer protection" camp might suggest that although privacy is primarily a matter for individual enforcement, some users are so ignorant or vulnerable that some public protective measures should be extended. Here it is of considerable relevance that SNSs are so often aimed at children and inexperienced young persons. This approach appears to be the one currently being pursued by the UK Information Commissioner, which has produced guidance on the use of SNSs targeted at young users only[69].

As matters stand, the real-world governance of SNSs by contract leaves the matter firmly in the latter camp. Individuals are left to give a formal indication of consent to privacy policies pre-dictated by the SNS and which can in general, also be changed by the SNS whenever they please. As Schneier[70] notes:

"*Facebook can change the rules whenever it wants. Its Privacy Policy is 2,800 words long and ends with a notice that it can change at any time. How many members ever read that policy, let alone read it regularly and check for changes?..[Facebook] can sell the data to advertisers, marketers and data brokers. It can allow the police to search its databases upon request. It can add new features that change who can access that personal data, and how.*"

This writer would stake her place in the first camp and agree with Regan that "*if privacy became less important to one individual in one particular context, or even to several individuals in several contexts, it would still be important as a value because it serves crucial functions beyond those that it performs for a particular individual. Even if the individual interests in privacy became less compelling, social interests in privacy might remain*.[71]"

Thus the debate about whether privacy should be publicly rather than simply privately regulated on SNSs can be located in the same discursive space as similar debates around other privacy invasive techniques to which formalistic "consent" is usually given such as employee surveillance, and data profiling and mining in the private sector, using devices such as credit card records, clickstream data and RFID chips. In the commercial sector, consumers often "voluntarily" trade privacy for convenience or for extras such as loyalty points, air miles, bargains, faster delivery times, etc. Such consent is however rarely fully informed and often not freely given, as in the context of employee surveillance.

---

[67] Regan P *Legislating Privacy: Technology, Social Values and Public Policy* (University of Toronto Press, 1995)
[68] Bennett C and Raab C *The Governance of Privacy* (2nd edn, 2007, Asghate), Chapter 2.
[69] See ICO 23 November 2007.
[70] Schneier on Security, September 21, 2006 at
[71] Supra, n 58, at p 212.

In Europe, data protection laws are explicitly founded on an individualistic concept of privacy as a constitutive human right[72]. Privacy is thus protected primarily by this notion of individual consent to processing of data[73]. But on SNSs the notion of consent fails as a gatekeeper protecting the privacy of users. Formal consent is given when a user signs up to Facebook, but with no vestige of choice or ability to negotiate conditions. The situation is even worse in example 2: as we saw, a user signing up to a Facebook "app" may not even have sight of terms and conditions before they are required to say yes. Finally the consent given by most or many SNS users, especially young and inexperienced persons – such as the student in example 1 – is almost always based on a misapprehension of risks. It is in human nature to want jam today – fun and frivolity – over jam tomorrow – safety and security in some murky future where relationships, job opportunities and promotions may be pursued. Much sociological and criminological literature has indicated that, universally, consumer perceptions of future versus current risks are fundamentally flawed[74].And it seems wrong that a one-time consent given today may prejudice that user for an indefinite future time, as is likely given the persistence of data on the Internet noted above.

The law is used to dealing with consent as a faulty risk management process in the context of consumer law. In consumer contracts terms are in the main imposed by the party with power – the business - upon the disempowered party – the consumer – regardless of whether there is an apparent formal consent given to those conditions by the weaker party. Such inequality of bargaining power is typically observed in standard form or "adhesion" contracts. Most jurisdictions have thus developed legal means by which contractual terms prejudicial to consumers imposed on them without true, informed or free consent can be declared void or unenforceable, or otherwise mitigated. In Europe, the primary means for this is the EC Unfair Terms Directive 1993[75], and in the UK, the Unfair Contract Terms Act 1976 as amended, and the Unfair Terms in Consumer Contract Regulations 1999[76]. In the USA, such protection is found in both common law and statute depending on the state in question, but terms in online consumer contracts have in the past been declared void or voidable on common law grounds such as unconscionability[77]. Means thus do exist to challenge unreasonable standard terms in SNS contracts. However it seems unlikely than a user would have reason to challenge such terms till after damage had been done by misuse of personal data, and even then it might be extremely hard to find causation between the misuse and the damage caused.

