Access to Personal Data in Social Networks: measuring the effectiveness of approaches to regulation

John David Haynes

Transfer Report from MPhil to PhD

City University London, Department of Information Science

October 2012

Revised 23rd October 2012

18,085 words plus title page, contents, abstract and appendices = total 36,476 words

Table of Contents

ABSTRACT

From 2003 when LinkedIn was launched and 2004 when Facebook started, online Social Networking Services (SNSs) have emerged as a major means of communication for social and business communities. Users enter into an agreement with providers when they sign up to online SNSs. In exchange for access to the features and facilities offered by the SNS, users allow exploitation of their personal data by the service provider. This is not always clear to users at the time and there is a widely-held perception that users are not adequately protected. In the UK, the Data Protection Act 1998 and the Communications Act 2003 provide regulatory frameworks for online services. This research sets out to test the hypothesis that law-based regulation alone does not provide adequate protection to users against the risks associated with use of SNSs. This research looks at the mechanisms by which a law-based regulatory framework has been put in place in the UK and compares this with other modes of regulation: self-regulation; regulation by design; and regulation by the way in which users behave. For instance, self-regulation occurs when SNS providers implement privacy policies. An example of design-based regulation occurs when SNSs have data encryption built into the development of their services to protect against unauthorised access to personal data. Users' behaviour regulates services by means of market pressure and by adopting safe practices such as opting out of general disclosure of personal data, for instance.

This research analyses the effectiveness of these four regulatory modes (Law, self-regulation, design and user behaviour) by assessing their impact on risk to users.

The research also examines attitudes of different stakeholders to the regulatory modes identified. The response of SNS providers and the extent to which they are influenced by legislation gives an alternative perspective on the effectiveness of legislation as a means of regulation.

Chapter 1 – Introduction

Background

In January 2010 Mark Zuckerberg, the founder of Facebook, is reported to have declared that the age of privacy was over (Johnson, 2010). In 2010 the default privacy settings for Facebook's then 310 million users were changed to make their profiles public. This caused an outcry and forced the company to revert to a private default, and to update its privacy policy.

Facebook, as a US-based company, is subject to the voluntary, self-regulatory Safe Harbor[1] scheme run by the US Department of Commerce. It is also subject to public pressure and this could be argued to be a form of regulation directly influenced by users. Are these two methods of regulation effective means of protecting personal data, or are there more effective methods that could be applied? For instance, does the legislative regulatory approach adopted in the UK with the Data Protection Act afford better protection of personal data?

One way of testing this is to compare the contrasting ways in which social media services, and specifically online social networking services (SNSs) respond to data protection regulation in the UK. There may be variations in attitudes to regulation and the different modes of regulation that may apply to this sector to protect users against misuse of their personal data. For instance, SNS providers who are based in the United States, and are members of the self-regulating Safe Harbor Scheme have adopted different provisions of the scheme (Connolly, 2008). Does this difference in approach make a material difference to UK users and are they exposed to greater risk as a result of non-compliance?

What is an online SNS?

Before going any further it helps to outline what is meant by online Social Networking Services (SNSs) and why regulation of access to personal data might be significant and topical. Online SNSs are internet services based on individual members who put up profiles (containing personal information) that are available to other users or members of the service. Users are able to link to other members to build up their own personal networks. This may include concepts such as: 'linking'; 'connecting'; 'following'; and 'friending'. In some cases personal profile information

[1] The US-based Safe Harbor regulatory regime operated by the US department of Commerce was set up to respond to the concerns of the European Union about protection privacy rights of citizens of member countries. The European Data Protection Directive requires minimum levels of protection for personal data of its citizens whether held in the EU or abroad. Potential trading restrictions can be applied to firms that do not comply with EU standards for data privacy. The Safe Harbor scheme is a voluntary, self-regulatory system – it does not appear to be independently managed, and there is no verification of the information provided by its participants.

may be limited to authorised members who have been specifically identified by a user as being part of their network. In other instances profiles may be available to all users of the service. At the most extreme end of this range, the information in personal profiles may be available to general internet users regardless of membership of the network service. The area of debate is around the release of personal data by the social network providers to third parties external agencies (such as advertisers and recruitment agencies) so that they can target their marketing. Tracking technologies such as cookies and beacons are widely used by social network providers to provide detailed information to commercial enterprises for behavioural advertising.

In a series of articles the Wall Street Journal describes the tracking technologies used by the most popular websites in the United States, including many of the largest SNSs (Angwin & Mcginty, 2010). Cookies are the most widely used tracker, and have been the subject of recent European legislation, implemented as a statutory instrument in the United Kingdom (*The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations*, 2011). A cookie is a small text file with a unique identifier that the website place in the user's browser to keep track of the online session. Many websites require cookies to operate effectively (they ensure the continuity of a session and can be useful if there is an interruption or if a user logs off and then logs back onto a website).

Where a website provider belongs to an advertising network or purchases the services of a tracking company, a third-party cookie tracks usage from site to site and records this data centrally for exploitation, by selling to advertisers, for instance. These advertisers, without necessarily knowing very much about an individual user, can target advertisements to them automatically. For instance a search of a travel site may indicate interest in visiting a particular city and subsequently ads for hotels in that city may start to appear in banner ads when browsing.

Persistent cookies have a public domain suffix which can be set up to recreate cookies that have been deleted from a user's browser. Cookies associated with Adobe Flash files can also re-install cookies.

Gathering all this personal data allows for extensive data mining by data aggregators. An alternative approach has been taken by Blue Cava, which has developed a very large database of all the devices on the Internet. It is constructed by creating a unique fingerprint of each device based on its settings detected by servers. Once a device has been identified it is possible to track online behaviour and to generate massive data sets that can be exploited by data mining techniques and by targeting services and advertising.

Other technologies include location-based tracking of mobile devices such as smart phones and data pads.

Sites without adequate security can be subject to scraping where an anonymous login allows access to the profiles of other members of the site, thus enabling the scraper to capture personal data without reciprocating.

Linking data gathered online with offline and published personal records (such as telephone directories or electoral registers) or blogs and tweets has also been reported in the press.

Research objectives

This research aims to describe the regulatory landscape and to compare the advantages and disadvantages of different modes of regulation. It will use a model of regulation based on an analysis of formal and informal measures to protect users from misuse of personal data. The research will use a combination of risk analysis and case studies to assess the relative effectiveness of different modes of regulation and to gain an insight into ways in which the regulatory landscape might be changed to protect users more effectively.

This work sets out to test the hypothesis that law-based regulation alone is not the most effective way of protecting users against the risks associated with use of SNSs. Risk assessments are used to compare the different modes of regulation. In order to test this hypotheses a number of research questions need to be asked:

- What methods are used for regulating access to personal data on online social networking services?
- What are the risks to users of having personal data on such services?
- How have law-makers responded to the inception and growth of these services?
- How have service providers responded to legislation?
- What effects do different regulatory methods have on risk to individuals?
- How does risk compare with other methods of assessing regulatory effectiveness?
- Is risk to users an effective method of comparing different modes of regulation?

Report structure

This report sets out to investigate the prior research in the area by means of a literature review (Chapter 2). Chapter 3 describes the work that has been conducted to date and the four research lines that emerged:

A. Reviewing the legislation

B. Investigating the privacy policies of SNS providers
C. Interviewing data protection experts
D. Developing a conceptual model

Detailed results of these lines are appended to this report. Chapter 4 discusses the findings from the research conducted to date and identifies potential avenues for further investigation, which are developed into a research plan in Chapter 5, which includes:

- identifying and measuring risks;
- assessing the effect of different regulatory modes on risk; and
- conducting case studies of SNS providers and workplace measures.

Chapter 2 – Literature review

Review methodology

Preliminary reading focused on the key texts in the areas or regulation, research methodology, and relevant legislation. Some of these texts were identified from academic departmental reading lists, and searches of library catalogues (notably the M25 union catalogue for academic and research libraries in and around London and the British Library).

Literature from peer-reviewed journals was identified by searching a range of aggregated electronic journals and bibliographic databases. They were chosen for their subject emphasis, comprehensiveness and the features that they offered:

GoogleScholar – general bibliographic database resource used as a starting point and as a 'catch-all' to supplement searches on more specialist systems
EBSCOHost – aggregated journals
Emerald – aggregated journals
World of Knowledge – social science and science bibliographic database including Social Science Citation Index
LexisNexis – comprehensive legal journals and news reports
ACM – informatics journals
UK and European legislation from www.legislation.gov.uk and http://eur-lex.europe.eu.

Key papers were identified by sorting on citation count coupled with an analysis of recent downloads for newer papers that may not have had time to build up a significant citation count.

Bibliographic search results were assessed for relevance by title and abstract. Where there was doubt, an assessment was based on examining the full text. The majority of journal articles cited in this review were downloaded as e-journal articles. Most books were read as hardcopies at the British Library, although in a few cases e-book versions were available and were downloaded.

Although this was a systematic literature review, some sources of information were identified by following references made by speakers at seminars and conferences, in blogs, on websites and via social media services. References identified in this way were tracked back to the original source and retrieved from peer reviewed journals or formal publications where possible.

Search strategies

The questions being investigated in the literature search were:

What methods can be used to regulate access to personal data on SNSs?

Can risk be used as a means of evaluating the effectiveness of different modes of regulation?

These are both large and complex questions and for the purposes of a literature review can be broken down into a series of literature search questions. This approach allows more comprehensive searching of the component concepts in the main questions and allows navigation and refinement to the specific question. The expectation is that the research question has not been expressed in this form before and that therefore there would be little literature specifically addressing the question. The focus of the literature review was on the following questions:

What are the risks associated with making personal data available via social networks?
How is access to personal data on social networks regulated?
How is the relative effectiveness of different modes of regulation evaluated?

Embedded within these questions are a number of concepts that require further exploration. These are addressed in the discussion below that considers each of the review questions in turn.

What are the risks associated with making personal data available via social networks?

The search is broken down into three concept areas as seen in Figure 1. Within each concept are synonyms that express that concept. In some cases truncation was necessary to spread the search scope. The process was iterative and the three concepts were combined using the Boolean AND operator to narrow the search down successively.

The core theme for this search was online social networking services. A general search (which will pick up some irrelevant material – such as 'offline' social networks) was narrowed down by introducing the concepts of risk and privacy. A manual trawl of the resulting items eliminated items that were not about the risks associated with personal data – for instance reputational risk to organisations where an employee defames a customer or a supplier or competitor using social media.

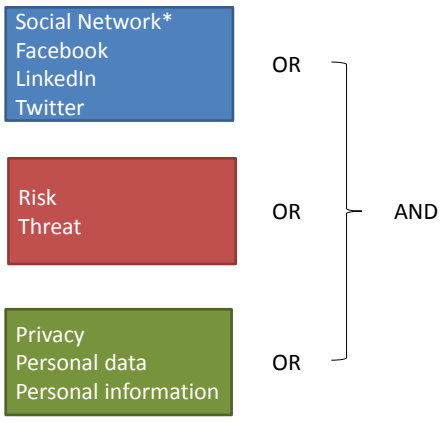


Figure 1 - Search query 1

How is access to personal data on social networks regulated?

The next search, Figure 2, combined the concepts of 'social network' with 'regulation'. This was narrowed down specifically to consider privacy and personal information to eliminate literature on copyright and social networks.

A key element of this research is to identify the different modes of regulation of access to personal data, with reference to social networks. For the purposes of this question 'personal data' is taken to mean data relating to an individual that can be uniquely associated with that individual. It refers to data that would not normally be in the public domain such as their political or religious views, information about their personal or private life, their personal finances and their behaviour or habits (this is particularly relevant to use of the internet in the workplace, as will be seen later on).

Personal data includes aggregated data as well as identifying data that can be associated with a specific individual, whether named or not.

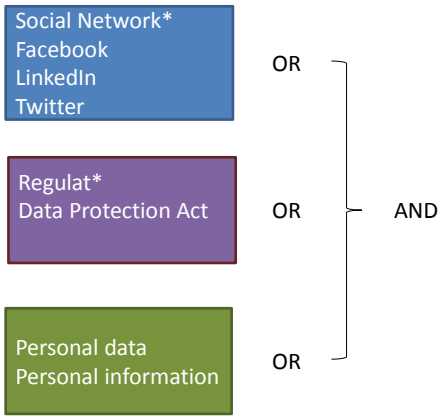


Figure 2 - Search query 2

How is the relative effectiveness of different modes of regulation evaluated?

The third question Figure 3 combines the concept of effectiveness/evaluation with regulation. There is a large, well-established body of literature on regulatory effectiveness and evaluation. The terms around 'evaluation', 'effectiveness' and 'assessment' were combined using the Boolean 'OR' operator before being refined by the 'AND' operator for combining with the concept 'regulation'.

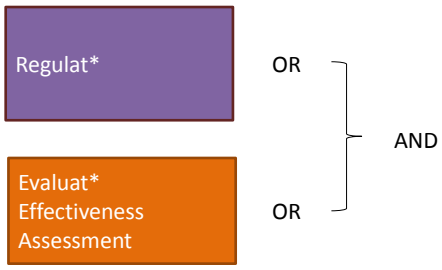


Figure 3 - Search query 3

Appraisal criteria

Where the search results were too broad, they were narrowed down to look at sources specifically relating to the UK, although care was taken not to eliminate literature about other territories that could provide comparative material for this study, or which might inform the methodology used for this study.

The scope of the searches focused on more recent material, mainly published from 2006 onwards, as this is when the current generation of SNSs emerged with the launch of Facebook etc. Apart from the paucity of literature about online SNSs before that date, this is a very rapidly evolving sector and older material is less likely to be relevant. Some exceptions were made for key references that are widely cited and which have had a strong influence on subsequent thinking. This particularly applies to regulation.

Bibliographic databases were selected for their subject coverage, with an emphasis on peer-reviewed journals. This was supplemented with hand-searching of key journals identified during bibliographic searches and by recommendation and searches for key authors. Selected key papers were also searched on ISI's Science Citation Index to identify subsequent references. These searches were repeated periodically to update the literature review.

Primary and secondary legislation were also directly accessed and commentaries on the legislation were referred to. There was a strong emphasis on monographs and multi-author handbooks for the legal literature in addition to peer reviewed literature, published reports and academic studies.

Context for this research

The nature of the problem

This research considers the nature of risk associated with use of online SNSs and focuses specifically on risks associated personal data on social networks. An internet user in effect makes a contract with an SNS provider when they sign up to a service. In exchange for providing personal data about themselves, they are given access to a range of services and features. They also benefit from having

access to the personal profile of others on the network. This may be tightly controlled, so that they can only see details of individuals who have given them permission to view their profiles, for example a reciprocal arrangement like 'friending' on Facebook or 'Join my network' on LinkedIn. The often less evident part of this equation is that in exchange for use of online SNSs, the service provider may sell on the personal data or access to personal behavioural data to third parties.

What is a social network?

With the widespread recognition of the power of social media as a marketing and promotion tool there is a plethora of guides and manuals on how to exploit social media for business success available (Clapperton, 2009; Comm, 2010). Some of the more authoritative guides provide a starting point for a common understanding of what social media are and how social networks fit into this sector. For instance The Social Media Management Handbook makes the distinction between social media, which have been around for millennia and digital social media, which have grown with the internet and which correspond to current usage of the term 'social media' (Wollan, Smith, & Zhou, 2011). Digital social media are described in terms of their characteristics:

Peer-to-peer communications
Content created and posted by users
Easy to use
Highly accessible, scalable and operates in real time
Public and transparent

Online social networking services (SNSs) can be characterised by their use and there has been a marked increase in their use between 2009 and 2011, mainly for social activities (89% of users) and with only 22% of users using it for informational activities (Dutton & Blank, 2011).

Kaplan and Haenlein identify six types of social media which they go on to classify according to social presence/media richness on one scale and self-presentation/self-disclosure on the other (Kaplan & Haenlein, 2010). This starts to address one of the fundamental issues of control of personal data, which is explored later on.

	Low social presence/media richness	**Medium social presence / media richness**	**High social presence / media richness**
High self-presentation/self-disclosure	Blogs	Social networking sites (e.g. Facebook)	Virtual social worlds (e.g. Second Life)
Low self-presentation/self-disclosure	Collaborative projects (e.g. Wikipedia)	Content communities (e.g. YouTube)	Virtual game worlds (e.g. world of warcraft)

(after Kaplan & Haelein, 2010)

Social networking services are placed firmly in the middle of the social presence / media richness scale and are classed as being high self-presentation / self-disclosure services. Kaplan and Haenlein go on to describe social networking sites as "*applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other*."

Cavazza divides social media into categories based on functionality of the sites (with some overlap for services with multiple functionality):

Publish – this is primarily for blogging, micro-blog, social stream services and wikis
Share – allows users to share externally sourced media, including material that they have created themselves
Discuss – bulletin boards and social search tools
Commerce – including reviews of services and tools for e-purchasing
Location – including event organisation and geo-location tools
Network – personal and professional networks of contacts
Games – social gaming, virtual worlds and casual gaming services.

(Cavazza, 2010)

This definition can be refined further by focusing specifically on social networking services which are a sub-set of social media. Boyd and Ellison make a distinction between social **networking** sites and social **network** sites. They define social networking sites (the subject of this research) as:

"*web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system*."

(D. M. Boyd & Ellison, 2007)

The main online SNSs covered by this research were selected on the basis of: their size, the fact that they offer a service in English, and their availability to UK users. They also meet the Boyd and Ellison definition of online social networking services:

Facebook
Windows Live Messenger
Habbo
Twitter
Gmail
Skype
Orkut
Bebo
Badoo

LinkedIn

(Wikipedia, 2011)

Exploitation of personal data

The term 'personal data' can have a variety of meanings. Schneier suggests that different types of personal data on social networks will require different measures to protect them (Schneier, 2010). He identifies the following categories of personal data (with some degree of overlap) that can be used as a typology of personal data:

Service data – data provided to the service provider to set up your account
Disclosed data – what you put up on your profile, this may include content that you have created
Entrusted data – like disclosed data, but is personal data that you have provided for 'friends' contacts' sites on the social network service
Incidental data is data that other people post about you – which may include text, photos or moving images
Behavioural data is data that the site collects about your behaviour on the internet, this may be restricted to the SNS, or may be based on monitoring your use of other web sites.
Derived data is derived from other personal data to make assumptions about you, your views or behaviour (or from a third party source such as a published directory)

A great deal of recent attention in the press has been devoted to behavioural data, which users may not have provided explicit, informed consent to use. The permission may be hidden in the terms of service that a user signs up to in order to gain access to the service. This information may then form the basis for intrusive advertising directed at the user when they open their browser. A series of articles in the Wall Street Journal by Julia Angwin and colleagues describes tracking technologies and some of the issues that arise, including privacy concerns (Angwin & Mcginty, 2010).

The idea of privacy

In defining privacy Warren and Brandeis quote from Judge Cooley, who spoke about privacy as: "*the right to be let alone*" in response to the growth of photo-journalism in the United States (Warren & Brandeis, 1890). Their argument was that common law provides a basis for protection of personal privacy. They stated "*The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*". They went on to state that "*...the individual is entitled to decide whether that which is his should be given to the public*".

In Warren and Brandeis's view there are limitations to the right to privacy, particularly in relation to public good and they acknowledge that "*To determine in advance of experience the exact line at which the dignity and convenience of the individual must yield to the demands of the public welfare or of private justice would be a difficult task*" (Warren & Brandeis, 1890). They argue that many of the laws already then available afford degrees of protection against invasion of privacy – such as

copyright law for publication of photographs or literary works, or the tort of breach of trust by publishing confidential information, or breach of implied contract where private information made available in the course of delivering a service is then made public. They enumerate some useful principles that help to define the scope of what they mean by "*the right to privacy*:

> *"The right to privacy does not prohibit any publication of the matter which is of public or general interest.*
>
> *The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.*
>
> *The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage*
>
> *The right to privacy ceases upon the publication of the facts by the individual, or with his consent.*
>
> *The truth of the matter published does not afford a defence.*
>
> *The absence of "malice" in the publisher does not afford a defence."*

Wacks contends that there is no right of privacy by statute in UK and that protections arise from common law (Wacks, 2010). That said, it could be argued that privacy is provided for in a number of UK General Public Acts including: the Data Protection Act 1998, the Communications Act 2003 and the Human Rights Act 1998. These are discussed in more detail in Appendix B.

One of the earliest privacy cases in England and Wales was Prince Albert v Strange, where the Prince Consort sought to prevent the publication of a catalogue etchings made by him and the Queen. The High Court found:

> *"The question here is, how far the publication of this Catalogue is in violation of the law? That there is property in the ideas which pass in a man's mind is consistent with all the authorities in English law. Incidental to that right is the right of deciding when and how they shall first be made known to the public. Privacy is a part, and an essential part, of this species of property. In Millar v. Taylor, the property which a man had in his unpublished ideas was admitted by all the Judges: Donaldson v. Beckett."*

("Prince Albert v. Strange," 1849)

Since then some commentators have distinguished between 'information privacy' and wider definitions of privacy. For example Westin includes in his definition of privacy: "*the claim of an individual to determine what information about himself or herself should be known to others*" (Westin, 2003). This is a theme comprehensively addressed in Smith, Dinev and Xu's review of Information Privacy Research (Smith, Dinev, & Xu, 2011). They make the distinction between physical privacy, which "*concerns physical access to an individual and/or the individual's surroundings and private space*" and information privacy, which "*concerns access to individually identifiable personal information.*" In their analysis of research the authors suggest that much privacy research has measured privacy concerns "*because of the near impossibility of measuring privacy itself*" (Smith et al., 2011). Privacy concerns include beliefs, attitudes and perceptions about privacy. This in turn may be informed by the experiences of individual, their awareness of privacy issues, personality differences, as well as demographic differences and the general culture or climate within which they live. They developed the ACPO macro model that suggests the relationship in privacy research: Antecedents → Privacy concerns → Outcomes. They point out the current privacy research rarely considers outcomes (i.e. changes in behaviour or of state) as a result of privacy concerns.

There have not been many cases in the UK courts about breaches of privacy or other damages resulting from disclosure of personal data on SNSs. In Applause Store Production Ltd & Anor v Raphael, where the defendant had created a personal profile of the claimant on Facebook containing some true information and some defamatory material the court found:

> *"It is reasonably clear that damages in cases of misuse of private information are awarded to compensate the claimant for the hurt feelings and distress caused by the misuse of their information: see for instance McKennitt v Ash [2006] EMLR 178 [162]."*

("Applause Store Productions Ltd. & Anor v Raphael," 2008)

Malhotra et al looking at internet users' information privacy concerns developed a multi-dimensional grid of privacy, following surveys of internet users, based on:

- Collection of data – gathering of individual specific data by sites
- Control – whether users have the choice of opting out, for instance
- Awareness of privacy practices – knowing how the data will be used

(Malhotra, Kim, & Agarwal, 2004)

An IP address, which can be attributed to an individual, can be regarded as personal data:

"If one considers the definition of personal data provided in Article 2 of Directive 95/46/EC, 'any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number' (18), it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data in all cases relevant here."

(Hustinx, 2010)

Westin suggests that privacy issues are different in democratic and authoritarian societies (Westin, 2003). It is not clear whether this is a qualitative difference or a matter of degree. It could be argued that in both types of society there is a balance between individual autonomy and public good.

If the UK is assumed to be a broadly democratic society, then the balance would tend towards individual autonomy. However, the UK's Draft Communications Data Bill, 2012 is perhaps a reflection of the move towards a more authoritarian society with greater emphasis placed on security at the expense of individual privacy (Home Office, 2012). The Bill makes provision for monitoring of social networking activity as well as other telecommunications traffic can be used to counter terrorist plots.

According to Lessig there are three different concepts of privacy that affect any considerations of regulation in this area:

Preserving dignity

Minimising intrusion

Constraining the power of the state to regulate

(Lessig, 2006)

Solove argues that information confined to a group should be considered private, even if that group is quite large (Solove, 2007). This could also apply to groups on the internet. In his view if a member of the group makes the information available beyond the group that is a breach of privacy: "*when information is contained within a particular group and a person causes it to leap the boundary, then this is a privacy violation even if the original group is large*."

The OxIS 2011 survey, found that nearly half of those surveyed thought that "*the current use of the internet is a threat to privacy*" (Dutton & Blank, 2011). However a large number of respondents

were happier to give out sensitive personal data. Next Generation Users[2] were less likely (42%) than non-users and ex-users (63%) to consider the use of computers and the internet a threat to privacy.

For gathering personal data Christiansen distinguishes between "*a user's voluntary sharing of such information*" and "*involuntary/uninformed collection by other parties*" (Christiansen, 2011). She goes on to describe three types of data collection:

> *"1. Collect personal data, then anonymize and aggregate it to sell to third parties and/or for use internally*
>
> *2. Collect personal data, keeping personal data within the company but providing the opportunity for advertisers to specify a certain range of traits for target marketing*
>
> *3. Collect personal data with the intention of selling the information, sometimes including specific profiles or names, to third parties"*

She also identifies some of the ways in which personal data can be used or misused, although this is far from comprehensive:

- *"Running of background checks by employers for hiring decisions;*
- *Pricing and assessing risk of injury or death by insurance companies (based on Internet searches, blogs, and confidential online support groups, for example);*
- *Termination decisions by employers (for example, if a user is criticizing the workplace or found to be lying to the employer);*
- *Recruiting and scholarship decisions by athletic coaches;*
- *Searching for relevant evidence by attorneys in the course of case preparation;*
- *Detecting political leanings for fundraising purposes and to target individuals who are undecided on an issue or a candidate; and*
- *Facilitating criminal attacks."*

(Christiansen, 2011)

---

[2] Next Generation User "...someone who accesses the internet from multiple locations and devices. ...someone who uses at least two internet applications ... on their mobile or who fits two or more of the following criteria: they own a tablet, own a reader, own three or more computers." (Dutton and Blank, 2011, p4)

These can be addressed by legislation, by means of 'do not track' lists (rather like the telephone preference service) and 'do not track' features added to web browsers. Finally Christiansen advocates better public education as a key means of reducing the risks associated with use of social media.

An alternative view suggests that too much privacy is a bad thing because it inhibits delivery of free services to users (Hammock & Rubin, 2011). Hammock and Rubin argue that the benefits of free services outweigh the costs of identity theft and other risks to which users might be exposed. In their view there is no economic argument based on data for increased privacy. The cost of internet fraud is estimated at $28bn per annum in the US and Europe, but the benefit of free services based on provision of personal data is estimated at $100bn, a substantial economic surplus.

This approach reduces privacy and access concerns to a simple economic argument and requires a lot of assumptions to be made on the value of economic benefit or loss associated with use of personal data. It does not take into account the potential loss of income associated with personal ownership of data. Tene and Polonetsky focus on data that has been aggregated and anonymised. They argue that the cost of protecting personal data to prevent re-identification would mean that "*many beneficial uses of data would be severely curtailed*". They suggest further research for one strand of this investigation: "*We call for the development of a model where the benefits of data for businesses and researchers are balanced against individual privacy rights*" (Tene & Polonetsky, 2012).

Risk

The focus on risk is one element of this research project. The English word 'risk' is derived from the Italian verb 'riscare' to run into danger. It acquired its commercial meaning in the 18th Century when it was applied to insurance losses. Since then, the usage of the word 'risk' has moved away from the idea of a measurable hazard calculated on probability and size of loss, to a more nebulous range of uses encompassing more subjective assessments of likelihood and impact. It is applied extensively in project management and in general management of organisations as well as in more traditional commercial environments such as banking.

A UNESCO Workshop identified risk as a significant area of potential research in information and communication studies. The report stated:

> *"Research is needed on the potential of digital communication and information networks to produce data about all human activity and with respect to all people.*
>
> - *How can we evaluate the impact of the development of computing and artificial intelligence needed to engage in surveillance?*

- *What is the potential for the (mis-)use of such data by government institutions or private enterprises?*

- *What are the dangers or risks to the public interest?"*

(Mansell, 2008)

Fischhoff et al suggested that it is often difficult to be objective in the assessment of risk:

> "*Within the philosophy of science, 'objective' typically means something akin to 'independent of observer'. That is, any individual following the same procedure should reach the same conclusion. However meritorious as a goal, this sort of objectivity can rarely be achieved. Particularly in complex, novel areas, such as risk analysis, research requires the exercise of judgement.*"

(Fischhoff, Watson, & Hope, 1984)

They go on to say: "*Thus, objectivity should always be an aspiration, but can never be an achievement of science*." They argue that researchers need to state what dimensions of risk they are considering: "*an analysis of 'risk' needs to specify which of these dimensions will be included. In general, definitions based on a single dimension will favour technologies that do their harm in a variety of ways (as opposed to those that create a lot of one kind of problem).*" In other words the way of measuring each dimension of risk will have an effect on the overall assessment of risk and as they state: "*Evaluating it fairly requires knowing what it was intended to accomplish.*" The steps needed to do this, they suggest, are: to decide which consequences to include, the development of a risk index based on different risk attributes, identification and application of simplifying assumptions to make the problem 'tractable'. The different attributes for a technology make up a vector which can then be turned into a single number. The authors argue that "*Developing a definition of risk requires a variety of explicit value judgments*." (Fischhoff et al., 1984)

Aven and Renn review a number of definitions of risk before arriving at a new definition of risk that addresses some of the concerns they raise about lack of precision and the need to separate risk measurement and the decisions on the response to risk:

> "*Risk refers to uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value.*"

(Aven & Renn, 2009)

They point out that "*The assigned probability and judgements about risk tolerability or acceptability are different dimensions, or separate domains in the world of risk professionals who make a clear distinction between risk assessment and judgement of acceptability.*" This allows for a qualitative approach to risks where probabilities or outcomes cannot be quantified. They conclude by stating that: "*Our proposed definition provides a conceptually consistent and practically compatible concept of risk without falling into the extreme of total subjectivism and relativism but also not pretending that risk is a measurable object similar to other physical entities.*"

Objectivity or subjectivity is a theme taken up by Hansson, who concludes that "*risk is both fact-laden and value-laden and that it contains both objective and subjective components.*" He suggests that: "*The real challenge is to identify the various types of factual and valuational components inherent in statements about risk and to understand how they are combined.*"

(Hansson, 2010)

There is a considerable body of research into risk and the internet and significant studies on risk associated with SNSs. Much of this focuses specifically on risks to children – an area that raises specific issues about vulnerability and this is beyond the scope of this study. The focus here is on risks associated with use of SNSs by adults and on ways of measuring those risks.

The Oxford Internet Institute is conducting a longitudinal survey OxIS which regularly surveys public attitudes to the internet and perceptions of risk. A recently published OxIS report describes the paradox of increases of bad experiences on the internet and an increasing trust in the internet (Blank, 2010). In other words bad experiences do not seem to undermine trust in the internet. It is suggested that the most experienced users of the internet are more likely to have a bad experience but are better able to cope with problems that arise, because they are more experienced

Weiss suggested that there needs to be a shift away from privacy-enhancing technologies that concentrate on access protection, anonymity and unlinkability. He advocates a move toward privacy safeguarding measures that enable greater transparency and that facilitate context and purpose limitation to personally identifiable data (Weiss, 2008). The author suggests privacy enhancing technologies should be combined with new safeguarding methods for Web 2.0 applications.

Regulation

The following factors have affected the rise of regulation in the UK:

- Crisis and scandal
- European Union - culture of greater regulation
- Power and Democracy

(Moran, 2005)

One of the purposes of regulation is to control risk. In the introduction to the Better Regulation Commission's report, the Chairman states:

> *"Our specific recommendations are, tough, for Government, and the most important of these calls is for our leaders to redefine our approach to risk management in a number of ways:*
>
> > *Emphasising the importance or resilience, self-reliance, freedom, innovation and a spirit of adventure in today's society;*
> >
> > *Leaving the responsibility for managing risk with those best placed to manage it and to embark on state regulation only where it represents the optimum solution for managing risk;*
> >
> > *Re-examining areas where the state has assumed more responsibility for people's lives than is healthy or desired; and*
> >
> > *Separating fact from emotion and emphasising the need to balance necessary levels of protection with preserving reasonable levels of risk."*

The report goes on to identify five principles of good regulation:

- Proportionality "*regulators should only intervene when necessary. Remedies should be appropriate to the risk posed and costs identified and minimised*"
- Accountability "*regulators must be able to justify decisions and be subject to public scrutiny*"
- Consistency "*government rules and standards must be joined up and implemented fairly*"
- Transparency "*regulators should be open and keep regulations simple and user-friendly*"
- Targeting "*regulation should be focused on the problem and minimise side effects*".

(Great Britain. Better Regulation Commission, 2006)

These principles apply to government regulation and specifically regulation that is based on legislation. However some of these principles could be applied to other modes of regulation including self-regulation and technology-based regulatory measures. Haythornthwaite suggests that government regulation should be based on a sound risk assessment and not be subject to public opinion, pressure groups and politics. However he recognises the need for a conversation between different interest groups in order to arrive at workable regulation. The administrative costs of regulation, 'red tape', is estimated at £30 – £40 billion a year in the UK. This is in addition the cost of lost opportunities and non-financial costs such as: erosion of personal responsibility, loss of trust. This suggests that regulation should only be used where absolutely necessary. Haythornthwaite puts forward the principle that government should not regulate where the individual taking the risk is the

only one that can be harmed (Haythornthwaite, 2006). This suggests that in the recent regulatory environment, legislation may not have been considered the best way of protecting users against risk.

In light of recent developments in the financial markets, the balance may shift back towards greater regulation. (Heffernan, 2011; Slattery & Nellis, 2011)

Regulating the internet

There are a variety of modes for regulating the internet generally and SNSs in particular. Ofcom identified the following types of regulation in relation to the internet:

- Personal responsibility – regulation by individual users
- Self regulation – regulation by site owners and content providers
- Self regulation – regulation by internet service providers
- Statutory regulation

(Ofcom, 2009)

An alternative view of regulation can be described in terms of a response to risk, and in particular risk associated with loss of privacy. Lessig identifies two main threats to privacy from the internet:

> *"The first is the threat from 'digital surveillance' - the growing capacity of the government (among others) to 'spy' on your activities 'in public'...The second threat comes from the increasing aggregation of data by private (among other) entities. These data are gathered not so much to 'spy' as to facilitate commerce." p223*

He identifies four modes of regulation, which he uses to mean "constraint" as responses to these risks:

> "*Against these two different risks, we can imagine four types of responses, each mapping one of the modalities that I described in Chapter 7:*
> *Law...*
> *Norms...*
> *Markets...*
> *Architecture/Code*..." p234

(Lessig, 2006)

These models of regulation can be consolidated into a single model (discussed in Chapter 4) which will form the basis for this research:

1. Legislation
2. Self-regulation
3. Design

4. User behaviour

The literature for each of these regulatory modes is considered in turn:

Legislation

A review of legislation and the resulting statutory regulation must take into account the nature of the UK constitution which governs the role of the different branches of government, including the legislature and the judiciary. Bogdanor argues that the current round of constitutional reform started in 1997 and the UK's entry into the Common Market in 1973 has effectively replaced one constitution with another (Bogdanor, 2009). He also argues that this is an on-going process. Recent changes include: devolution; home country legislatures and the London Assembly; PR in devolved administrations; and European elections. Other significant developments that affect the regulation of access to personal data include: Human Rights Act 1998, reform of the House of Lords, Freedom of Information Act 2000, the regulation of political parties and electoral expenditure, and the Constitutional Reform Act 2005 which makes the Lord Chief Justice (not the Lord Chancellor) head of judiciary.

Bogdanor argues that Britain has an uncodified constitution making it more difficult to follow changes to the constitutional order:

> *"A society is distinguished from a mere conglomeration of individuals in that it comprises a group of people bound together by rules; and a constitution is nothing more than a collection of the most important rules prescribing the distribution of power between the institutions of government - legislature, executive and judiciary - and between the individuals and the state".*

He suggests that under the Human Rights Act 1998 judges are likely to play a more important role in defining rights (Bogdanor, 2009). One purpose of a constitution is to protect minorities against the majority, which is what the Human Rights Act 1998 does. It is based on a European Convention and is part of the package of membership of the EU. Formerly sovereignty of parliament was the dominating principle in the UK's constitution; and hence a written constitution was deemed unnecessary. Now other factors are important and sovereignty of parliament is not the only consideration. Although the author argues in favour of a codified constitution, he advocates this as a process.

The Human Rights Act 1998 enshrines "*the right to respect for private and family life*". The other relevant piece of legislation is the Data Protection Act 1998 and Statutory Instruments derived from the Act and the equivalent European Directives. These two pieces of legislation are described in the chapter on legislation.

Oppenheim gives an early account of legislation relating to the internet and other electronic environments. In his chapter on Conflict of Laws (Chapter 9) he asks which law applies to a service based in one country but delivered to a user in another. He puts forward the idea that cyberspace should have its own jurisdiction and that its laws would apply to any transactions that took place in that space (Oppenheim, 2001).

Lessig's argument develops this theme to suggest that the norms and laws of both physical and cyberspace apply:

> "*We have this desire to pick: We want to say that they are either in cyberspace or in real space. We have this desire because we want to know which space is responsible. Which space has jurisdiction over them? Which space rules? The answer is both. Whenever anyone is in cyberspace, she is also here, in real space. Whenever one is subject to the norms of a cyberspace community, one is also living within a community in real space. You are always in both places if you are there and the norms of both places apply. The problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once*." p298

(Lessig, 2006)

Self-Regulation

Self-regulation by users of their use of the internet falls within the scope of user behaviour, which is considered later in this chapter (LaRose, Lin, & Eastin, 2003).

Haufler defines self-regulation as:

> *"Self-regulation occurs when those regulated design and enforce the rules themselves".*

(Haufler, 2001)

One of the most prominent self-regulatory regimes affecting the social media services used in the UK is the EU Safe Harbor arrangements with the Federal Trade Commission. Although governed by Treaty, it is a voluntary arrangement with no external verification of registrations required. This has been reviewed previously and many concerns were raised about inconsistent and inaccurate registrations, as well as the very loose compliance requirements (Connolly, 2008).

There has been some reaction against self-regulation following the financial crisis of 2008 and its aftermath, which was widely perceived as a failure of self-regulation (Slattery & Nellis, 2011). Even before the crisis some commentators were suggesting that self-regulation is ineffective on its own (Collins, 2006).

Cannataci and Bonnici examine self-regulation by Internet Service Providers (ISPs) and point out that self-regulatory approaches are constrained to some degree by national boundaries. This could also apply to SNSs (Cannataci & Bonnici, 2003).

The European Union has seen a move to co-regulation, where the responsibility for regulation is placed on the regulated industry, but with supervision by the state. This is sometimes referred to as "regulated self-regulation" and can be characterised as a combination of law-base or state regulation and measures taken by industry (self-regulation) (*Study on Co-Regulation Measures in the Media Sector. Final Report*, 2006).

Privacy policies are another manifestation of self-regulation by industry. An initial investigation of the privacy policies of the largest SNS providers is described in Appendix C.

Design

Reidenberg first put forward the idea of 'Lex informatica' where the structure and architecture of cyberspace became a means of regulating it (Reidenberg, 1998). In Code 2.0 Lessig states:

> *"In real space, we recognize how laws regulate – through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates – how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is."*

(Lessig, 2006)

In other words *"code is law"* in Lessig's catch-phrase. He goes on to argue that it is possible to build systems to reflect the values that are considered important or fundamental. Indeed it is impossible to avoid reflecting some values in the build, architecture or coding of cyberspace. Later he says: "*There is regulation of behaviour on the internet and in cyberspace, but that regulation is imposed primarily through code*." For example "*code that encrypts regulates to protect privacy*".

The code itself can be regulated (e.g. the US government requirement that it have access to encryption codes built into any system) as well as being an agent of regulation. He terms these East Coast code (e.g. laws enacted in Washington DC) and West Coast code (system design and architecture based in Silicon Valley).

Lessig goes on to look at the way in which code regulates privacy on the internet. Zittrain talks about loss of control over personal data (Zittrain, 2008). Lessig argues that the interests threatened by breach of privacy are diffuse and disorganised (unlike the copyright interests that are also affected by the internet). There are compelling interests arrayed against privacy interests, namely national security. Zittrain suggests that this is reason why privacy legislation in the US is relatively neglected

compared to copyright legislation. One solution might be his view that "*the protection of privacy would be stronger if people conceived of the right as a property right.*"

(Lessig, 2006)

Recognition of the importance of system architecture in regulation is seen in the Information Commissioner's 'Privacy by Design' initiative, an example of regulation by code (*Privacy by design*, 2008). The principle is that any system or service that is established should consider privacy issues from the initial design stage onwards, rather than being tacked on as an afterthought.

User behaviour

User behaviour is expressed collectively in societal norms and in market behaviour, as well as individually.