Control over SNS terms and conditions in order to protect user privacy, would, it is suggested, be far better exercised proactively by model contracts for SNSs, or industry or co-regulatory codes of conduct, rather than retrospectively by litigation. In the US, Facebook is unusual among the major SNSs in being signatory to TrustE, the

[72] DPD, Art 1.
[73] It is true that in fact the DPD does not favour consent over other practices which justify processing of data, such as the "legitimate interests pursued by the controller" (DPD 95, Art 7(f)). However both the recitals and surrounding documentation, and the use of "explicit" consent as the main criterion for processing of *sensitive* personal data indicate the conceptual if not legal primacy of consent. See recital 33, DPD 95.
[74] See further Apgar D *Risk Intelligence* (Harvard Business School Press, 2006); Rauhofer J " GIKII paper available at http://www.law.ed.ac.uk/ahrc/gikii/docs2/rauhofer.pdf
[75] 93/13/EEC: L 95/29.
[76] SI No 2083.
[77] See Coomb v Paypal case, Bragg v Linden Labs.

industry privacy seal program. This means in principle that Facebook's privacy policy is subject to third party review. However as EPIC, the Electronic Privacy Information Centre note in their briefing on SNSs and privacy[78], review by TrustE has not been satisfactory in the past, with members involved in well-publicised privacy scandals, and "TrustE has even been described as untrustworthy by certain commentators."

In the UK a number of bodies – including the Consumer Association, Which?[79], the ICO (as noted above)[80] and the government-sponsored Get Safe Online[81] campaign - have been active in promoting the idea of codes of conduct for SNSs; and the Home Office is reportedly in talks at time of writing with industry leaders such as Bebo about a more generalised code. Similar activity can be found in Australia[82] and Canada[83]. However in all these jurisdictions, more effort seems to have gone towards advising users how to act wisely on SNSs (an educational perspective), rather than in persuading SNSs to adopt rigorous, clear, consistent and non-oppressive terms in both their written documents and in – importantly- their *code*.

As noted in the introduction, the second strand of governance on SNSs – and arguably the most important form – is what the SNS software or code – in the Lessigian sense - allows the user to do. In example 1 above (the "Oxford case"), for example, we saw that the default code settings in Facebook allow anyone in a user's "Network" to see the personal details of any other user in this Network – sometimes with contra-intuitive privacy-invading consequences. In example 2, the code relating to apps forces users to give third party software providers access to all the personal data Facebook holds even where this is clearly unnecessary for functionality (how much data is needed to send a virtual bunch of flowers?). Similarly the code allows third party users by default the right to identify by tags photos of users on Facebook. Finally and significantly, in example 3 we saw how Facebook Beacon was originally introduced as a default choice and was later adjusted by code, after public outcry, to provide "opt-in" functionality.

Adjusting code is a far more effective privacy-protection mechanism than adjusting the text of contractual privacy policies, for the very obvious reason that conditions imposed by code cannot be "breached" as such (code can of course be hacked, but this is likely to be beyond the competence of most). Code is also a far more efficient way to regulate norms consistently in a transnational environment than law, even privately-ordered law such as contract. The same Facebook code can run in the UK and the USA enforcing the same privacy norms. By contrast privacy policies and terms and conditions may need adjustment to reflect individual national laws.

Is there an argument then for suggesting that codes of conduct should in the main prescribe *code solutions* rather than, as at present, mainly seek to modify contractual terms and/or user behaviour? The idea that software can adjust and regulate human and industry behaviour has of course been prevalent in Internet law circles since it

[78] Available at http://epic.org/privacy/socialnet/default.html .
[79] See
[80] Ref n X
[81] ref
[82] Ref Oz
[83] Can ref

was popularised by Lessig in 1999[84]. The particular influence of *defaults* in software is now also beginning to be recognised in legal scholarship. Kesan and Shah[85] have done extensive work in this area, and report on the extensive power defaults , and how they can be used and manipulated as a policy tool.

"*First, defaults provide users with agency. Users have a choice in the matter: They can go with the default option or choose another setting. Second, a default guides a user by providing a recommendation.*" And later "*Defaults are important not only in affecting a person's actions, but also in shaping norms and creating culture*[86]."

Kesan and Shah report also that defaults can *disempower* users. "*…default settings will be not be seen as defaults but as unchangeable. After all , if people don't know about defaults, they will assume that any alternative settings are impossible or unreasonable. The influence on people's perceptions of their control over software configurations is a core concern with software regulation*[87]."