Norms regulate services by creating default ways of working. For instance, there is a developing norm that users should be able to opt in to sharing their personal details with advertisers, rather than having to opt out.

Instead of regulation Tene and Polonetsky argue that "*Policymakers should engage with this normative question, consider which activities are socially acceptable, and spell out the default norms accordingly*" (Tene & Polonetsky, 2012). They go on to suggest that risk analysis is a more rational basis for data protection than data minimisation (i.e. only collecting that data that is directly necessary for the original purpose is was gathered for.

Solove describes privacy in terms of social network theory and the norms that apply:

> "*Social network theory often focuses primarily on connections, but networks involve more than nodes and links. There are norms about information sharing that are held within certain groups, such as norms of confidentiality*."

(Solove, 2007)

Regulation by the market e.g. demand by consumers is affected by privacy concerns. Evidence seen in the responses to Facebook over changes to the privacy settings. However it is difficult to separate this from the changes that took place as a result of pressure from regulators such as the Canadian Privacy Commissioner (Denham, 2009).

Lessig dismisses the idea of the market as a means of protecting personal privacy on the internet (Lessig, 2006). However other commentators have suggested that a market for personal data is beginning to develop (Yassine, Shirehjini, Shirmohammadi, & Tran, 2012). This could in future

become an effective means of regulating access to personal data, or a means of protecting personal privacy on social networks.

Is some form of feedback mechanism possible so that systems regulate themselves? Parallels can be seen in biological regulation where for instance increased blood sugar leads to a rise in insulin production which lowers the blood sugar level, which in turn is detected by the body which responds by reducing the production of insulin. An auto-regulatory system (not to be confused with self-regulation, which in this context means regulation controlled by the bodies being regulated rather than an independent third party) might be an interesting avenue to explore and may be one of the characteristics of regulation by the market (Lessig, 2006).

The Information Commissioner in the UK has actively educated users to take responsibility for protecting their own privacy. User education was also seen as one strand of an effective strategy for avoiding some of the risks associated with online SNSs. This is a reflection of Dry's historical analysis of risk and regulation and the benefits of individuals taking greater responsibility for risk assessment (Dry, 2007). This could be seen as a possible mechanism for regulation by the market. Users' behaviour is modified in response to perceived risk, affecting the demand for SNSs.

Mixed approaches to regulation

Lessig argues that combinations of the four modalities protects the individual: "*Here again, then, the solution is a mixed modality strategy. As LAW creates the incentive for a certain change in the CODE of spam (it now comes labelled). That law is enforced through a complex set of MARKET and NORM-based incentives*". p. 267.

(Lessig, 2006)

Solove draws parallels between privacy and copyright and suggests that there has to be a balance between freedom and control of information (Solove, 2007). He concludes (p190) that "*We are witnessing a clash between privacy and free speech*" and suggests that (in the United States) "*we can rework the law to make it a useful instrument in balancing privacy and free speech*". He suggests that lawsuits provide a middle ground between a libertarian approach (leaving law out of considerations of privacy) and "*An authoritarian approach which involved direct restrictions on internet expression*". In his view the law should recognise the variety of situations where privacy is a consideration and it "*should also increase its recognition of duties of confidentiality*" (p191).

Social norms are a powerful means of regulating behaviour and can be a strong alternative to resorting to legal remedies. To some extent social norms also drive legislation by placing pressure on law-makers as well as on those administering the law.

Finally Solove (p200) advocates parties working out disputes between themselves without resorting to the law and refers to Lessig and Reidenberg's view that technical architecture can be used to protect privacy (Solove, 2007; Weber, 2002).

Spinello takes up Lessig's theme of modes of regulation and questions whether special regulation is needed for the internet, the so called 'law of the horse'. This is a debate about whether special legislation is needed for the internet – termed "the law of the horse" (i.e. if special laws are not required for horses, why is one needed for the internet?). Spinello concludes that this is not the case (Spinello, 2006).

So what of the United Kingdom? Buckley Owen et al point out that the lack of a national information policy in the UK means that responsibility for regulating information and communication services falls across several different agencies (Buckley Owen Cooke, L., Matthews,G., 2012). The one most directly concerned with regulating access to personal data on social networks is the Information Commissioner's Office, under the terms of the Data Protection Act 1998 and discussed in detail in Appendix B.

Lofstedt et al argue that the relationship between public and regulators has changed over the last 20 years (Lofstedt, Bouder, Wardman, & Chakraborty, 2011). Several major scandals have led to greater public distrust. This has resulted in a shift from a consensual style of regulation to a model based on public participation, transparency, and more powerful non-governmental organisations (NGOs).

Lessig's view is that a combination of law, norms and architecture/code is the most effective means of regulation of privacy on the internet (Lessig, 2006). He does not believe the market is an effective regulator in this instance and concludes "*Collective action must be taken to bend the architectures towards this goal* [protecting privacy], *and collective action is just what politics is for. Laissez-faire will not cut it.*"

This view is open to challenge, especially in light of emerging views about a market for tradeable personal data. However it is difficult to evaluate these different approaches without some way of measuring their effects. The purpose of this research is to develop a methodology, or at least an approach based on risk analysis to compare these modes of regulation.

Measuring regulatory effectiveness

A starting point for a review of regulatory effectiveness might be to look at its effect on risk. Hutter (2005) documents the move towards risk-based regulation in the UK and Europe but points out that

risk is often subjective and therefore difficult to define precisely (Hutter, 2005). The author goes on to talk about the use of impact and probability estimates as a basis for prioritising risk.

This research proposes to use the measurement of risk as a tool for evaluating regulatory effectiveness. This is based on the premise that one of the purposes of regulation is to manage risk. One of the problems with this is that there are different views of what risk is. Aven and Renn discuss risk in terms of something of human value and suggest that both uncertain events (likelihood) and outcome (impact) need to be taken into account in assessing risk (Aven & Renn, 2009). Different methods of assessing regulatory impact were introduced to improve the reputation (and effectiveness) of EU regulation (Torriti, 2007).

The idea of using risk measurement for assessing regulatory impact has been around for some time. The author suggests that risk regulation provides the foundations for assessing regulatory impact. The British Computer Society in 2007 describes compliance with the Data Protection Act in terms of risk management (Room, 2007).

However not all commentators are convinced about the value of risk-based legislation. Haythornthwaite takes the view that where the risk is confined to an individual and does not harm wider society, it should become their individual responsibility, for instance by taking out insurance (Haythornthwaite, 2006).

Heyvaert goes further in suggesting a shift in risk regulation (based on work on climate change) and a move to integration and orchestration and away from individualisation and compartmentalisation (Heyvaert, 2011). So for instance rather than looking at the risks associated with use of online SNSs, we may need to consider wider risks associated with internet use. For instance the risks associated with gathering and exploitation of behavioural data or the inadvertent download of malware are systemic risks of internet usage. Risks associated with making personal data available to a range of providers (again not just SNSs) leave the door open to abuse of that data.

Liu and Terzi have developed a 'privacy score' that "*measures the user's potential privacy risk due to his or her online information sharing behaviour*" (Liu & Terzi, 2010). Their mathematical models are intended to estimate the sensitivity and visibility of personal information. However the models apply to individuals' attitudes to sensitivity of different types of personal data, the nature of the network, and the size of individual personal networks online. It is difficult to see how different regulatory modes would affect the scores that are derived from this model.

Swedelow et al have constructed a universe of almost 3,000 risks to provide a means of evaluating European and US regulation over a 35-year period (Swedlow, Kall, Zhou, Hammitt, & Wiener,

2009). This provides a resource for theory testing and theory building and this serves as a potential test-bed for analysing risks associated with use of online SNSs.

Chapter 3 – Research to date

Methods in information science research

"*The primary goal of research is to link the empirical and the theoretical*". (Ragin, 1994)

This review of regulation calls on a variety of methods from sociology, economics and legal studies. The emphasis is on qualitative methods to identify issues and argumentation supported by quantitative studies of behaviour and attitudes. Textual analysis is particularly relevant in exploring privacy policies of online SNS providers. This research is intended to influence information policy relating to personal data and is informed by the range of research methods used in information science.

Hjørland uses domain analysis to define the scope of information science. Specifically he identifies eleven domains of which two are of direct relevance to this study:

> *"empirical users studies; and*
>
> *studies of structures and organisation in the communication of information"*

(Hjørland, 2002)

However he concludes that:

> *"empirical studies of users may represent an important approach to domain analysis in IS if they are informed by proper theory. They may, for example, provide information about differences in information needs in different communities. They should be combined with other approaches, including:*
>
> - *bibliometric studies;*
> - *epistemological and critical studies; and*
> - *studies of structures and institutions in scientific communication.*"

The last of these headings makes uncomfortable reading because of the emphasis on "*scientific communication*". He bases this on the UNISIST model of the main categories of information sources and the key players in this. The model breaks down when applied to online SNSs, where one of the characteristics of these services is user-generated content. The agencies that are responsible for managing and distributing this information do not fit easily into the categories of: Publishers; Abstracting and indexing services; Libraries; Information centres; and Clearing houses, although Data centres could apply. Therefore a new model is needed if this research is to be considered a part of the domain of information science.

Robinson in setting out "*to derive a conceptual model for information science, which is both academically sound and practically useful*" extends Hjørland's model of information science to a wider-ranging definition: "*Information science can be understood as a field of study, with human recorded information as its concern, focusing on the components of the information chain, studied through the perspective of domain analysis, and in specific or general contexts*." (Robinson, 2009). Personal data on online SNSs can be taken to be human recorded information (including behavioural data from tracking cookies and web beacons). Components in the information chain include SNS stakeholders: users; service providers; and regulators. Although the primary focus of this work is on risks to users, the roles of the other actors (or components) in the information chain are also considered.

Rowlands, Eisenschitz and Bawden consider the limitations of the political economy frame for the study of information policy and suggest that it is inadequate in light of non-market conceptions of information and the emergence of human rights legislation (Rowlands, Eisenschitz, & Bawden, 2002). They suggest that the study of information policy fragments into: laws, regulation, IM practices, and institutional cultures. They suggest that "*inquiry into the political realm can never be value-free*" and that there are no objectives truths in information policy. The frame used to analyse information policy is a set of values and concepts people use to make sense of the world around them.

Research lines

This research started in March 2010 during the period to July 2011 the following activities took place:

- Initial literature survey
- Preliminary consultation with subject experts
- Preliminary survey to identify issues for further investigation
- Presentation of a poster session at the City University Research Symposium in June 2011
- Development of mind-maps of the issues covered in this topic
- Extensive reading and consultation with colleagues about research methodologies

The following research lines were defined during the initial research to establish the scope for this work:

A. Review legislation
B. Investigate privacy policies of SNS providers
C. Interview Data Protection experts
D. Develop conceptual model

These research lines were pursued in the period July 2011 to July 2012 and were based on the preliminary survey to identify issues that affect use of social networks in the workplace.

A qualitative approach was adopted. A particular challenge of social research is combining the insight provided by qualitative research with the generalisability of results that comes from statistically significant quantitative work. Much of the discourse on research methods attempts to reconcile these two approaches.

In his chapter on bridging the Quantitative and Qualitative Divide Turrow describes process tracing that uses qualitative analysis focused on processes of change within cases to uncover causal relationships (Turrow, 2004). Underlying quantitative findings focus on tipping points – explaining points in time-series data where changes occur. He suggests that sequencing qualitative and quantitative approaches in a single study allows triangulation of results and provides better insights into the phenomenon being investigated.

A qualitative survey of individual users (Appendix A) and professionals responsible for data protection identified the following issues:

1. Mixed views about the efficacy of data protection legislation as a means of regulating access to personal data
2. Concern about lack of enforcement or difficulty of enforcement of data protection legislation across national boundaries
3. The need for social network service providers to be more open about what they do with personal data, and defaulting to more secure settings
4. The need for greater education and awareness of the risks associated with posting personal data on social networks
5. View that better encryption standards will help to protect personal data

A. Review legislation

A key component of this research was a systematic study (Appendix B) of the legislation that applies in the UK to protect users against the risks associated with putting personal data up on SNSs. This examined the Data Protection Act 1998, the European Data Protection Directive and the Safe Harbor Treaty between the EU and the United States. This research also identifies relevant secondary legislation such as statutory instruments and European directives and statements.

This research is based on 'black letter law' research which involves reviewing legal sources and related material to address the following questions:

1. What are the rules governing access to personal data on social networks
2. Why did the rules come about?
3. What is their effect?
4. What can be changed?

The study is appended to this report and the conclusions are discussed in Chapter 4.

B. Investigate privacy policies of Social Network service providers

This piece of research reviewed the privacy policies of the largest, English-language SNSs available to UK users (Appendix C). This concentrated on the top 10 service providers (by numbers of users) which are thought to each have more than 100 million registered users.

Weft QDA, a textual analysis tool, was used to mark-up, code and analyse the text of the privacy policies and to identify common themes. Rather than starting with a pre-set coding frame, this was developed based on what actually appeared in the text. This is a method known as literary warrant. Once the coding frame had been developed this was applied to all the policies. As new themes emerged they were back indexed. The research questions were also revisited to ensure that the coding reflected the scope of this research.

C. Interview Data Protection experts

This strand of the research provided a preliminary exploration of specific aspects of regulation by interviewing experts in the field. This carried forward themes identified during the first two strands above. This was a preliminary exercise and will be developed further in the next stage of this research. The following organisations were approached during the preliminary research:

- Regulators such as Ofcom, Information Commissioner's Office,
- Academics in Regulation, Internet Law, Information security and governance
- Industry experts such as Law firms, Information security consultants, Trainers in Computer Law

Semi-structured interviews provided the main approach to interviews with data protection experts. A set of open questions was devised to tease out the issues surrounding the development of data protection legislation, shortcomings and ways in which it might develop in future. At this early stage of the research active note-taking was the principle means of recording the interviews, with check back to individual interviewees where points required clarification.

D. Develop conceptual model

The fourth strand of work was to develop a conceptual model that described the interaction between regulatory modes and access to personal data in social networks. The conceptual model is described in Chapter 4 and will be tested and refined during the case studies.

The conceptualisation is based on a review of the literature and an analysis of the data from the previous research strands and forms the basis for this conversion seminar.

Chapter 4 – Discussion

Research questions

The initial focus of this research proposal was to consider risk as a means of evaluating different modes of regulating access to personal data. The following research questions were posed in the original research proposal:

> *The starting point of such a study might be to consider the interaction between risk and regulation. Is there a conceptual model that adequately describes this interaction? Is a model of social regulation or of economic regulation more applicable to personal information? Is legislation the only way of regulating access to personal information? How do different approaches affect the risks associated with personal information? Can we use the measurement of risk as a tool to assess the effectiveness of regulation of access to personal information?*

Some preliminary research was conducted during 2010-11 to identify some of the main issues that arise in the use of personal data on SNSs. This shifted the focus of the research to encompass the following questions:

- What methods are used to regulate access to personal data on social networks?
- How effective is legislation in regulating access to personal data on SNSs?
- How have SNS providers responded to the legislation?
- How have employers responded to the challenges of workplace use of SNSs?
- Are there other means of regulating access to personal data apart from legislation?
- How can we compare the relative effectiveness of the different modes of regulation?

Effectiveness of the law as an instrument of regulation

A preliminary survey of users and data protection officers (Appendix A) suggests that there is some scepticism about the effectiveness of the Data Protection Act as a means of regulating access to personal data on social networks. Although some respondents found it to be effective, many considered that the legislation alone was insufficient. Several respondents saw other modes such as self-regulation, user education, and technology as important elements in the protection of personal data. This can be represented by a model comprising four different modes of regulation:

1. Legislation
2. Self-regulation
3. Design
4. User behaviour

One of the early tasks of this research is to test the validity of this model and to develop it in the context of SNSs.

Legislation

A review of the legislation in the UK as it applies to use of personal data on SNSs suggests that the Data Protection is the main focus for legislative regulation. This in turn is based on the EU's Data Protection Directive and associated legislation. It is also dependent on the Human Rights Act 1998, which requires the right to privacy (Figure 4).

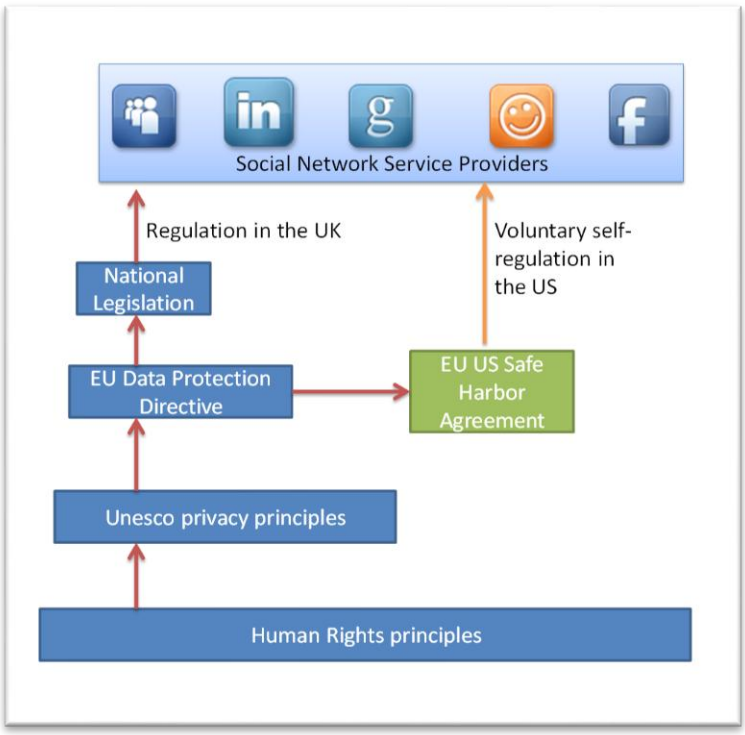


Figure 4 - Legislative regulation in the UK

However there is a problem of interpretation of the Act and whether it applies to SNS providers. Objections to application of the Act focus on the exemptions described in Article 32 "*publication...of any journalistic, literary or artistic material*" and Section 36 refers to data processed "*only for the purposes of that individual's personal, family or household affairs*". However it could be argued that the exemptions do not apply to online SNSs, because it is not the intent of most users to publish their personal data. The second basis for exemption could also be called into question when it is quite clear that personal data is traded with third parties or within commercial groups for the purposes of advertising. This could be seen as being in breach of the 2nd data protection principle – extension of purpose – i.e. using personal data for a purpose beyond that for which it was originally gathered. SNS provider might claim that by signing up to the End User Licence Agreements (EULAs) users are

agreeing to their personal data being used in this way. However it would be difficult to claim that users knowingly gave away their data rights when they agreed to the EULA.

Attempts to define users as Data Controllers suggest that users have complete control over the processing of their personal data on SNS. This is not the case, because the service providers (who one could argue are the true data controllers) are processing and using personal data in ways not envisaged by users. Although users have access to privacy policies and EULAs, it is difficult to argue that this is informed consent, as they are long, often complex and difficult for the layperson to understand.

Another objection to the application of the DPA to SNS providers based in the United States is that they are covered by the EU-US Safe Harbor Agreement. As far back as 2002 commentators were concerned about the fundamental differences in approach to data protection in Europe and the United States (Muir & Oppenheim, 2002). The Safe Harbor Agreement is essentially a self-regulation scheme that is considered weak and with too many loopholes. There is little evidence to date to suggest that the agreement has been rigorously enforced by the US Federal Trade Commission (Connolly, 2008; Reay, Dick, & Miller, 2009) although there are now some moves to make the enforcement of this agreement more rigorous.

Recent developments in European legislation attempts to address novel uses of personal data such as use of internet cookies and sending unsolicited e-mails to individuals. While these cover some of the areas of potential misuse of personal data, the provisions as currently as introduced as a Statutory Instrument in the UK in 2012 are not realistic in their expectation that personal data can be deleted and 'forgotten'.

While there are important principles in the DPA that can be applied to SNSs, preliminary findings suggest that it is insufficient as a tool to effectively regulate access to personal data on social networks. Further research is needed to explore ways in which other modes of regulation can enhance (or replace) the protections afforded by legislatively-based regulation.

A new model of regulation

This research started by considering the interaction between risk and regulation. In order to do this a conceptual model has been proposed to describe this interaction. It can be argued that regulation has three main purposes:

- To reduce risk
- To minimise market inefficiencies
- To create opportunities for service innovation

This research focuses on the first of these and proposes to use risk assessment as a means of evaluating the relative effectiveness of different modes of regulation.

The model focuses specifically on reduction of risk to users and looks at the nature of the risks that users face. This can be characterised by the degree of personalisation of the data and its sensitivity in terms of perceived or actual harm that might arise from misuse.

Privacy

Privacy is bound up with data protection, but it is important to make the distinction between these two concepts. Defining privacy and the limits to this concept is a starting point. For instance, distinctions can be made between privacy and: non-intrusion, seclusion, secrecy, and autonomy (Tavani, 2000). Other commentators have made a distinction between 'personal' and 'private' which have distinct meanings in the context of Data Protection (McCullagh, 2009).

Privacy is not co-terminous with personal data. For instance, misuse of personal data is distinct from, although related to, privacy. Nevertheless it is necessary to consider what is meant by privacy. The literature review covered the origin of some definitions of privacy and this showed that there was not a single consistent view of privacy. For instance, Westin identifies "*four psychological conditions or states of individual privacy—solitude, intimacy, anonymity, and reserve*" (Margulis, 2003). However later commentators have made the distinction between information privacy and other types of privacy such as that related to personal space (Smith et al., 2011).

Is privacy necessarily a good thing? The starting point for many studies is that personal privacy has to be preserved and that any failures in the regulation of access to personal data is necessarily a bad thing. However some commentators caution against blanket application of privacy laws to anonymised (and consolidated) information because "*many beneficial uses of data would be severely curtailed*" (Tene & Polonetsky, 2012). The benefits of exchange of personal data, include: improved services to users; cheaper delivery; and better security and protection.

Some research suggests that the more use that despite stated concerns about privacy, people often reveal considerable personal data when they start to interact with an online service. This is known as 'the privacy paradox' (Bonneau & Preibusch, 2009; Sobel, 2007).

Risk to users

Other aspects of protection of personal data, apart from privacy, are protection from abuses such as: fraud, bullying, and harassment. Some of these could be seen as aspects of privacy "*the right to be let alone*", or opening people up to risks such as financial loss through fraud (Warren & Brandeis, 1890). This study focuses specifically on use of personal data by advertisers, while acknowledging wider issues such as unauthorised access to personal data provided to a SNS by its users.

Personal data can be described in terms of proximity and sensitivity of data. Different modes of regulation could be evaluated in terms of its effect on each category of personal data.

Risks associated with personal data can be described in terms of:

Effect on : individual, society, industry, government

Nature of risk: loss of dignity, loss of personal control, financial loss, loss of liberty or life, loss of rights

Severity of consequence

Probability of occurrence

So for instance a risk might be the following event: non-attributable personal data is made available to advertisers via a web beacon or browser cookie. The consequence of this is intrusive advertising, but there may also be a problem of loss of dignity (as when colleagues have sight of advertisements for personal products) or breach of confidentiality – e.g. if buying a present for a friend or relative in the same household or workplace – and they see the ad.

Harassment, bullying and the associated loss of dignity is a significant risk faced by users or by the subjects of users' postings on their profiles. In Teggart v TeleTech UK Ltd an industrial tribunal found in favour of the respondent defending their dismissal of an employee for gross misconduct after he posted salacious and damaging allegations about a co-worker on his Facebook profile. Interestingly the tribunal also referred to Article 8 of the Human Rights Act:

> *"When the claimant put his comments on his Facebook pages, to which members of the public could have access, he abandoned any right to consider his comments as being private and therefore he cannot seek to rely on Article 8 to protect his right to make those comments."*

("Teggart v TeleTech UK Ltd," 2012)

Model of personal data

In the review of the privacy policies of the 10 leading SNSs (Appendix C), the following types of personal data identified in SNS privacy policies. These have been grouped by type of personal data:

Type of personal data	Data elements
Identity	Name [IDs such as passport number, driving licence number, National Insurance number, NHS Number, Pupil Number] – not in survey Gender Sexuality Race / ethnic origin

Type of personal data	Data elements
	Place of birth
	Nationality
	Age
Location	Address
	Current location
Security	Username
	User login / password
Attitudes and interests	Interests
	Religion
	Political affiliation
	Holidays / places visited
Education and employment	Occupation / employment status
	Education
	Criminal history
	Schooling / education
	Scholastic achievement grades
	Employment history
Finance	Banking details
	Income
	Home ownership
Health	Health status
	Medical history
Personal network	Marital status
	Family status
	Personal details of associates (colleagues, friends, household members, relatives)
Behaviour	Activities (-sites visited, groups joined, services / products purchased)

Who are the players?

In order to understand regulation of access to personal data on SNSs, it is important to identify the players or agents involved in the process and the ways in which they are affected by regulation. Figure 5 below shows how personal data and advertising data flows between the different agents.

Users and other users are grouped together as the advertisers may not necessarily distinguish between them. Users provide personal data to their SNS provider via an ISP. The ISP is included because as an agent they may be subject to regulation or to legal action by other agents. The SNS Provider may make personal data available to associates and affiliates or to advertisers, who may be affiliated organisations or third parties. The privacy policies of many SNS providers refer specifically to sharing personal data with third parties (usually anonymised) or else with affiliates. Previous studies have shown that affiliates can number in the hundreds or even thousands, depending on what definition of affiliate is used. An investigation of the top 50 internet services showed that some providers were part of groups with up to 2,300 subsidiaries (Gomez, Pinnick, & Soltani, 2009).

Personal data is also relayed to other users – either as an activity log ('X has just updated their profile, or just made friends with Y'), either directly or via groups that they have in common. This may be seen as less of a problem because by becoming a friend or connection with someone there is an implied expectation that personal details will be shared with them or among the mutual groups.

It becomes more relevant when the SNS provider shares personal data with third parties or with associates and affiliates (in some cases contractors are claimed as affiliates). This may be anonymised data – many SNS privacy policies make reference to this, or it may be identifiable personal data. For this reason they have been grouped together. The advertisers then push tailored advertisements to targeted users. In doing so they may use tracking technologies to monitor internet behaviour and to build up profiles of individual users. This can be used in conjunction with a registration system or login to a service provided by the advertising company to create identifiable (i.e. not anonymised) personal data.

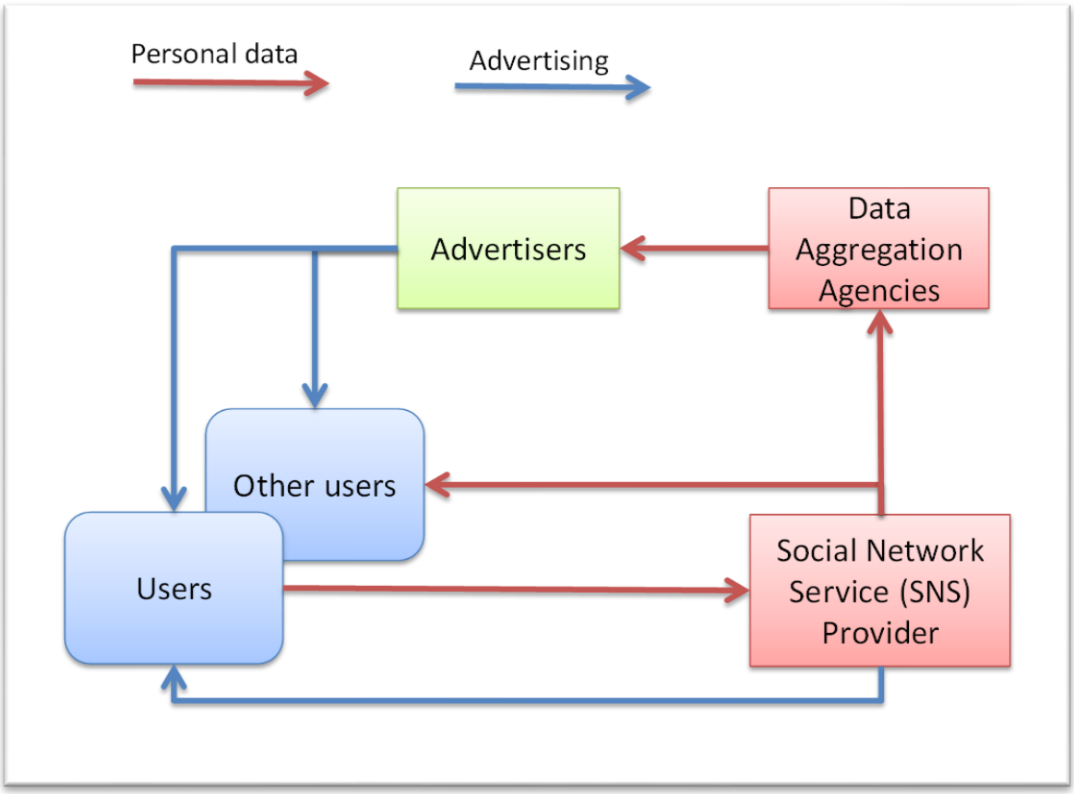


Figure 5 - Relationship between different agents in an SNS

What is being regulated?

Regulation can be viewed in terms of who is being regulated. For instance, is it the industry, their agents, or the consumers that is being regulated?

The Data Protection Act 1998 focuses on the responsibilities of the data controller who can in some cases be seen as representing the SNS provider (See Appendix B for a more detailed discussion). Part of the problem arises in the definition of data controller.

Self-regulation is focused on the SNS providers and to some extent the ISPs as manifest in their privacy policies and End User Licence Agreements (EULAs).

Design is normally enacted by SNS providers and their agents when setting up and modifying their services. They can build privacy into the design their systems so that defaults are for less disclosure. However this may be seen as being in conflict with their desire to extend their membership and range of services available to members.

Users also regulate by their behaviour either collectively (as in market demand) or individually by the way in which they interact with services and the degree to which they reveal personal data. User education is seen as one way to improve individual security.

It could also be argued that activities are being regulated rather than individuals and organisations. For instance, exchange and use of personal data could be subject to self-regulation (in privacy policies), legislation (as with the Data Protection Act) or by design (as with data encryption to protect against unauthorised access to personal data).

Limitations of regulation

Although there has been some attempt in the UK to bring together different strands of regulation, there is still a problem of jurisdiction which makes it difficult to enforce the principles of data protection to SNS providers based outside the UK. The Information Commissioner's Office is responsible for enforcing the Data Protection Act in the UK, but has also been instrumental in educating users about secure use of social networks and in promoting the idea of 'Privacy by Design' for service providers.

It is not always clear to what extent Data Protection regulations apply to social media, and whether other laws such as the Communications Act 2003 might also apply to some aspects of service provision.

Lessig's model of regulatory modes highlights the problem of a fragmented approach to regulation. He suggests that an effective strategy is to link these approaches together rather than depending on any one mode of regulation (Lessig, 2006).

Wu describes the failure of regulation of the communications industry. Instances of regulatory capture, where a few large suppliers dominate the markets, have strong connections with, and

influence, over regulators and effectively protect their markets by raising the barriers to entry so high that competition is stifled. This market regulation discourages new entrants to the market and reduces innovation that arises from new services providers (Wu, 2010). It may also be a warning to the online sector, especially if there is an attempt to regulate a few large providers.

The other problem of regulation is extraterritoriality – SNSs are international and can choose which regulatory regime applies to them. Some choose to reside in a territory with weak regulation. Many commentators have commentated on the inadequacies of the self-regulatory approach data protection in the United States – intended to provide a regulatory gap for US firms to allow them to operate in European markets which are subject to the Data Protection Directive. Because it is essentially self-regulated with no obligation for independent verification of the measures that they may take to protect consumers' interests. A review of the Safe Harbor Scheme found that even within the loose constraints of the Safe Harbor principles, only 348 out of 1,597 registered companies complied with the most basic of principles of the framework. Most entries were out of date, inaccurate or simply untrue, so that for example, many companies said that they had a published privacy policy, but did not make them available on the internet (Connolly, 2008).

Self-regulation

Self-regulation by an industry can apply if there are suitable sanctions for non-compliance such as expulsion from a grouping with consequent loss of credibility and market share.

Surrogate regulation, where the responsibility for regulating a professional group or industry is vested in a professional or trade body, can also be effective. Membership of the body becomes a condition of being allowed to trade. This can be seen with the established professions and some sectors in the UK (such as civil engineers, lawyers, doctors and architects). This approach takes the burden of regulation away from the state and the costs of regulation are borne by the regulated individuals or industry.

Alternative modes of regulation

The growth of internet communities and interactions has allowed the effective development market driven regulation. This can be seen in social pressure on providers to comply with market expectations. For instance recent changes in the Facebook privacy settings without full consultation with users led to an outcry and pressure to retract. However, this may be because of the implicit threat that legislators may feel obliged to respond with new regulations to counter the concerns of their voters (BBC News, 2011).

Reputational systems may be one way forward as seen with Trip advisor or Amazon. However there are problems of skewing if there are few reviews and one or two extreme views. With larger

numbers, some statistical methods help and can be incorporated into the scoring system. The problem is that with a few large providers there is less shopping around and less incentive to look at third party sources before deciding to join a network. Peer pressure is probably a significant factor – you join the network that your friends are on.

Describing privacy

One initiative in 2009 looked at the privacy policies of the top 50 websites and coded these policies using a series of icons developed to describe different provisions in the privacy policies (Gomez et al., 2009). This could be a useful way forward and development of this idea is one potential avenue for this study. However it would need to address the following issues, if it were to become a useful service for consumers:

- Raise awareness among users, so that they know to refer to this service as a port of call. Some of this will be down to credibility of the service in terms of its independence (from providers), its coverage and its comprehensiveness
- It should ideally be integrated into applications such as browsers to facilitate ease of use
- There would need to be a mechanism for moderation of the entries on the database – to verify that they are correct, to keep them up to date and to deal with any conflicts (for instance, if a service provider did not agree with their designation)
- Service providers would need some incentive or compulsion to use the service or to contribute data, and to provide links from their website to the classification on the Know Privacy site
- Resourcing to ensure that the database is properly maintained and that the data continues to be checked and quality assured

A successful example of a system of descriptive icons is the Creative Commons[3], with widely recognised symbols to denote different levels of permission and conditions of use of intellectual property. Other commentators have already noted the potential parallels between Creative Commons and protection of privacy on SNSs (Bickerstaff, 2009).

[3] The Creative Commons is based on a community with a strong interest in access to and exchange of ideas as expressed in publications and other intellectual outputs.

Model for future regulation on the internet

Drawing parallels with the Creative Commons model for sharing intellectual content and developing the Know Privacy initiative, it may be possible to design a self-regulatory system for management of access to personal data on SNSs. In the proposed scheme an agency would run a privacy policy database on behalf of the SNSs. Users would be able to follow links from descriptive icons on the SNS site to the appropriate database entry (Figure 6).

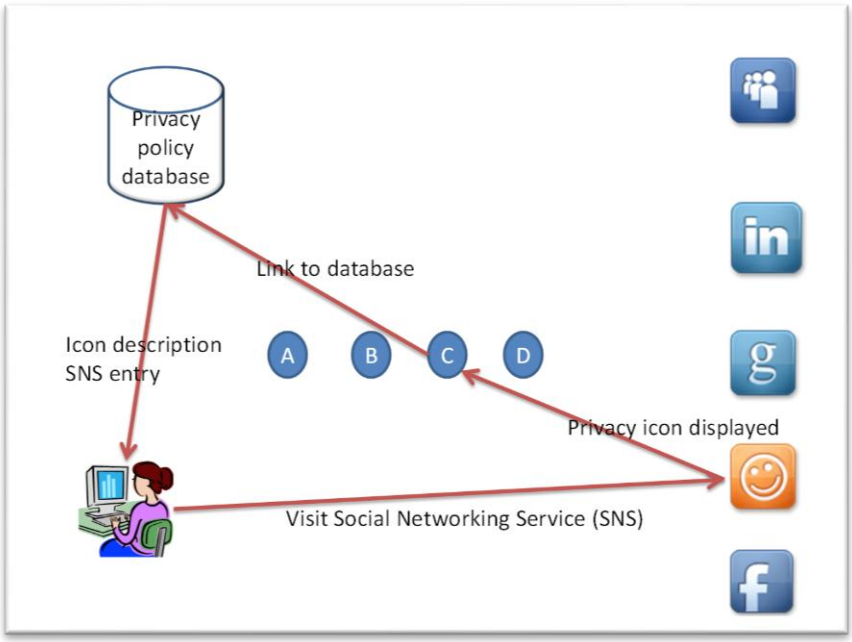


Figure 6 - Privacy policy database

The proposed system would incorporate user feedback, so that there is an element of control by consumers (Figure 7). This would operate like a star system used on user review / recommendation websites. Application of simple algorithms would remove 'outliers' so that excessive skewing of scores by a few atypical scores is minimised. Users would also be able to look up individual entries for SNS providers on the central database for independent validation of the privacy settings and behaviour of the participating SNSs. The user feedback provides one element of control of the entries and is self-policing.

To complete the validation and authentication of the SNS entries on the database an independent certifying authority, paid for by the SNSs would check the privacy settings claimed by the SNS providers and verify the entries (Figure 8). If there is a discrepancy between what is claimed and what actually exists, there would be a clear indication of this in the database. The user would see the certification via a link on the SNS or by directly accessing the central privacy database.

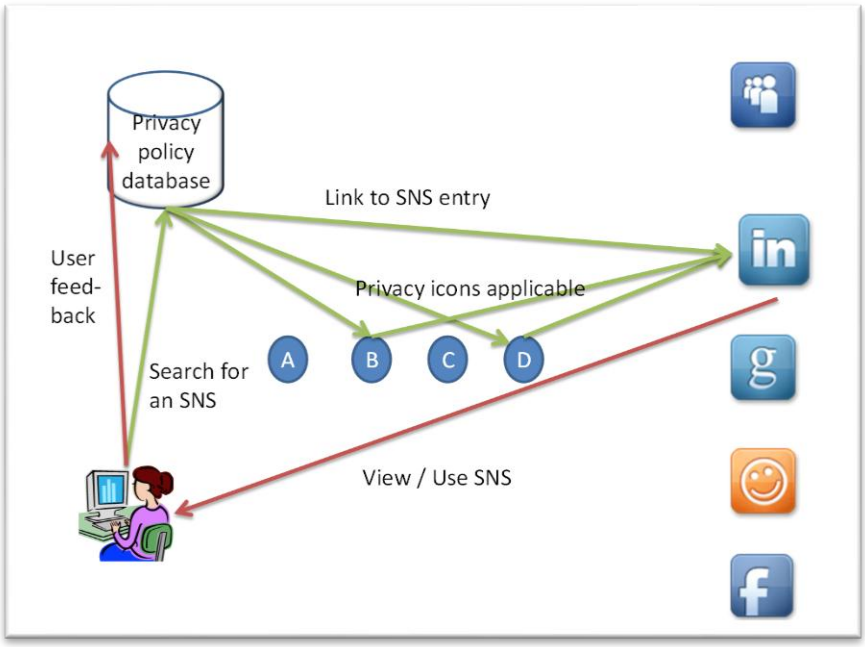


Figure 7 - User feedback on privacy performance

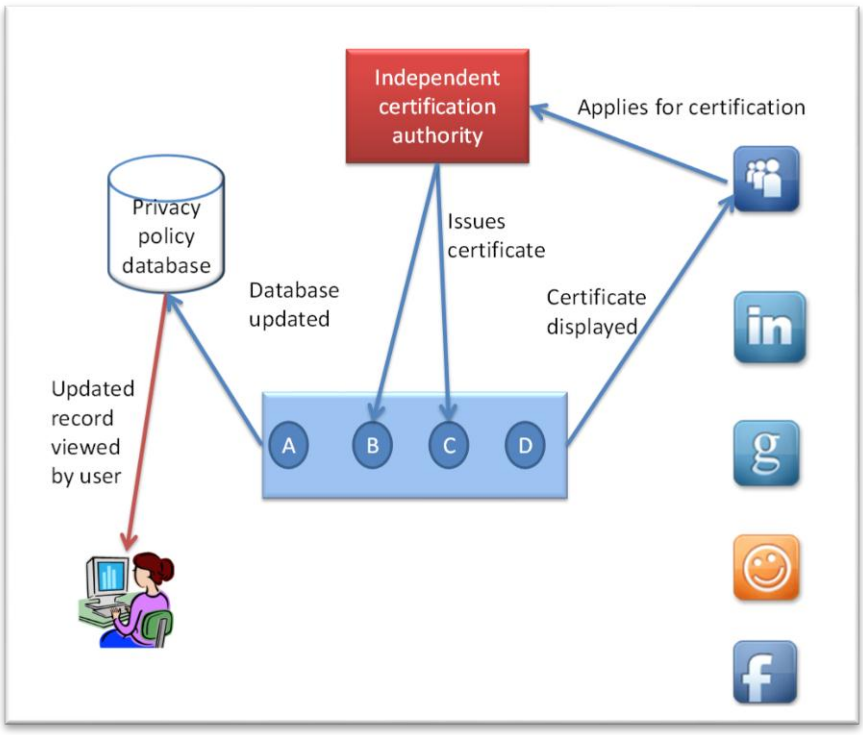


Figure 8 - Certification of SNS sites

Chapter 5 – Research Plan

The first part of the research has concentrated on setting the limits of this investigation by defining what we mean by users, the different regulatory methods being evaluated and the perceived risks of using SNSs. It also identified workplace policies on social networks as a potentially rich area of investigation and one that has been explored elsewhere (Boudreaux, 2011).