Do defaults more empower or disempower online users of SNSs? In the consumer environment, it is an acknowledged fact that consumers as a population, especially in the online world, have a tendency to inertia. Put simply, many will not know that settings other than the default exist; many more will never try to find out, whether through ignorance, fear or simple lack of time or energy or imagination. Thus in the world of on-line spam, opt-out has proven to be useless as a means to reduce the amount of spam, and opt-in has accordingly been adopted by the EU[88], if not the US, as the legal default. In the SNS environment, anti-privacy pro-data collection software defaults may not only disempower users who do not know or care that these defaults can be changed, but also reify or reinforce a norm of less than adequate privacy protection on SNSs. Given the tendencies already noted above on SNSs towards "disclose now, worry about it later", this is a disturbing conclusion.

By contrast a voluntary or state-imposed code which required certain standards in default setting would produce a contrary influence: reinforcing a norm of adequate privacy protection. In all the examples given above, some thought about the effect of defaults could have produced a more privacy-protective result which was nonetheless compatible with the primary social networking focus of the site. In all these cases however, the income generation model of SNSs – disclosing as much data as possible for collection either by the SNS itself or third party partners – suggested a different model for the setting of defaults. It is thus apparent that some form of public regulation – whether by co-regulatory "soft law" codes or by the threat of mandatory legislation – would probably be necessary to persuade the SNS industry to move towards privacy-protective defaults. Nor, it should be stressed, is it impossible to imagine an SNS with privacy-protective defaults and a successful business model. Some already exist – often serving specialised privacy-conscious niches, such as

[84] See also, from a wide literature, Burk D L "Legal and Technical Standards in Digital Rights Management Technology" 2005 74 Fordham LR 537 and Reidenberg JR "Lex Informatica: The Formulation of Information Policy Rules Through Technology" 1998 76 Tex LR 553.
[85] 2006 Ref. See also 2003 paper.
[86] Ibid at 596.
[87] Ibid at 596-7.
[88] Ref Privacy and Electronic Communications Directive 2002. cf Can-spam act. See Edwards chapter in Edwards L ed *The New Legal Framework for Electronic Commerce* (Hart, Oxford, 2005).

SNSs for gay people, or certain religious groups -where privacy in relation to "outsiders", is as important as networking within the social group[89].

Given the industry profit drivers towards setting defaults at "maximum disclosure" and the privacy drivers towards setting them at "minimum disclosure", how should a code be drafted so as to reconcile these two interests? A third interest is of course that of the users themselves – what do they want? Why to network and make social relationships! Kesan and Shah suggest that one approach to determining defaults is to go with the "would have wanted" standard: what would the user and the SNS have agreed to if negotiation costs had been zero and so an arms' length rather than a standard form agreement had been negotiated? The trouble here is that, as we have already demonstrated, the user is likely to make unwise choices about their privacy in the SNS environment. They are not fully informed[90], nor are they in a good position to make risk assessments balancing social advantage against privacy risks – especially the young and vulnerable. Furthermore many users do not have the technical knowledge or ability to change defaults they might have agreed to as a starting point, but only on the basis they could later change their mind. As a result the "would have wanted" standard does not seem appropriate to SNS privacy defaults, at least without substantial amendment[91].

Beyond specifically pushing the code defaults already discussed in the examples 1-3 above towards a more privacy protective default setting, a number of general types of rules for software defaults in SNS sites might be worth debating.

*Automatic data expiry*. Mayer-Schoenberger[92] points out that in the non-digital world, data naturally dissipated over time. On the Internet however personal data persists, is retained, combined, disseminated and often becomes inaccurate. Could personal data profiles on SNSs be set to expire by default after six months or a year? Users could be warned by email and opt in to retaining their profile if that was what they wanted. This would address some of the problems of persistence of embarrassing personal data on the Internet years after its hasty disclosure.

*A general rule that privacy settings be set at the most privacy-friendly setting when a profile is first set up.* At first glance, this seems unreasonable. A Facebook profile at its most privacy friendly setting is not visible to anyone except its creator, and eventually, any users added as "friends" by the creator. Clearly this is not a desirable start state for social networking. However such an initial state would inform all users that privacy settings do exist, and force them to learn how to make use of them before they moved on to networking. It is unlikely, however, to be an option the SNS industry, or even users themselves, would favour.

*A general rule that personal data in profiles is "owned" by the user and cannot be manipulated by the SNS or third party users without their explicit consent*. This

[89] See for example kaioo.com, where privacy is seen as a key selling point: described at http://www.iht.com/articles/2007/12/02/technology/network03.php . In the UK, Bebo, a leading SNS for young children, individually and manually vets the user profiles of every one of its young user base, to provide privacy and safety guarantees (personal interview by Chris Marsden).
[90] See Kesan and Shah, p 619.
[91] Kesan and Shah themselves acknowledge cases when this is so: see ibid at XX.
[92] Ref "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing,"

would have the effect of giving users clear and explicit control over their "tagging" or identification by their photos, either on one SNS or across different sites, as discussed in example 2 above. It would also prevent the creation of, eg, the Facebook "NewsFeed", which has also been the subject of privacy-activist and user criticism[93], without explicit user consent.