The forward research plan builds on findings to date and sets out to test the hypothesis that risk can be used as a means of evaluating the relative effectiveness of different modes of regulating access to personal data on SNSs. This in turn will help to throw light on question of whether legislation alone is the best way of regulating access to personal data on online SNSs accessed by users in the United Kingdom. The research proposes to extend this view to the use of social media in the work place and will consider employer attitudes.

The proposed research has the following main strands, which are described in detail below:

- Identifying and measuring risks
- Assessing the effect of different regulatory modes on risk
- Case studies of workplace measures and SNS providers

Approach

The main focus of this research is on the effect of regulation on risk to users of online SNSs. An initial view of this topic would suggest that an empirical approach to measuring risk should form the basis for comparison of different regulatory modes. However many of the risks identified are difficult to measure objectively, despite various attempts to do so. The research may be limited to a qualitative evaluation of perceptions of risk or a quantitatively indicate approach where the regulatory effects may be described in terms of their tendency to increase or decrease the probability of a risk occurring and their tendency to increase or decrease the impact of the risk event if it occurs.

Another avenue to explore will be the effect of regulation on perceptions of risk by users and the response of different stakeholders to regulation or potential regulation. These approaches call on well-established social science methodologies including ethnography, case studies and attitudinal surveys. Outhwaite and Turner suggest that social science methodology has two meanings:

> "*methodological issues arising from and related to theoretical perspectives, as in Marxist, functionalist or feminist methodology*"

and

"*issues of specific research techniques, concepts and methods*."

(Outhwaite & Turner, 2007)

This research focuses on the second of the two definitions.

McNeill maps the development of social science research from thinkers such as Marx, Durkheim and Weber as well as the early social research of Charles Booth in London in the late 19th and early 20th Centuries ("Charles Booth Online Archive," n.d.; McNeill, 2005). He goes on to describe the Chicago School which pioneered anthropological research, through to the research by feminist scholars in the 1980s.

Both qualitative and quantitative approaches are proposed for this research to offer a degree of triangulation of research findings. The qualitative results (e.g. from semi-structured interviews and examination of legislation) will be based on textual analysis to identify themes and topics for further exploration. The data will provide material for development of a working hypotheses about the relative effectiveness of different types of regulation. This Grounded Theory approach will then be tested by means of a survey of different stakeholders in the provision and use of SNSs.

In social science the development of hypotheses has been the focus of much attention. Glaser and Strauss in their study on Social Loss of the Dying proposed a system of 'grounded theory', where data drives the development of a hypothesis which is then tested by gathering new data to test the hypothesis is extensively used in social sciences (Glaser, 1978; Glaser & Strauss, 1967). This can be an iterative process with several rounds before a refined theory with predictive capabilities is established. It is an example of hypothetic-deductive research and falls within the bounds of the scientific method. It could deploy qualitative or quantitative methods to gather the data (Glaser & Strauss, 1966).

Whilst it is important to acknowledge any assumptions or starting points for the research, an approach based on Glaser and Strauss's Grounded Theory seems more appealing, where an initial hypothesis is generated from a pilot study and this is further investigated using empirical data to test the hypothesis. This method is described in detail by Charmaz who states that "*theoretical sampling is less of an explicit procedure than a strategy that you invoke and fit to your specific study*" (Charmaz, 2006).

Other empirical data such as prosecution figures will also be examined to validate or refute the working hypotheses. This works on the principle of falsifiability of the hypothesis. In other words, the question will be framed in such a way that it is possible to disprove the hypothesis with empirical data if it is false.

Ragin combines qualitative and quantitative techniques in 'fuzzy sets' where individual entities have varying degrees of membership of a set. So for example, one could study varying degrees of risk associated with personal data or applying to users (Ragin, 2000). He goes on to suggest that if Theory 1 proposes cause and effect and Theory 2 proposes multiple causes of the same effect, Theory 1 may still be valid. Applying Ragin's principle to this research one could posit that Data Protection legislation will result in lowered risk to users of SNSs. This hypothesis is not necessarily undermined by the view that several different modes of regulation working in concert may be even more effective in lowering the risk to users.

The challenge then is to separate out the effect of legislation by undertaking a series of case studies for instance, to establish the effect of legislation on risk and outcomes.

Methodology

Identifying and measuring risks

The first part of this research will be to identify risks starting from the universe of general risks compiled by Swedlow and associates (Swedlow et al., 2009). The research will also consider specific risks associated with SNS use and reported in the literature. This will be enriched with additional analysis of risks identified during the initial survey (Appendix A) and developed further. These will feed into a risk model which can then be tested and validated by surveying representatives of the following stakeholder groups:

- Users (questionnaire survey and interviews)
- Regulators (interviews)
- Employers (interviews)
- SNS providers (interviews)

A series of semi-structured interviews will be undertaken, with the aim of eliciting responses from a diverse group of respondents. Using a structured sample of responses will be combined with the results of an investigation of the literature to identify as many of the relevant risks as possible. The following topics will be explored:

- Attitudes to risk associated with social networks, usage of social media and view on effectiveness of different types of regulation of access to personal data
- Users of personal data (e.g. advertisers) and the extent to which their behaviour is affected by UK legislation – in comparison with other modes of regulation
- Views of social network service providers on effectiveness of legislation in the UK and other forms of regulation

- View of regulators and what they perceive to be the challenges for future regulation of access to personal data

The next step will be to develop measures of risk. Two dimensions need to be considered when attempting to measure or quantify risk:

1. the **probability** of occurrence; and
2. the **impact** that risk has if it comes to fruition.

Some methodologies combine these into a single risk value – this is often possible where the risk impact can be measured in terms of numbers of occurrences, or numerical values such as economic cost or benefit. One of the challenges of this stage of the research will be to determine whether it is possible to assign a numerical value to the impact of allowing access to personal data on online SNSs. An obvious line to follow would be to assign a monetary value to the cost/effect of releasing/not releasing personal data.

Another avenue that will be explored will be court cases related to release of personal data on online SNSs. Initial indications are that there is not a sufficiently large body of cases to estimate economic costs in the UK or even across the whole EU. However the small number of cases that may exist could provide additional insights into the risks and issues that arise. The following aspects will be considered when examining court cases:

Published breaches of privacy
Recorded breaches
Convictions
Costs to individuals of data breaches
Estimated total breaches and cost
Cost to businesses, government and society of breaches

The Information Commissioner's Office will be approached for guidance on work that they may have commissioned in this area which has not already been published. Approaches will be made to EU wide initiatives and to other active regulators such as the Canadian Privacy Commissioner and the European Union Data Protection Review Working Group for any work that they have done on quantification of risk.

Assessing the effect of different regulatory modes on risk

The effect on risk of four regulatory modes will be assessed by looking at how they would affect users. The proposed modes to be investigated are:

I. Legislation
II. Self-regulation
III. Privacy by design
IV. User behaviour

Their effect will be assessed in terms of whether they increase or decrease the likelihood and impact of a risk event taking place. The proposed parameters for comparison of the regulatory modes are as follows and will be revised during the investigation:

- Adaptability to changing technology
- Comprehensiveness
- Which risks addressed
- Effects on risk
- Impact on stakeholders
- Cost of enforcement
- Benefits (savings) from enforcement (i.e. consequence of not regulating)
- Alternatives available

Legislation will be used as the point of reference for comparison with other regulatory modes. This refers back to the original question: Is UK legislation alone the best way of regulating access to personal data on online SNSs accessed by users in the UK?

In the UK the Data Protection Act 1998 (DPA) is the main instrument for legislative regulation of access to personal data. The DPA will be examined in depth because it forms the most visible and widely applied regulatory approach to protection of personal data in the UK. This will build on work already completed (Appendix B).

A detailed textual analysis of existing primary and secondary legislation in the UK will inform the choice of respondents and questions for discussion with the regulators and legislators. The interviews will explore the issues that specifically relate to SNSs.

Interviews with legislators and regulators will consider the intention behind the legislation and will be compared with Hansard reports on the parliamentary debates when the legislation was being developed. The interviews will also consider possible future intentions and directions for regulation. Proposed question areas are:

What measures are in place to deal with social network providers/services?
Views on the required measures to effectively regulate this area?

What approaches might be adopted by the regulators in future?

This is a form of socio-legal research, distinct from the scientific research method. Feldman in the Nature of Legal Scholarship states that "*scholarship is related to the good of knowledge*" (Feldman, 1989). He suggests that the scientific method is not appropriate for legal scholarship for the following reasons:

> The limitations of the scientific method – observation may change the thing being observed, difficulty in constructing a null hypothesis when there are many possible hypotheses to test. The inappropriateness of the falsifiability rather than verifiability of hypotheses because of the impossibility of constructing a null hypothesis for most social science questions.
>
> His second objection is that "*claims to scientific objectivity are often inflated*". By this he means that study of law and legal systems is not value free and that objectivity is therefore difficult to attain in legal studies.
>
> Thirdly he states "*In refusing to use legal techniques, either to investigate that claim or to discover the state of the law, one discards analytical tools of some interpretative value*." In other words he is suggesting that legal research methods may be more appropriate than scientific methodologies for research in this domain.

Feldman goes on to suggest that scholarship can be evaluated "*as being more or less in tune with certain formal values which are integral to a serious search for truth. These include*:

"(1) a commitment to employing methods of investigation and analysis best suited to satisfying that curiosity; (2) self-conscious and reflective open-mindedness...; and (3) the desire to publish the work for the illumination of students, fellow scholars or the general public and to enable others to evaluate and criticise it."

(Feldman, 1989)

Case studies of workplace measures and SNS providers

The final stage of the data gathering will involve case studies of online SNS providers and of employers. These will provide an in-depth view of the factors that underpin the privacy policies of SNS providers and the measures taken by different types of employer to protect personal data of employees and customers in SNSs.

These case studies will not include participant observation, which might be more appropriate where the investigator were employed by the organisation being studied. It will however call on

hermeneutics, which will involve a deep understanding (known as '*verstehen*') of the context of the situation or phenomenon being studied (Brady & Collier, 2004).

Ragin identifies four types of case study:

> *"1. Cases are found – empirically real and bounded, but specific. Identified and established as cases in the course of the research process*
>
> *2. Cases are objects – Cases are real and bounded but general and conventionalized. Cases defined by the literature – e.g. nation-states*
>
> *3. Cases are made – "theoretical constructs that coalesce in the course of the research" - see emerging patterns and construct theories around them*
>
> *4. Cases are conventions – "general theoretical constructs, ...as products of collective scholarly work and interaction...external to any particular research effort"*

(Ragin & Becker, 1992)

The investigation of privacy policies of SNSs and of employer policies fall into the first category of case study – "*empirically real and bounded but specific*".

The research proposed will use participant observation (ethnography), which is seen as an appropriate methodology for studying "*complex social relations and organisational processes*" in organisations (Delbridge & Kirkpatrick, 1994).

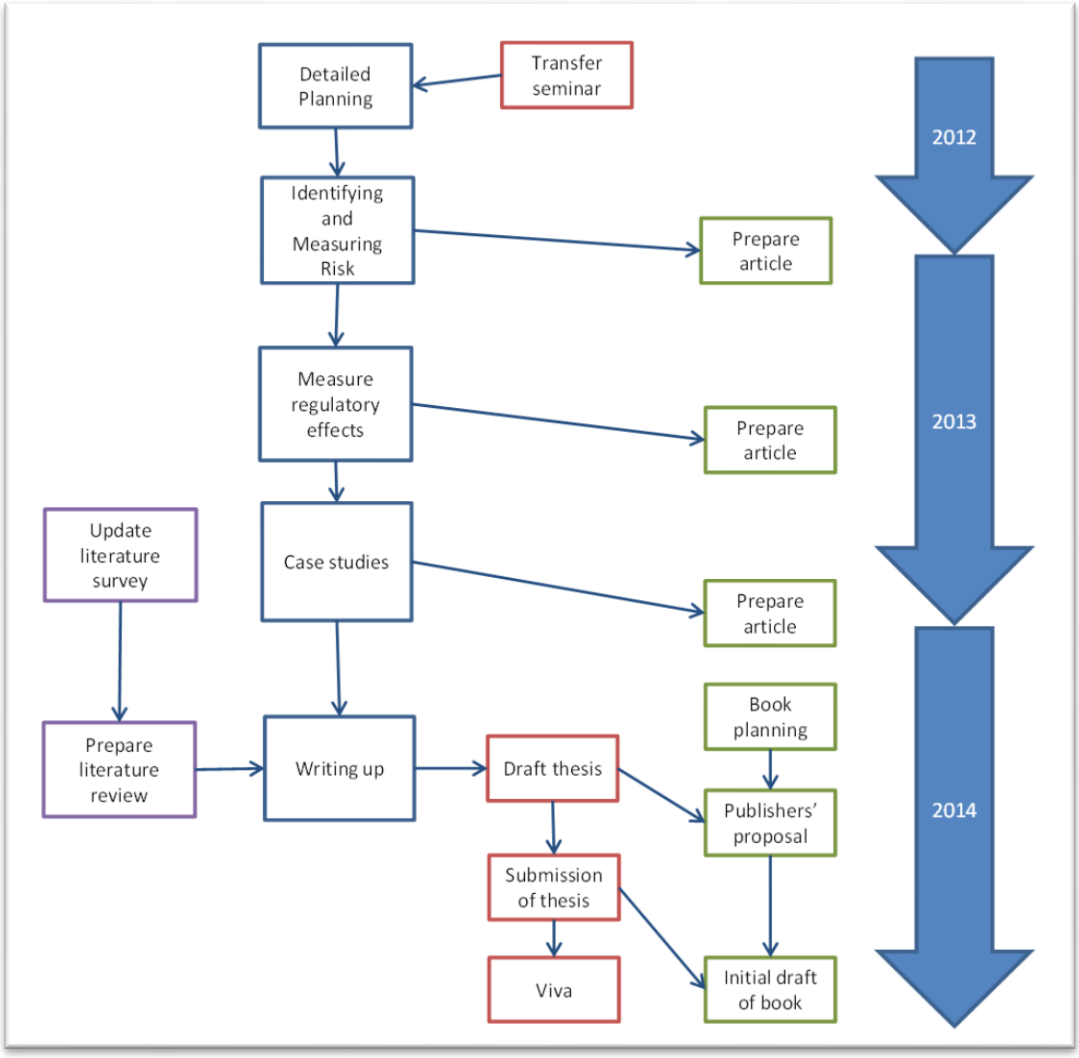
Miller uses local ethnography and comparative anthropology for his study of Facebook based on case studies conducted in Trinidad. His starting point is that each experience of Facebook is unique. He sets this in the cultural context "*but what any given population actually uses, based on that facility, quickly develops its own local cultural genre and expectations which will differ from others*". He goes on to say that "*there is no such thing as Facebook from the perspective of cultural relativity. Facebook is only the aggregate of its regional and particular usage*". He posits fifteen theses on what Facebook might be (based on user experiences) and this in turn may affect attitudes to personal data and who should have access to it under what conditions (Miller, 2011). These are themes that will be turned to in this study.

Timetable

The main investigation will take place during the period October 2012 to May 2014, with analysis and writing up during the latter half of 2014. The timetable below indicates the proposed schedule for this work.

Date	Research Activity
October 2012	COMMENCEMENT OF MAIN RESEARCH
	IDENTIFYING AND MEASURING RISK
October-November 2012	Modelling stakeholder types and risk types
October-November 2012	Design interview survey of stakeholders
November-December 2012	Identify and contact respondents
December 2012-February 2013	Conduct interviews
January-March 2013	Data analysis
March-April 2013	Risk analysis for stakeholder groups
March-May 2013	Review of court cases
March-May 2013	Investigation of methods for quantifying risk
April-May 2013	Application of quantification methods to this research case
	ASSESSING THE EFFECT OF DIFFERENT REGULATORY MODES ON RISK
June 2013	Develop conceptualisation of regulatory modes
July 2013	Update legislative review
August 2013	Applying different regulatory modes to risk
	CASE STUDIES
March 2013	Identify case study candidates
March-June 2013	Approach and secure workplace case studies
September-December 2013	Conduct workplace case studies (data gathering)
December 2013 – January 2014	Analysis of workplace case studies
September-December 2013	Approach and secure SNS case studies
February-April 2014	Conduct SNS case studies
April-May 2014	Analyse SNS case studies
	WRITING UP
December 2013-February 2014	Analysis and discussion
February-March 2014	Update literature review
February-May 2014	Preparation of draft thesis
June 2014	Review of draft with supervisors
July-August 2014	Preparation of final version
September 2014	Submission of thesis
September-October 2014	Preparation for viva
December 2014	COMPLETION

These research activities are presented as a flowchart below, along with a broad indication of the envisaged timescale:



Research ethics and project risks

The main ethical issues are associated with surveying individual attitudes and perceptions. Data gathered will be kept securely and the results will be anonymised to prevent the possibility of identification of an individual based on their reported profile. The names of participants in the survey will not be published. However interviews with legislators and regulators will be difficult to anonymise. Where this is the case, respondents will have the opportunity to review the interview notes and any quotes proposed before they are included in the thesis or any resultant publications.

Where interviews are conducted with individuals representing organisations, comments and quotes will be notified to the participants so that they have an opportunity to block or revise them prior to publication.

There are a number of project risks associated with this research that need to be taken into account and planned for:

Risk	Response	Result
Lack of access to the right people – especially service providers and legislators, undermining the validity of the findings	Minimise probability: Early identification of targets. Establish contact at conferences and meetings	Get into diaries of busy and difficult to access people
Difficulty in constructing a representative sample of stakeholders for survey, making it difficult to draw conclusions about attitudes in the general population	Avoid: construct a qualitative survey that obtains a wide range of views	Provides a qualitative response, which may not be regarded as well as a quantitative survey
Difficulty reconciling different models of risk, makes it difficult to establish a testable proposition for this research	Minimise probability: Evaluation of different models before picking one or developing a new one. Concentrate on testing the selected model.	Possibly a new model of risk developed. Greater focus for the research by having a single testable model to work with
Difficulty finding a means of quantifying risk making it difficult to test the relative effectiveness of different modes of regulation.	Minimise impact: use qualitative measures of effect on risk to evaluate different regulatory modes.	Development of a new method or assessing regulatory effectiveness.
Inconclusive results make it difficult to make positive assertions	Minimise probability by framing questions in such a way that it is possible to make a positive assertion whether the results are positive or negative	Conclusions expressed in such a way that it is possible to publish the results.

Appendix A – Preliminary survey of users and employers

Background

This preliminary research set out to identify the issues that affect privacy in social networks and identify the types of regulation that are used. This involved surveying: data subjects who use social networks, data subjects who do not use social networks, legal experts, regulators (ICO), experts studying the area of regulation, and professionals responsible for information governance including records managers, risk managers and ICT managers.

An initial set of semi-structured interviews identified topics for further exploration in an electronic survey and helped to frame the question areas.

The purpose of this preliminary research was to develop a working hypothesis about regulatory effectiveness and risk measurement of assessing the effectiveness of different modes of regulation of access to personal data, with reference to social networks.

The aim of the survey was to identify the range of issues associated with personal data on social networks that could be the basis for further study in the main research proposal. The sample selected was not intended to be statistically representative. It is anticipated that further on in the research a quantitative survey may be used to gather empirical data on attitudes to specific issues or on reported behaviour on social networks.

Methodology

Qualitative survey

This research was conducted as a qualitative survey supplemented by interviews with academics, regulators and researchers. The survey was delivered as an online questionnaire designed and delivered using www.surveygizmo.com (academic licence). It was selected for its ability to formulate different question types, its basic analysis capabilities and its ability to export results for analysis in other applications.

Respondents

The survey was in two parts: to UK-based professionals responsible for information governance and data protection in their organisations, and to a small sample of individuals to discover personal attitudes to protecting personal data on social networks. The survey to information governance professionals was distributed via the following lists:

- BCS IRMA LinkedIn Group
- BCS ISSG LinkedIn Group
- BCS Law LinkedIn Group

- BCS Internet LinkedIn Group
- BCS Doctoral Consortium LinkedIn Group
- Data Protection and Security LinkedIn Group
- IRMS LinkedIn Group
- JISCMAIL Data-Protection
- JISCMAIL Records-Management-UK

It may also have been forwarded to other groups by members of the above groups – although this information was not recorded.

The survey respondents were self-selecting. The principal concern was to keep it within the bounds of professionals responsible for information governance in UK-based organisations. This means that the reporting (apart from an initial analysis of the types of respondents) has been kept anumerate, on the basis that any figures for responses hold no particular significance.

The corporate survey was open for approximately 4 weeks and was then closed and the results exported to a spreadsheet for analysis.

Data coding

A data export of rows (by respondent) and columns (by question) was also performed. This sheet allowed for use of the Excel sort and filter function during the analysis. This was particularly useful to begin to identify possible areas where there may be a correlation between responses to different questions. For instance: Are representatives of larger organisations more concerned about some issues rather than others; or Do representatives of organisations that do not allow use of social networks in the workplace have a different perception of risks from representatives of organisations that do allow social networking?

The analysis was data driven, which means that there was no initial coding framework in place for the open-ended questions. For each question the responses were encoded as they were read. A two-letter mnemonic code was created for each new topic that was identified and this was entered on a separate list along with the full expansion of the topic title. The codes were added in a separate column alongside the column containing the responses. Where a theme re-occurred the appropriate code was added to the response. The codes were then examined for overlap and where it was considered that two topics were closely allied they were merged into a single topic. The associated codes were revised and replaced using the search and replace function in Excel. Sorting the code column then allowed grouping together of responses by topic. A further refinement of the coding took place after all the questions had had the preliminary analysis and coding. Topics that sere similar across more than one question were consolidated so that there was a wider perspective on

each issue mentioned. It was important to make sure that each code was unique across the whole survey result.

The resulting sorted grouping of quotes for each open-ended question were copied to a Word document for incorporation into the reporting of results.

Ethics

The survey reporting is non-attributable in line with the statement made at the start of the survey. This was intended to encourage respondents to be open about their concerns and views about protection of personal data on social networks. The analysis has been careful to avoid inadvertently identifying individuals or organisations by being too specific in the reporting of results.

Survey results

Background about the respondents and their organisations

A total of 52 completed responses was received from LinkedIn and JISCMail discussion lists. Many respondents belonged to more than one group. The largest single group was the Information and Records Management Society (52%), the British Computer Society Information Security Specialist Group (15%), then CILIP and the Archives and Records Association (both 13.5%). Only two members of the National Association of Data Protection Officers responded to the survey. The preponderance of records managers, archivists and library / information professionals was reflected in the job titles with 13 'Archivists' or 'Records Managers'. Nine respondents had 'Governance' and five had 'Data Protection' in their job titles. A further four appeared to be IT professionals and two appeared to be legal professionals.

The majority of respondents worked in the public sector (including health and education) which accounted for 80% of responses. The remainder worked in the private sector (10%) or in consultancy (8%) and one person worked in the voluntary sector. The majority represented organisations that had 1,000 or more employees (67%). None worked in organisations of fewer than 10 people.

46% of respondents worked for organisations with a policy on use of social networks of which half were allowed to use social networks at work and half were not. Most of the organisations that allowed employees to use social networks at work did not have a policy on their use.

Use of social networks in the workplace

Where social networks at work, most used Twitter (96%), Facebook (93%) and LinkedIn (71%). This selection was based on the top ranked English-language social network service, each with more than 80 million registered users. They were used for personal, professional, advertising and public information purposes – with considerable overlap between the categories.

Benefits
Respondents identified the following benefits of using social networks in their organisations:

- Advertising and promotion
- Professional networking, sharing and collaboration
- Staff awareness and training
- Access to information

Advertising promotion, dissemination and sharing of knowledge were seen as a benefit of social networks. Examples cited included: reaching younger audiences, marketing and promoting services, advertising events. It is seen as a rapid way of disseminating information to target audiences. It was even seen as a way of breaking down information silos in one case. Professional networking was the other major benefit identified by nearly half of the respondents. This included networking with clients, keeping up to date and forming communities of practice/interest.

Among those that do not use social networks at work: staff convenience, keeping staff happy and access to information, were seen as potential benefits.

Risks
The following risks were associated with the use of social networks in the workplace:

- Reputational risk to the organisation if, for instance employees publish defamatory or damaging information on a social networking site. The information has the potential of reaching a large number of people very quickly, with an international reach and involvement of the media. If it is a work-related site or the employee reveals where they work, comments can be attributed back to the employer and there is a concern that the employer could become liable, although one respondent felt that this was a low risk.
- Accidental disclosure of information could lead to loss of intellectual property. Confidential information could be disclosed with data protection of commercial consequences. Once disclosed, the data can be used inappropriately or could, if personal data, be a source of discrimination, bullying or stalking.
- Security breaches by exposing the organisation to malware for instance. Lack of awareness of security issues on the part of users was of particular concern. There are also capacity and service disruption issues related to use of social networks at work.
- Non-compliance with the Data Protection Act and other regulation. This particularly applies if the service provider is outside the UK and consequently personal data is transferred overseas.(with DPA, copyright etc)
- Time wasting during work was another concern if staff become distracted by social networking during working hours
- Other risks identified were compromised data quality, threats to personal safety, breaches of personal privacy and service disruption.

Non-use of social networks

Respondents from organisations that do not allow use of social networks in the workplace were concerned about the temptation for staff to waste time on social networks rather than getting on with their work. Security and the risk of exposure to malware were also mentioned by several respondents, as was the impact of social networks on the bandwidth or other aspects of system capacity. Inappropriate use and compromised privacy or confidentiality were also mentioned, as was reputational risk. Higher organisational or government policy were also quoted as reasons for not allowing use of social networks.

Privacy was a factor for some organisations in deciding whether to allow use of social networks by their staff whilst at work.

Interestingly many non-users said that their organisations could be persuaded to allow use of social networks in the workplace, provided there were guidelines in place to prevent abuse and time-limited access to prevent time-wasting. Several respondents felt that if there was a good business case for use of social networks e.g. to advertise events or as a public information service, they would be allowed.

Protecting personal data

As most of the respondents were responsible for data protection or information governance in their organisations and a wide range of measures was considered for protecting personal data on social networks. When asked what precautions should be in place most respondents envisaged several different methods being used in concert.

Educating users or providing guidelines on use of social networks were the most frequently mentioned precaution. This ties in with ensuring that individuals are aware of their responsibilities for appropriate use of social networks:

> *Employers should ensure that staff receive adequate training in the use of SNS & there is clear guidance on acceptable personal and business use*
>
> *Staff need to be briefed clearly about the implications of sharing their personal information.*
>
> *if access is to be allowed, then a full policy statement on whom is responsible for what needs to be in place and agreed.*

Monitoring and moderation of social network sites were mentioned as possibilities, although there may be some privacy issues attendant on this approach.

Technical measures such as software filters, time-limited access and other security measures should be put in place, although there was no specific mention here of encryption of data. Some felt that the service providers should take greater responsibility for data security:

> *the providers of websites could do more to promote security, and make the most secure setting the default, rather than something you have to select.*

Two respondents mentioned better regulation or enforcement of regulation, which we come to later on, in the context of the Data Protection Act 1998.

When it actually came to implementing precautions, educating users and providing guidelines or policies on use of social networks were the most popular measures. Some organisations restricted access according to specific sites that were approved for work purposes.

Future developments

Many respondents felt that there were no specific developments over the next two years that would affect the use of personal data on social networks. Some thought that, while the internet might influence their work, social networking was specifically excluded.

Those that felt there were developments considered a number of factors, which fell into five main themes:

- Technical
- Managerial
- Legal and Political
- Social and Behavioural
- Economic and Market

The speed of technical change may influence other factors such as improved security measures, possibly applied by the service providers. Emerging technologies such as cloud-based services may continue to develop, because "*institutions are becoming more reliant on this technology*". There may even be the "*development of a private cloud for the public sector*". Another respondent suggested that the "*proliferation of smart phones and tablets will greatly increase the use of social networks*". There may also be developments in the exploitation and use of personal data: "*the need to accept cookies is one area where there may be a rethink on access in some organisations*". Increased data mining is seen as a general threat or as a specific risk to firewall security.

On the management side, at least one organisation is currently reviewing its policy on new and emerging technologies. One respondent foresaw: "*an increased use of social networking sites as a means of corporate communication and data sharing*".

Legal and political changes ranged from war (although it was not clear whether the respondent meant cyberwar, economic war, or direct physical combat) to regulatory issues. Some foresaw increased regulation (including new laws and regulation) or improved enforcement of regulations. For instance, the forthcoming changes to electronic commerce regulations, revision of the European Data Protection Directive, new FCC regulations in the United States and more stringent data privacy laws might all be influences. Others thought that increased non-compliance would be the issue. One felt that "*court cases which may take place and provide legal precedents may help to shape future legislation in this area*".

Social and behavioural influences such as "*more acceptance of it* [social networking] *as a business tool, but with social overtones*" and "*recognition by people that they have little control over the huge portfolio of data they may have shared and published over many years on these sites*" were also considered.

Social networking for marketing purposes may increase over the next two years. This is an economic or market related issues. For instance: "*social search and more blatant targeted marketing may change attitudes amongst users*".

Data Protection Act 1998

Many respondents felt that the UK's Data Protection Act (DPA) was ineffective or only partially effective for protecting personal data on social networks. This reflects an earlier interview with a representative of the Information Commissioner's Office who suggested that the Section 30 (domestic use) and Section 36 (freedom of the press) exemptions excluded social networks from the provisions of the Act. Service providers outside the UK were seen as a barrier to effective implementation of the DPA: "*most social networks go way beyond UK/EU boundaries and the data flies all over the world*" and "*the issue is jurisdiction – why should American firms care about our laws when what they are doing is perfectly legal in their country?*". Another asserted that "*most service providers are based outside the EU, making assertion of rights under DPA ineffective*".

Lack of enforcement was seen as another factor limiting the effectiveness of the DPA. "*Not effective unless enforced*". As one respondent pithily said: "*show me the prosecutions*". Others said "[The DPA] *isn't really enforced strongly and the fines are relatively small*" and "*the penalties are a low threat compared to the benefits of stealing identities*".

Several respondents saw user awareness as a key issue, without which legislation is ineffective: "*what is lacking is education of people as to how their information may be used/stored*", "[The DPA is] *not very effective as many users are ignorant of protection of their personal data*" and "*the public*

ends up in charge of their own protection rather than the site providers. As most people don't have a knowledge of the DPA, this is a concern". Another saw it as an issue of personal responsibility: "*its effectiveness is limited by the fact that people putting up personal info might be construed to be consenting to the distribution of their information*".

There was also a concern that the speed of technological change made it difficult for legislation to keep up: "*I think the DPA is lacking – it's not being adapted of updated to cover emerging technologies*".

Finally, one respondent pointed out that "*there is a mismatch between public concerns when personal data is lost by an organisation, and the degree of personal data that individual are willing to post on SN* [social networking] *sites*".

In contrast, some respondents felt that the Data Protection Act was an effective tool for protecting personal data on social networks or that the situation was improving because of "*increased enforcement powers of the ICO*". In the words of one respondent: "*the ICO has the teeth to prosecute the employer for breaches by those it permits to use social networks on the employer's website*". A number of areas for improvement were identified:

> *"The problem is understanding, application and enforcement – particularly of the individual as a data controller and the limits of the 'domestic purposes' exemption"*
>
> *"I think it is effective, however* [I] *do think that consent should not be implied"*
>
> *"I think it's just about adequate, but public education on the subject is rather limited. The developers of the social networks need to make it clearer about who will see your personal details and easier for users to specify their own restrictions"*
>
> *"The Act is fine, but there is some catching up to do in terms of its application"*

Further comments

There was a perception that protection of personal data was not the main issue in use of social networks in the workplace, nor it is the role of the average organisation to protect personal data on social networks. Barriers such as the high cost of preventive measures would make this impractical. Again there was concern that employers could become liable for the actions of people posting on the site, especially if "*helping to promote (or failing to stop) an environment that is discriminatory/bullying*".

One person mentioned encryption as a way of controlling access to personal data and several respondents suggested that informed consent should be required for disclosure of personal data or for changes to privacy settings of social network systems. Others felt that personal responsibility was the issue: "*we need to rely on the individual's common sense and basic awareness of privacy rights to create social networks that are self-governed and self-policed*" and "*individuals should take responsibility for their actions*". This could tie in with: "*more awareness for users regarding the implications of entering personal and sometimes sensitive personal data*", "*educating and enabling users to look after their information responsibly*", and "*making staff aware of their responsibilities when using social networks.*"

There was a final point about risk:

> *"Like all issues involving the internet, there are risks that are being run now that have not got proper mitigation in place to minimise those risks. Each facilitator and their employees have to assess those risks and put reasonable steps in place to protect the interests of firstly the employer and secondly to retain the convenience of the employee."*

Annex – Survey questionnaire

Social Networks and Privacy

Introduction

Department of Information Science, School of Informatics, City University

Please complete this survey to help identify issues that are of concern to users and potential users of social network services.

For the purposes of this survey, social networks are web-accessible services, in which personal profiles are visible to other users of the service. In other words, individual users provide personal data (such as name, address and occupation) in exchange for access to the social network service and to other users.

This survey is intended to explore the issues associated with access to personal data on social networks. This is part of a research degree at City University London to examine ways in which access to personal data is regulated. The objective of this study is to examine the effectiveness of different methods of regulating access to personal data on social networks.

This survey is directed at users and non-users of social network services. Data gathered in this survey will be consolidated so that individual respondents cannot be identified.

David Haynes, March 2011

1.) Do you have an active profile on a social networking site (such as Facebook, Twitter or YouTube)?

Social networks are web-accessible services which require individual participants to put up personal profiles that are visible to other users of the service. Individuals often have to provide personal data (such as name, address and occupation) in exchange for access to the social networking service and to other users.

( ) Yes

( ) No

Use of Social Networks

2.) Which of the following Social Networking sites do you use?

Tick all that apply

[ ] Facebook

[ ] Twitter

[ ] Tagged

[ ] Orkut

[ ] MySpace

[ ] Badoo

[ ] LinkedIn

[ ] Others (please specify)

3.) How often do you use a social networking site?

*If you use more than one social networking service, please answer for the **most frequently** used service.*

( ) Daily or more often

( ) Once a week or more but less than once a day

( ) Once a month or more but less than once a week

( ) Less often than once a month

4.) What do you consider the main benefits of using social networks?

5.) What do you consider the main risks of putting your personal data on social networks?

6.) What measures or precautions should be taken to protect your personal data on social networking services?

Consider what precautions could be taken by: you; service providers; the industry; national governments; and international regulators.

Non-Users

7.) Is there a particular reason why you do not use social networking services?

Please give details

8.) Was personal privacy a factor in your decision not to use social networking services?

If so, please elaborate

9.) Would anything persuade you to use a social networking site such as Facebook, LinkedIn, FaceBook, Twitter or other social network service?

Please give details

Issues - All respondents

10.) Are there any developments that you think are likely to affect the use of personal data on social networks in the next 2 years?

For instance, are you aware of new services, technology changes, or forthcoming legislation that might have an effect

11.) How effective do you think the Data Protection Act is for protecting personal data on social networks?

The Data Protection Action, 1998 governs the handling and use of personal data collected in the UK, regardless of where it is held. It is based on 8 Data Protection Principles that can be found on the Information Commissioner's website.

12.) Do you have any further comments about the issues surrounding protection of personal data on social networks?

Please give details below

Future contact

13.) If you are interested in the results of this survey or in participating in a follow-up survey, please indicate below:

Please select all that apply. If you give your e-mail address it will only be used for the purposes you have indicated in this response and will not be passed to a third party.

[ ] I would like to be sent a summary of the results of this survey

[ ] I am interested in participating in a follow-up survey

[ ] I am willing to be interviewed

[ ] My e-mail address is:

Thank You!

David Haynes

David Haynes is studying for a research degree at the Department of Information Science in the School of Informatics at City University, London. He can be contacted at: david.haynes.1@city.ac.uk

---

Appendix B – Legislative background to the regulation of access to personal data

This review is intended to provide the legislative background to the regulation of access to personal data on social networks. This is part of an investigation into the nature of regulation and its impact on the use of personal data on social network services (SNS) available to UK users. The review adopts a thematic approach starting with the background to the legislation and then considering each of the data protection principles in turn. The review is focused on regulation as it applies to online SNSs offered to users in the United Kingdom. Legislation is one of four modes of regulation being explored in the wider study. In order to frame this analysis the following questions need to be addressed:

1. What are the rules governing access to personal data on social networks
2. How did the rules come about?
3. How can the situation be improved?

What are the rules?

The starting point for this review is the UK's Data Protection Act 1998 and the European Directives, Regulations and Decisions that apply to this domain. Secondary legislation such as UK Statutory Instruments (Regulations) is also considered. To a lesser extent, non-binding EU Recommendations and Opinions are also taken into account where they relate specifically to social media.

European legislation

UK legislation is governed by the Treaty on European Union 1992 treaty and the earlier EC Accession Treaty signed by the United Kingdom in January 1972 . Treaty based law does not require additional domestic legislation. Voluntary participation by states usually involves the following steps: negotiation, signature, ratification, adhesion, accession. However States can record reservations. Article 21 of the Vienna Convention on the Law of Treaties allows states to make reservations (i.e. exemptions to parts of a treaty by a State). Other bodies have their own regulations such as European Law originating from the European Union. The EU tends not to allow reservations and Article 288 the Treaty on the Functioning of the European Union 2007 defines what is binding under EU law. Need to distinguish between binding law and soft law in making an argument. The United Kingdom is a dualist state in that any international obligations have to be incorporated into national law. However certain acts are directly applicable and do not need to be adopted separately. Regulations governing competition, discrimination and free movement are examples of this.

Laws derived from treaty obligations to the European Court of Human Rights (ECHR) is another area that affects data protection. Unlike the EU, the ECHR allows reservations (Article 57 ECHR)

On social networks the European Economic and Social Committee issued an opinion, which particularly highlights the risks to children and "*those with poor digital literacy*"(*Opinion of the European Economic and Social Committee on the "impact of social networking sites on citizens/consumers" (own-initiative opinion) (2010/C 128/12)*, 2010) . It identifies the concerns about "*the risks of the illegal and abusive use of SNS, which rides roughshod over a number of basic human rights*." It identifies a mixture of threats to individuals (particularly to children) and more generic risks that happen to users of online SNSs. Risks that might be relevant in the workplace include:

- Cyber bullying
- Privacy breaches
- Reputational damage
- Assault on personal dignity

As well as hazards associated with geo-tagging, and facial recognition technologies, spreading of viruses via SNS was also identified. The opinion goes on to recommend measures to improve digital literacy. It suggests that SNS providers should self-regulate or participate in co-regulation at Community or national level. This would allow operators to sign up voluntarily to a code of practice that would be monitored and enforced by the regulatory authorities. It also recommends the appointment of "*a community-level Ombudsman responsible for all issues relating to the protection of human dignity, privacy and data protection in the electronic communications and audiovisual sectors, with specific responsibility for SNS*."

Data Protection Act 1998

In the United Kingdom the Data Protection Act 1998 (DPA) regulates the processing of personal data. Section 6 of the DPA defines the role of the Information Commissioner, appointed by Her Majesty and gives him or her specific powers under the Act. Section 6 also makes provision for appointment of members of an Information Tribunal to hear and determine appeals against a notice from the Information Commissioner. Since 2010 the Information Tribunal has become the Information Rights Tribunal in the General Regulatory Chamber of the First Tier Tribunal. This was formed from the incorporation of a number of tribunals into a centralised tribunal system (*The Transfer of Tribunal Functions Order*, 2010).

Secondary legislation arising from the Act includes statutory instruments and case law that sets precedents in the way in which the law is interpreted. In addition the ICO from time to time issues regulations and guidelines which are available on the ICO website.

Communications Act 2003

The Office of Communications (Ofcom), set up by the Communications Act 2003, does not have a specific interest in regulating privacy, but does have a role in licensing communications service providers. It also has an interest in attitudes to social media which has been the subject of its own research which is considered elsewhere (Office of Communications, 2008).