*Code to allow portability and interoperability.* Such code would allow any user on any SNS to move to another SNS with all their data (and remove it permanently from the old site). Why would such code be privacy-promoting? As the ENISA report points out[94], because, at present, SNS interoperability is almost zero, there is a very high overhead on users shifting to a new site. As a result users will put up with a bad deal rather than make the effort of replicating all their personal data and "friends" connections elsewhere. Effectively, lack of portability of data and interoperability between SNSs, empowers the site owner and disempowers the user. Furthermore, because personal data has to be resubmitted every time a user decided to engage with a new software application providing social services (eg a photo blogging site; an instant messaging site; a calendar application) there is a strong tendency to make the "home" SNS" site your "data warehouse" and use its functionality for all your needs. As a result, personal data is all placed, increasingly, in one basket. Facebook has facilitated this tendency further with its extensive reliance on third party "apps" to make its site continuously fresh and appealingly novel. Finally when personal data is increasingly warehoused in one place, it becomes more vulnerable both to attacks by malicious hackers and "data grabs" by the government or litigators using subpoenas or equivalent. Although the technology may not be sophisticated enough, regulatory drivers towards portability and interoperability in SNS code would thus be likely to both empower the user and reduce their privacy invasion and security risks.

**Last thoughts?**

In conclusion, it is always possible that rather than rushing to generate industry compliance with "soft law" which mandates software defaults, or even considering legislation of a more traditional variety, we should be doing nothing at all. This is not because the problem is trivial – the above amply demonstrates it is not - but for a number of other reasons. First, it is becoming accepted wisdom that where technology appears to create social problems in the "web 2.0 society", legislating in haste often leads to getting it wrong and repenting at leisure[95]. Second, it is quite plausible that this is a blip problem. The youth of today who are currently enthusiastically giving away their personal data on the Internet will shortly grow into the young adult generation of tomorrow who are very well versed in how to manipulate the Internet and may have no difficulty in deciding when and where to use privacy defaults and similar controls. (This writer has her doubts, revolving around the general historical prevalence of consumer inertia and lack of information as to risks – but it is possible.) Certainly this appears to be the hopeful attitude many privacy commissioners and governments are taking, given the welter of educational advice appearing in various jurisdictions.

[93] Ref Danah Boyd. Schneier supra.
[94] ENISA report, supra n X, at
[95] See Professor Chris Reed's Manifesto for Inertia in a Web 20 World, blogged by the writer at http://blogscript.blogspot.com/2007/09/manifesto-for-inertia-in-web-20-world.html .

Finally, it is possible that the future these young social networkers will grow into will be one where privacy is simply no longer prized. The SNS phenomenon in itself, as much commented on above, shows a clear shift of values from prizing privacy to prizing disclosure and visibility in the social online space. (Nor is this merely an online phenomenon – observe the rise of the "famous for five minutes" generation, who will reveal anything from their sexuality to their unhappy childhood on shows like *Jerry Springer* and *Big Brother* to achieve a soupcon of celebrity.) We have already noted above, however, that commentators like Regan argue persuasively that even if privacy is not individually valued, it may still be of value to, and need protected by, society as a whole.

But even if privacy is no longer valued, surely privacy harms will still result from disclosure? Perhaps not in all cases. Anecdotal conversations with young people often reveal a fatalistic attitude, along the lines of "well by the time I'm looking for a job/promotion/partner, there will be so much data out there, that either everyone will have something embarrassing on their record, or else it will be impossible to sort through al the material on the Internet to check me out." Another version of this is that in time we will turn into a more forgiving, sympathetic society; if the eternal memory of Google remembers everyone's faults equally, we will have to, in turn, employers and lovers, colleagues and referees, forgive each other's sins for fear of being equally castigated. Time will tell if this sanguinity is accurate. Some privacy harms, it seems, will persist even in a more Christian with a small C society. ID thieves, cyber stalkers and civil litigants looking for evidence are probably not going to go away. Given this sad truth, a serious look at how we should regulate social networks to seek some compatibility between the human urge to be gregarious, and the human need (and right) to be private, seems urgently needed