Regulation of Investigatory Powers Act 2000

Regulation of Investigatory Powers Act 2000 prohibits unlawful interception of communication including electronic communications:

> *1 Unlawful interception*
>
> *(1)It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of:*
>
> *(a)a public postal service; or*
>
> *(b)a public telecommunication system.*

This could apply to personal data on social networks where there is an intent to gain unauthorised access (also covered by the Computer Misuse Act 1990).

Computer Misuse Act 1990

Section 1 of the Computer Misuse Act 1990 states:

> *1 Unauthorised access to computer material.*
>
> *(1)A person is guilty of an offence if—*
>
> *(a)he causes a computer to perform any function with intent to secure access to any program or data held in any computer [F1, or to enable any such access to be secured] ;*
>
> *(b)the access he intends to secure [F2, or to enable to be secured,] is unauthorised; and*
>
> *(c)he knows at the time when he causes the computer to perform the function that that is the case.*

It could be argued that by signing up to a service and voluntarily putting personal data on a social networking site a user is allowing the SNS provider to pass on personal data to third parties and that this therefore does not constitute computer misuse within the terms of the Act. The applicability the Computer Misuse Act depends on 'unauthorised access'. If a data subject gives consent for his or her personal data to be made available via the social network site, it is effectively authorised by them.

Many of the concerns that do arise with personal data are about misuse of the data, not misuse of the computer to gain access to the data.

Human Rights Act 1998

Schedule 1, Article 8 of the Human Rights Act 1998 identifies the following right:

> *Right to respect for private and family life*
>
> *Everyone has the right to respect for his private and family life, his home and his correspondence.*

The UK ratified the Human Rights Treaty in 1953 and enacted its own legislation 1998, which came into force in October 2000. It "*gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights*", which originates from the Council of Europe, a distinct and separate body from the European Union and its agencies.

A Court (defined in the Act) may make a Declaration of Incompatibility if any provisions of a piece of primary legislation are incompatible with any rights under the Convention. This constitutional role means that any primary legislation (whether it has already been enacted or is proposed in a Bill) must observe the right to respect for private and family life.

The Human Rights Act allows individuals to refer their cases to the European Court of Human Rights once all appeals are exhausted in the UK Court system.

As well as the constitutional role of the Human Rights Act, there is the right to privacy which underpins much of the Data Protection Act and the presumed rights of UK residents using social media services.

Secondary legislation and opinions

In the UK statutory instruments are the main source of secondary legislation. These take the form of regulations. Privacy and electronic communications directives are based on European Directives.

In addition to the directives the European Data Protection Supervisor (EDPS) issues Notices and Opinions, which provide additional guidance to European Union institutions, national governments of member countries and citizens of Europe.

Enforcement

The Information Commissioner has powers under the Data Protection Act 1998 and related statutory instruments and orders to enforce the principles of data protection in the UK. The role of the Information Commissioner's Office (ICO) is "*to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals*". As well as monitoring

compliance and taking action where there are breaches of the Act or the Regulations, the Information Commissioner provides advice and guidance. The ICO also has an educative role offering guidelines for young people on protecting their personal data (*Your Personal Little Book about Protecting your Personal Information*, 2009).

The ICO publishes guidelines for organisations about specific data protection issues as well as guidelines targeted at different sectors, such as: business, finance, charities, health, education, local authorities, marketing, and MPs and political parties.

The concept of 'privacy by design' has been around for a long time, and is implied in the European Data Directive which refers to: "*appropriate technical and organizational measures...at the time of the design of the processing system...in order to maintain security and thereby to prevent any unauthorized processing*" (Paragraph 46). The ICO issued guidelines on this in November 2008. The guidelines do not have force of law but are intended to represent good practice for service providers and systems developers. Privacy should be one of the primary considerations when a new information system that handles personal data is being developed. A review funded by the Information Commissioner concluded that privacy by design was increasingly being recognised by data protection authorities as a way of addressing growing concerns about privacy in information systems. The approach seems to work best "*When they are part of a system of incentives, sanctions and review*" (*Privacy by design*, 2008).

The Information Commissioner has the power to impose a monetary penalty on a data controller if he deliberately contravenes the data protection principles. It could be argued that selling personal data from profiles put up on social network services would be seen as a deliberate contravention.

The UK's Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 raised the maximum fine (monetary penalty) that the Information Commissioner could impose to £500,000 for breaches of the Data Protection Act. This SI came into effect in April 2010.

Recent moves have been made to increase the maximum fines for breach of the Act. The ICO has also been active in targeting serious breaches for public sanction by 'naming and shaming' offenders

How did the rules come about?

European Data Protection Directive

European law applies directly and indirectly to the United Kingdom. European legislation or Acts can be divided into binding acts which are mandatory and non-binding Acts. Binding Acts include: Directives, which are addressed to Member States so that they can enact national legislation in compliance with European requirements, and Regulations and Decisions, which are directly imposed by the Commission. Non-binding acts include: Recommendations, Resolutions, Opinions and Communications.

The UK's Data Protection Act 1998 is based on Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, commonly known as the Data Protection Directive (DPD). The Directive is binding on the United Kingdom under the provisions of the Treaty on European Union 1992 (also known as the Maastricht Treaty). The DPD is intended to allow "*the free movement of goods, persons, services and capital*" between Member States and "*also that the fundamental rights of individuals should be safeguarded.*" The DPD refers in several places to "*the right to privacy*" as one of the rights and freedoms of individuals.

The DPA sets up the "*provision for the regulation of the processing of information relating to individuals*" and encompasses the eight Data Protection Principles described in the DPD. These in turn are derived from the OECD Guidelines (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980). This arose from a concern about discrepancies between the privacy laws of different OECD countries which could act as a potential trade barrier by inhibiting the exchange of data between countries. The rapid growth of databanks containing personal data was a particular concern. The table below shows how some of the principles set out in the OECD Guidelines are related to the Data Protection Principles enshrined in the European Data Directive and incorporated into UK legislation as part of the Data Protection Act 1998.

OECD Guidelines	UK Data Protection Act, 1998
Collection Limitation Principle There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	Principle 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless— (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

OECD Guidelines	UK Data Protection Act, 1998
Data Quality Principle Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Principle 4 Personal data shall be accurate and, where necessary, kept up to date.
Purpose Specification Principle The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	Principle 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.
Use Limitation Principle Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: • a) with the consent of the data subject; or • b) by the authority of law.	*See Principle 2 above*
Security Safeguards Principle Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.	Principle 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The OECD principles include the following, which are covered in the main body of the DPA:

"Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above."

(*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980)

The following additional principles have been incorporated into EU and UK legislation:

"Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6

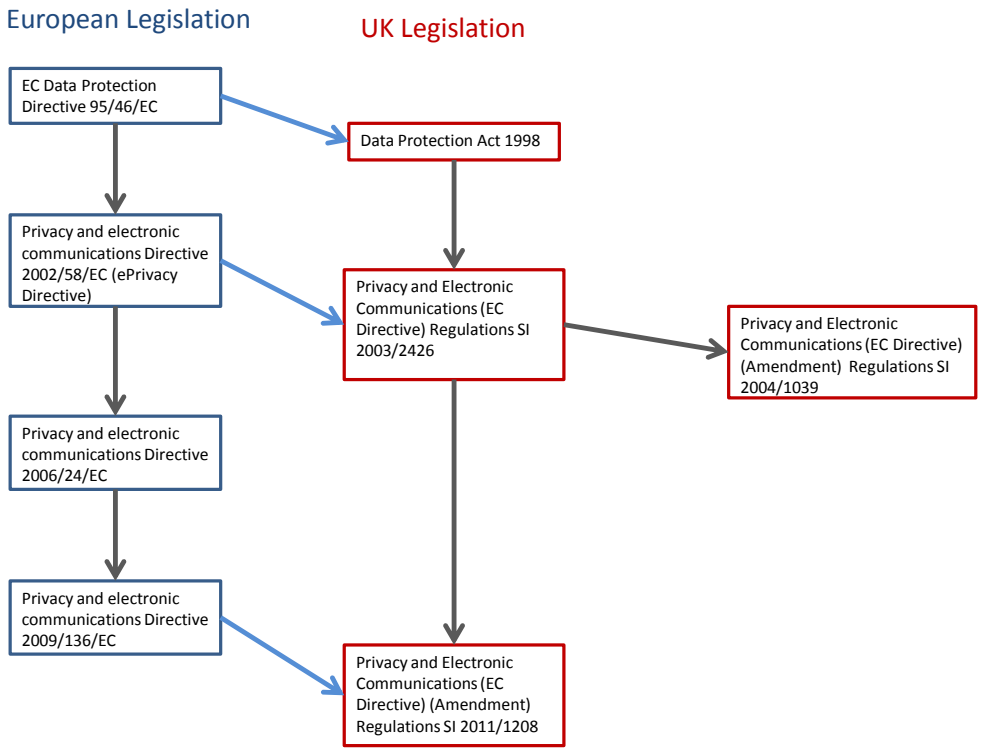
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

There is a clear correlation between the OECD principles and those incorporated into the Data Protection Act. However the Act goes further in developing the concept of trans-border data flow and retention of personal data.

The diagram below illustrates the relationship between major pieces of UK and European data protection legislation. The principle of Subsidiary means that member states of the European Union enact their own legislation within a framework determined by the European Union. European Directives are incorporated into UK national law by means of new legislation, such as the Data Protection Act 1998 (itself replacing the Data Protection Act 1984), or by means of statutory instruments such as the Privacy and Electronic Communications Regulations issued in 2003, 2004 and 2011.



Statutory Instruments

A review of the statutory instruments that have come into effect since the 1998 Act and which might be directly relevant to SNS providers.

Firstly, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 gives a new definition of "*personal data breaches*" and places the obligation on data controllers to notify the information Commissioner of any data breaches. The Regulation makes provision for penalties for failure to do so and specifies that the Information Commissioner should be notified event of a personal data breach. It is an amendment of the Privacy and Electronic Communications (EC Directive) Regulations 2003 and implements Articles 2 and 3 of Directive 2009/136/EC.

The other relevant development is the rationalisation of registration fees for data controllers into two tiers. The Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009 sets the fees payable by data controllers for registration under the DPA at £35 for all charities, companies with a turnover of less than £25.9m and fewer than 250 staff, and for public authorities with fewer than 250 staff. The remainder (so-called "tier 2" data controllers) pay a fee of £500. This might have an effect if any of the SNS providers that decide to submit to UK law.

Exemptions

Part IV of the DPA makes specific exemptions, two of which were highlighted in a telephone interview with an advisor from the Information Commissioner's Office: section 32 'Journalism, literature and art' and section 36 'Domestic purposes'.

The section 32 exemption relates to "*processing ...undertaken with a view to the publication by any person of any journalistic, literary or artistic material*". It goes on to define publish as: "*make available to the public or any section of the public*." Clearly putting up a personal profile on a social network may qualify under this definition, if it becomes visible either to the community of subscribers to that service, or to a wider internet audience through search engines such as Google. Some social networks allow users to restrict the visibility of their profile to a group selected by them, and this would probably fall outside the exemption. The second aspect of this is what constitutes "*journalistic, literary or artistic material*".

Section 36 refers to "*Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes)*". Here the question is whether the data is solely processed by the individual (data subject) user of the service, or whether it is also processed by the service provider and therefore whether it is exempt from the data protection principles. This is very similar to the wording in the European Data Directive (paragraph 24):

> *"Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive"*

Article 3 of the Directive states:

> *"2. This Directive shall not apply to the processing of personal data:*
>
> ...
>
> *-by a natural person in the course of a purely personal or household activity."*

For example Bond raises the issue of data ownership and, specifically, who the data controller is (Bond 2010). He suggests that social network service providers as well as individual users of SNSs have obligations as data controllers. He goes on to say: "*The fact that there is a business driver to the use of social media means ... that the household exemption does not apply and so the question arises as to whether or not the privacy policy notification and other practices of an organisation that is using a service such as LinkedIn for business development purposes are sufficient*."

Section 55 of the Act covers "*unlawful obtaining etc. of personal data*" and states:

"(1) A person must not knowingly or recklessly, without the consent of the data controller-

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data."

However if the data controller is also the social network service provider, presumably they give their consent to pass on personal data to advertisers for the purposes of direct marketing, for instance.

Data protection principles

We saw earlier how the data protection principles enshrined in the DPA have a pedigree reaching back to the OECD Guidelines (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980). These principles provide a good starting point for analysing the applicability of legislation to regulation of access to personal data. As expressed in the DPA, the eight principles which are discussed below. This review now considers each principle in turn.

Principle 1 – Fair and lawful processing

"1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

When the data was gathered was the person from whom it was gathered deceived as to the purpose to which personal data would be put?

There is a view that the DPA does not apply to SNS Providers because it is not clear who the data controller is when it comes to social media. It could be the individual who puts their own personal data up on a social network profile, or it could be the service provider for the social network service. One consideration is that users (who are also data subjects in this context) do not alone "*determine the*

purposes for which and the manner in which any personal data are, or are to be, processed" (DPA, Section 1, subsection 1 defines a data controller). The service provider also processes personal data for the purposes of selling it to advertisers.

At least two of the conditions in Schedule 2 of the DPA (referred to in the first principle listed in Schedule 1 of the Act) could be argued as being met by social network services:

1. The data subject has given his consent to the processing.

In order to gain access to a service, users normally sign up to EULAs (End User Licence Agreements) which make provision for the service provider to utilize and exploit data provided the user. This probably qualifies as 'consent' referred to in Schedule 2, Section 1. This not only applies (in many cases) to personal data on an individual profile, but also information about the individual posted by other users of the service. This could include photographs of individuals automatically tagged by the system or tagged by individuals, including the user directly.

Schedule 3 of the DPA requires that "*explicit consent*" is given to the processing of sensitive personal data, which may be implied when the user signs up to the service. However given the length and complexity of many EULAs, it is unlikely that many individuals would have read the conditions in detail, so would not be able to provide explicit (or informed) consent. Paragraph 33 of the European Data Directive refers to:

> *"Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent"*

Schedule 2, Section 6 of the Act makes provision for the "*legitimate interests pursued by the data controller*" provided it does not prejudice the rights and freedoms of the data subject. As mentioned earlier the Human Rights Act asserts "*Everyone has the right to respect for his private and family life, his home and his correspondence.*" The question then becomes, is this right for a private life contravened by having his or her personal data passed on to third parties by SNS providers?

Principle 2 – Extension of purpose

> *"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."*

If data is gathered for the purposes of providing a social network service to users of the service, it could be argued that selling on that data for financial gain to advertisers is in contravention of the second principle.

The next question has to be whether the data that is 'sold on' to advertisers contains any personal data where a living person can be identified from the personal data or from that and other data in the possession of the data controller.

Section 10 covers the "*Right to prevent processing likely to cause damage or distress*" and could cover, for example, malicious social network entries, hounding by advertisers and spammers and stalking. Section 11 goes on the state the right to prevent processing for purposes of direct marketing, although the onus is on the individual to first provide "*notice in writing to a data controller*" before the courts will intervene.

The data portability theme in the Article 29 Working Party statement raises some of the same issues that were discussed in the 'right to be forgotten' proposal in the EU ePrivacy Directive (2009). Transfer of personal data from one service to another implies that it is removed from the source after it has been copied to the destination. For the reasons described above, there is no absolute guarantee that the data can ever be totally removed from the source. If the data has ever been transmitted via a satellite communications relay, signal leakage means that extra-terrestrial measures (and faster than light travel) would be required to eliminate all copies of personal data. In other words it is impossible to guarantee the elimination of all data once it has been stored or transmitted.

Opinion 2/2010 of the European Commission on online behavioural advertising focuses specifically on the issue of cookies or other tracking devices placed in browsers to follow the behaviour of users online. The Opinion highlights the issue of informed consent and recommends an 'opt-in' principle should be implemented. It also highlights the fact that ad network providers and website publishers effectively become data controllers and have some data protection responsibilities. It is of the view that "*creation of very detailed user profiles...in most cases, will be deemed personal data*". It states that:

> "*Ad network providers should: i) limit in time the scope of the consent: ii) offer the possibility to revoke it easily and iii), create visible tools to be displayed where the monitoring takes place.*"

This reinforces the "*right to refuse*" mentioned in Testimonial 66 of the amended ePrivacy directive when discussing cookies.

Principle 3 – Adequate and relevant data

> *"3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."*

Principle 3 is problematical because personal data is not clearly defined in the context of SNS providers.

Data put up on personal profiles in many social networks falls within the definition of sensitive personal data (section 2) including:

- Racial origin
- Political opinions
- Religious beliefs
- Physical or mental health
- Sexuality

However a lot of the information put up is of a fanciful nature – and may not be accurate or necessarily true. In these cases one might legitimately question whether it qualifies as personal data. For example the Section 32 exemption for literary work might apply. If this is the case, copyright law may apply. It also introduces the question: 'Is the data subject under an obligation to provide accurate or truthful data in these services?'

Principle 4 – Accurate and up-to-date data

"4 Personal data shall be accurate and, where necessary, kept up to date."

Section 14 on "*Rectification, blocking, erasure and destruction*" presents difficulties in that a court may not be able to "*order the data controller to rectify, block, erase or destroy those data and any other personal data ... which appears...to be based on the inaccurate data*." If the data has been entered by the data subject and is (at least partly) based on fantasy, it would be difficult to apply this provision.

Principle 5 – Retention only as long as compatible with purpose

"5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

Principle 5 states that personal data "*shall not be kept for longer than is necessary*". However some social network providers have come into conflict with users that have requested deletion of their profiles. This might arise for instance where the relatives of a deceased member request deletion or removal of a profile from the public domain.

There is the wider issue of policing access to personal data and the fact that it is impossible to truly delete anything from the internet. Once information is in the public domain on the internet or anywhere else, it would seem an insurmountable problem to identify every instance of that data and to require its deletion. In addition there are back-ups to websites – required for operational purposes to which it would be impractical to retroactively apply a deletion and digital archiving projects where

the internet or parts of the internet are being archived for study and as a primary resource for future researchers.

A first reading of the statement from the Article 29 Working Party suggests that personal data is viewed in some respects like a physical entity that has a specific location and can consequently be transferred or destroyed (erased). This belies the enduring nature of data on the internet and the nature of knowledge –that once discovered is impossible to deliberately 'undiscover' information. This would mean that any legislation requiring data controllers to enact the 'right to be forgotten' will be impossible, particularly in the context of social networks and other environments where personal data may be widely distributed.

The 'right to be forgotten' may work better in a controlled environment such as within a company dealing with employee or customer information. Even then, with most data being held electronically, it would be very difficult to ensure that all copies, back-ups and versions of personal data had been removed. The service providers will almost certainly have their own back-up and archiving procedures in place, so that even if data is removed at a user's request it will still persist (although it may not be available online and might be quite difficult to obtain). This makes it very difficult to guarantee imposition of the terms of the 'right to forget'.

Principle 6 – Rights of data subjects

> *"6 Personal data shall be processed in accordance with the rights of data subjects under this Act."*

Principle 6 would require SNS providers to ensure that personal data is processed in accordance with the rights of data subjects under this Act.

Principle 7 – Unauthorised access

> *"7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Recent European directives on electronic communications have modified the scope of the Data Protection Act to regulate electronic monitoring and advertising. The ePrivacy Directive (2009/136/EC) makes specific provision for regulating use of cookies and offering users the right to refuse them and a user-friendly manner (Recital 66). The directive also refers to "*unsolicited commercial communications (spam)*" to allow internet service providers to initiate legal proceedings against spammers. This has a direct impact on the majority of SNS providers.

Principle 8 – Transfer of data beyond the EEA

> *"8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."*

Principle 8 is intended to prevent transfer of personal data outside the EEA unless there is "*an adequate level of protection ... of personal data*". However if the social network provider is extra-territorial, the question of transfer of personal data may be difficult to enforce.

Section 5 deals with application of the Act and states that:

> *"...this Act applies to a data controller in respect of any data only if –*
>
> *The data controller is established in the United Kingdom and the data are processed in the context of that establishment, or*
>
> *the data controller is established neither in the United Kingdom nor in any other EEA State but uses equipment in the United Kingdom for processing the data ..."*

As many social network providers are not based in the UK and deliver their services via the internet, some that the view that the Act does not apply to their services. In other words if the Data Controller is not in the UK or an EEA country, the Act does not apply to them. However paragraph 3 (d) states that the Act applies to:

> *"any person who...maintains in the United Kingdom –*
>
> *An office, branch or agency through which he carries on any activity, or*
>
> *a regular practice"*

This raises the question of what constitutes "*an office, branch or agency*" or a "*regular practice*" and whether provision of an internet service available within the UK falls within this definition.

Some of the major SNS providers such as Facebook, LinkedIn and Google are based in the United States, although many also have offices in the European Union. US operators are covered by the Safe Harbour Agreement between the EU and the US Federal Department of Commerce. The Agreement provides a legal framework that allows transfer of personal data to US based organisation. However its scope and mode of operation is significantly different from the workings of the European Data Directive. In particular there is a concern about its self-regulatory nature, the lack of active enforcement of its provisions, and the lack of any compulsion for independent certification of compliance. The TRUSTe service is one of the main independent certifying bodies. A review of the Safe Harbour agreement suggested that the majority of those firms registered did not fully comply

with its provisions. However some recent commentary suggests that the Federal Trade Commission is beginning to prosecute US firms that breach the terms of the Agreement.

The future – how might the legislation be improved?

Developments in the legislation

In 2009 the European Parliament made a recommendation on strengthening security and fundamental freedoms on the internet[4]. This included:

- Full and safe access to the internet for all
- Strong commitment to combating cybercrime
- Constant attention to the absolute protection and enhanced promotion of fundamental freedoms on the internet; and
- International undertakings

Article 29 Working Party

Article 29 of the Data Protection Directive makes provision for the establishment of a Working Party, with representatives of the national data protection authorities of Member States, plus the EU Data Protection Officer and a representative of the European Commission. As well as an annual report it commissions its own research and consultations and advises the Commission on legislative and other measures that can be taken to improve the data protection framework.

The Article 29 Working Party reviewed the framework for data protection in 2010 in light of changes in technology and emerging practice internationally. The communication, a comprehensive approach on personal data protection in the European Union COM (2010) 609 encompasses legislative and non-legislative measures for data protection. The Communication signals specific intended actions by the European Commission in a number of areas including:

- Notification of breaches
- Data minimisation
- Consent
- Measures for self-regulation and other non-legislative approaches
- Harmonisation of rules and processes

The data minimisation measures have elicited particular comment in the discussion lists:

"The Commission will therefore examine ways of:

- strengthening the principle of data minimisation;

[4] Strengthening security and fundamental freedoms on the internet European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the internet (2008/2160(INI))

- improving the modalities for the actual exercise of the rights of access, rectification, erasure or blocking of data (e.g., by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle);

- clarifying the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired;

- complementing the rights of data subjects by ensuring 'data portability', i.e., providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers."

From this we can conclude that even legislators and state regulators acknowledge the need for non-legislative measures for data protection.

Legislation cited

European and International legislation

(*Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services*, 2009)

(*Opinion 2/2010 on online behavioural advertising*, 2010)

(*Opinion of the European Economic and Social Committee on the "impact of social networking sites on citizens/consumers" (own-initiative opinion) (2010/C 128/12)*, 2010)

Accession Treaty (*Treaty between the Member States of the European Communities and the Kingdom of Denmark , Ireland and the United Kingdom of Great Britain and Northern Ireland*, 1972)

Data Protection Directive (*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*, 1995)

Maastricht Treaty (*The Treaty on European Union*, 1992)

Treaty of Rome (*The Treaty on the Functioning of the European Union*, 1957)

UK legislation

Communications Act 2003 (*Communications Act*, 2003)

Computer Misuse Act 1990 (*Computer Misuse Act*, 1990)

Constitutional Reform Act 2005 (*Constitutional Reform Act*, 2005)

Data Protection Act 1998 (*Data Protection Act*, 1998)

Freedom of Information Act 2000 (*Freedom of Information Act*, 2000)

Human Rights Act 1998 (*Human Rights Act*, 1998)

Regulation of Investigatory Powers Act 2000 (*Regulation of Investigatory Powers Act*, 2000)

ePrivacy Regulations (Amendment) 2011 (*The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations*, 2011)

ePrivacy Regulations 2003 (*The Privacy and Electronic Communications (EC Directive) Regulations*, 2003)

(*The Data Protection (Notification and Notification Fees) (Amendment) Regulations*, 2009)

(*The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations*, 2010)

(*The Transfer of Tribunal Functions Order*, 2010)

Appendix C – Review of Privacy Policies of online SNS providers

Introduction

The privacy policies published by SNS providers represents a self-regulatory approach to protecting users' interests. They are also subject to legislative regulation as may be seen by the 2012 findings by CNIL, the French regulators, on Google's consolidated privacy policy for all its public services (*Google Privacy Policy: Main Findings and Recommendations*, 2012, *Letter to Larry Page, Google from the European Privacy Authorities 16 October 2012*, 2012).

Boyd and Hargittai report on concerns about privacy settings on Facebook and suggests that contrary to many assumptions, users of Facebook are concerned about the risks associated with personal information by on SNSs (D. Boyd & Hargittai, 2010). This reflects more general concern about what personal data is held by SNS providers and the way in which it is being used. Access to personal data on social networks is regulated in a number of ways. This investigation looks at one of these, self-regulation and its expression in the privacy policies of the main social network providers. It goes on to consider the relationship between privacy policies and legislation.

A review of the privacy policies of the nine most popular global SNSs available to English-speakers was undertaken in October – December 2011. The rankings were initially identified by Wikipedia entry which referred to the Alexa page rankings. The table was cross-checked with Alexa.com website. The actual ranking may not be too critical – as long as we can be sure that the major providers have been picked up in this way. The method of ranking is more significant when smaller, more specialist social network services are involved. The following SNS providers' privacy policies were analysed in this investigation:

SNS Name	Description/Focus	Date launched	Registered users	Registration	Global Alexa[1] Page ranking
Facebook	General.	February 2004	800,000,000+[86]	Open to people 13 and older	2[87]
Twitter	General. Micro-blogging, RSS, updates	July 15, 2006	300,000,000[303]	Open	9[304]
Badoo	General, Meet new people, Popular in Europe and Latin America	2006	133,000,000[15]	Open to people 18 and older	117[16]
LinkedIn	Business and professional networking	May 2003	120,000,000[174]	Open to people 18 and older	13[175]
Bebo	General	July 2005	117,000,000[17]	Open to people 13 and older	2,279[18]
Orkut	General. Owned by Google Inc. Popular in India and Brazil.[230]	January 22, 2004	100,000,000[231]	Open to people 18 and older, (Google login)	106[232]
Myspace	General	August 2003	100,000,000+[207][208]	Open to ages 13 and older.	131[209]

SNS Name	Description/Focus	Date launched	Registered users	Registration	Global Alexa[1] Page ranking
Google+	General	June 28, 2011	50,000,000[130]	General, Open	NA (Alexa only records data for Second-level domains)
Ning	Users create their own social websites and social networks			Open to people 13 and older	273[223]

("List of Social Networking Websites," 2011)

The Weft QDA software was used to assist with coding of the policies for the purposes of data analysis. The review of the privacy policies set out to answer the following questions:

- To what extent do privacy policies regulate access to personal data?
- What protections do privacy polices offer to UK users of SNSs?
- Who do privacy polices relate to other forms of regulation? – do they for instance refer to legislation?
- What remedies are afforded to users for breach of privacy?
- Is there a way of enforcing privacy policies
- Do policies change in response to legislation or other pressures (e.g. court cases or rulings by privacy commissioners)?

What information is held about a user?

Social network providers collect a wide range of data about their users. Some of this is compulsory, and much of it is voluntary, as it depends on what individuals choose to put on their profiles. However some information is effectively collected without informed consent (i.e. the user is either unaware or not fully informed about the extent and type of data that is gathered from other sources). For example, Facebook, Google+ and Orkut allow members to tag photos with the names of those pictured in the photographs. In December 2010 Facebook started rolling out a facial recognition feature that automatically suggests tags for photos on members' profiles using facial recognition software. This was reported on by several commentators, including the Electronic Frontier Foundation (Galperin, 2011).

Mandatory personal data

As a minimum most SNS providers require name, e-mail address and password in order to set up and use an account. Google+ stipulates username rather than name. Badoo and Facebook require date of birth, gender and location. LinkedIn requires gender, location and employer name.

Voluntary personal data

Depending on the SNS, users can add a range of personal data including the following mentioned in the privacy policies: religion, sexual preference, ethnic background, interests and hobbies, as well as adding content such as blogs, playlists, photos and videos and comments. For some services such as Twitter, adding a location is also optional.

Other users

However it is the information not explicitly requested from users that raises a concern about consent. If a user is not made aware that such data is being gathered it is difficult for them to make meaningful decisions (or indeed any decisions) about who should have access to that data. This additional data may come from other users, or from tracking data gathered by the SNS provider. A distinction must be made between aggregated data, which is dealt with later, and personal data where an individual can be identified.

Facebook, Google+ and Orkut all mention tagging by other users. For instance, if someone tags a photo with a personal name (the policy is directed at users, but it is not clear what protections are available to non-users whose photos are tagged), that information is added to your profile. With all three services the user has the option of whether the tagged content appears on their profile or not. Facebook allows users to block someone from tagging content with their name in future, but it is not clear whether this can also be retroactive. Orkut allows users to opt out of being tagged via the personal preference settings, and Google+ allows users to remove personal tags.

Third parties

Most of the privacy policies mention third parties, normally developers of APIs or service providers. In some cases they also include advertisers purchasing access to members of a SNS. Badoo and Bebo do not provide personal data to advertisers and LinkedIn states: "*We do not rent, sell, or otherwise provide your personally identifiable information to third parties without your consent, except as described in this policy or as required by law*."

The other policies state what they do provide and the conditions that apply. Several make the distinction between data gathered by them and by the third party. In the latter case users are advised to check the privacy policies of the third parties. For instance Ning states:

> *"Any Personal Information you provide on third-party sites or services is provided directly to that third party and is subject to that third party's policies governing privacy and security. We are not responsible for the content or privacy and security practices and policies of third-party sites or services. We encourage you to learn about third parties' privacy and security policies before providing them with Personal Information."*

Ning may obtain information from third parties: "*This includes certain Personal Information that may be provided to us through the installation and use of Ning Applications on third party web sites*." Where this is combined with personal data on the Ning platform, this is treated as personal data and falls within the remit of Ning's privacy policy.

Tracking usage

The other type of personal data gathered automatically by most SNS providers is tracking data. This requires use of tracking technology to record activity and behaviour, both within the SNS and on the internet generally.

Several of the privacy policies provide an explanation of tracking technologies and how they are used. The two most commonly cited technologies are cookies and web beacons. They are used to customise the user experience of the SNS facilitating login, preferences and keeping track of individual sessions.

Google+, LinkedIn, Orkut, Ning and Twitter all state in their privacy policies that they track user activity. LinkedIn does this "*in order to accurately categorize and respond to customer inquiries and investigate breaches of our terms*". Twitter describes the data it gathers as: "*Log Data* [which] *may include information such as your IP address, browser type, the referring domain, pages visited, your mobile carrier, device and application IDs, and search terms.*" It also states that this data persists for up to 18 months.

Tracking technologies are also used for delivering advertising to users, or to gather data about user preferences for behavioural advertising. For instance a users' pattern of web interactions and sites visited may trigger ads from suppliers relevant to the sites visited.

Badoo, LinkedIn and Ning all mention that third parties may place cookies on the browsers of visitors to the SNS. However they all warn that as SNS providers they have no control over what the third parties do with them.

Several SNS providers offered links to further information on how to disable or block cookies. However they emphasise the benefits of tracking technologies and suggest blocking cookies may limit the range of services and the functionality of the site. Bebo refers users to the Network Advertising Initiative to opt out of targeted ads.

One provider states that it transfers personal data to advertisers: "*Bebo may transfer information about you and your use of Bebo, such as your name, personal contact information, IP address, information stored via cookies, and other demographic information about you, to advertising affiliates*".

A couple of providers state that they will not pass on personal data to third parties. For instance the Facebook privacy policy states: "*We may also ask advertisers to serve ads to computers, mobile phones or other devices with a cookie placed by Facebook (although we would not share any other information with that advertiser).*" LinkedIn states: "*Any information provided to third parties*

through cookies will not be personally identifiable but may provide general segment information (e.g., your industry or geography, career field, or information about your professional or educational background) for the enhancement of your user experience by providing more relevant advertising." Orkut keeps personally-identifiable data separate from data gathered by cookies, the implication being that this is not passed on to third parties, but not explicitly stated.

Aggregated data

Most of the policies reviewed make a distinction between personally-identifiable data and aggregated data. Where information about an individual cannot be identified from the aggregated data it falls outside the definition of personal data discussed at the start of this paper.

Aggregated data consists of system and behavioural data gathered by the SNS providers, such as IP address, browser used, sites visited, options selected, as well as general categories (sometimes self-defined) and characteristics selected by advertisers such as: age, gender, occupation, location, and interests. The data is used for marketing and promotion, industry analysis and demographic profiling (Badoo), service provision (Bebo and Twitter) and advertising (Facebook, Orkut and Twitter).

Who has access to personal information?

Types of audience

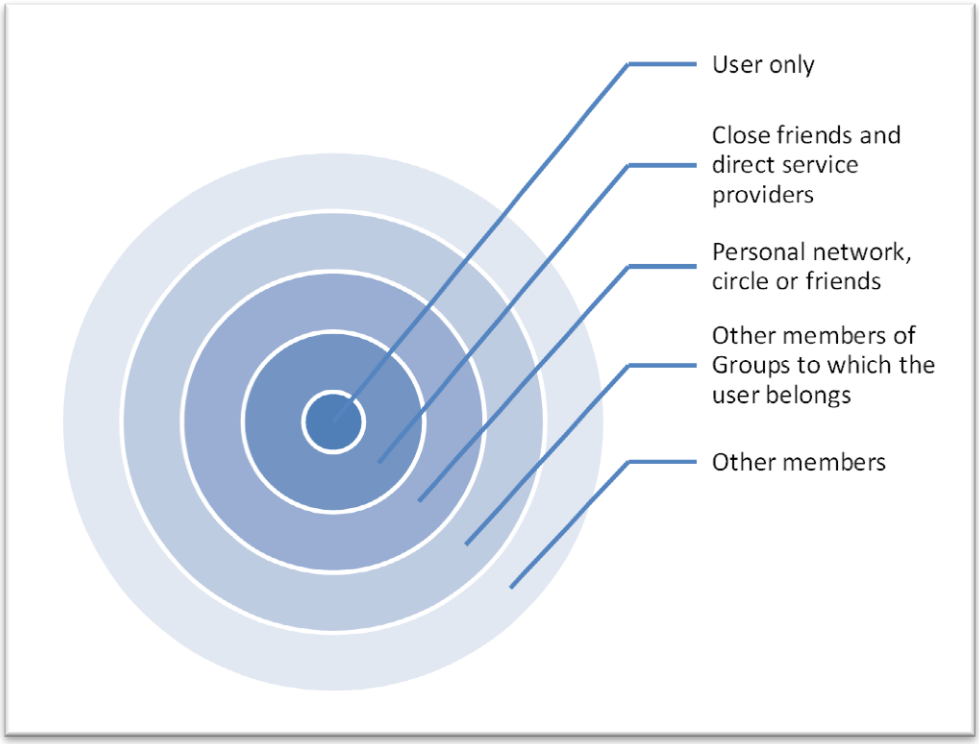
One key aspect of privacy is control over who has access to personal information. There may be degrees of privacy, depending on the sensitivity of the information and how widely it is circulated. Some of the privacy policies attempt to define different types of audience for personal data or content posted by users. For instance Facebook allows users to select: Public (anyone including non-members of Facebook), Facebook Friends, and Customised audiences.

Degrees of closeness

A user may put information on his or her profile in the expectation that it is only available to their network, circle or friends. Other information may be intended for a more general audience, such as in LinkedIn where part of the purpose of joining is to see job and business opportunities. Some information may be made available to advertisers paying for access to personal data. There are different rings of access to personal data depending on its sensitivity, and the potential risk associated with providing access to it.

The further out from the centre, the less sensitive the information. For example, the inner circle might include financial information and personal data such as date of birth for verification purposes. The next level may include sensitive information such as personal interests and data required to complete transactions such as purchasing. This might be shared by close personal friends or direct

service providers. A wider group is designated contacts, networks (LinkedIn) , friends (Facebook) or circles (Google). A less personal group might be other members of group or discussions to which a user belongs. This identifies others with a similar common interest, but a user many not necessarily want members of one group to know which other groups he or she belongs to. For example, belonging to a church choir and a work-based football team may not have many synergies. The outer circle is other members of the SNS service. Beyond the outer ring, is the general public, including non-members of the SNS.



Sometimes there is an assumption that personal information on profiles is only available to other members of the network. However for the general SNSs reviewed in this paper, this is not always the case. For instance, both Facebook and LinkedIn state that profiles are visible to external search engines and are therefore discoverable by non-members of the SNS.

Law enforcement agencies

Several of the privacy policies refer to the right to make personal data available to law enforcement agencies or as part of legal obligations or court proceedings. Although not specified in any of the policies viewed, this could include a requirement to make personal data available to security services and agencies in the United States under the Homeland Security Act. This has been covered extensively by the Electronic Frontier Foundation on its website (www.eff.org).

Control of access to personal data

All the privacy policies reviewed offered some degree of advice or guidance to users on protecting their privacy. This ranged from detailed instructions how to change privacy settings to general advice on being aware of who might be able to access any content put up on personal profiles or in postings.

Being able to opt in to services where personal data is provided or out of default settings were given as possible controls by some of the SNS providers. For instance, LinkedIn, Ning and Orkut all explicitly allow users to opt out of receipt of advertisements. LinkedIn has opt out clauses for surveys, social ads, and providing contact information to other users. Google's privacy policy is the only one that offers an opt in for users to share sensitive personal data with third parties. MySpace offers an opt out to the appearance of users' content in other users' streams.

Some providers offered the ability to amend or delete personal information gathered from other sources. This particularly applied to tagging of photos or videos in which a user appears and is identified by other users. However this is not always easy and is not necessarily retroactive.

Informed consent is not a concept that appeared in any of the privacy policies, yet it is essential for any meaningful control over personal data. For example, it is not always clear what the default privacy settings are, or they are changed without users' knowledge or consent. Facebook addresses this by stating in its privacy policy that: "*If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances*." However this commitment to inform users about changes to policy falls short of a commitment to notify users of changes to default privacy settings on the network.

Where access to personal data is under the control of the user, some SNS providers offer guidance and advice on what information should be made available via their profiles. For instance Badoo warns: "*We also do not recommend that you put email addresses, URLs, instant messaging details, phone numbers, full names or addresses, credit card details, national identity numbers, drivers' licence details and other sensitive information in your Profile which is open to abuse and misuse*." There is a more general warning from another SNS provider: "*Bebo recommends that you exercise discretion in deciding what information you disclose on the internet or otherwise*."

The ultimate control of personal data is the right to remove it from a social network site. SNS providers gather data about individuals, both members and potential members form a variety of sources. This means that for instance there may be a 'shadow' profile of an individual on a SNS

even before they register to join. Once someone becomes a member, further data may be gathered from other users or from reports of internet activity via other websites. When someone dies, providers such as Facebook allow close relatives to apply to have a profile removed. An alternative is to memorialise a profile – so that friends and family can use the SNS as a way of remembering the deceased.

Badoo will deactivate an account for 30 days on request for removal, before deleting the account. This allows users to change their minds. However some data will persist for longer until routine housekeeping operations are able to remove remaining data. Bebo has a similar 30 day grace period before permanent deletion of a profile. Facebook will deactivate and then delete an account at the users' request, taking up to 90 days to purge all personal data relating to the user. Google will amend or delete personal data at a users' request, once they have verified their identity. LinkedIn will also remove a profile at a user's request although they reserve the right to keep certain data for law enforcement purposes. They also warn that any data shared with other users cannot be recalled. Orkut suggests that some data will persist in back-up copies even after the deletion request is completed. Twitter also deactivates an account for 30 days before beginning the deletion process, which can take up to 7 further days.

Relationship to legislation

Legislation represents one of the main modes of regulation of access to personal data, along with self-regulation as expressed in privacy policies. Some of the privacy policies refer to the legislation that might apply to the gathering, storage and processing of personal data. In the UK the main legislation regulating access to personal data is the Data Protection Act 1998. In an interview with an advisor from the Information Commissioner's Office (given powers of regulation under the Data Protection Act), it was suggested that personal data on SNSs might be exempt under Sections 32 and 36 of the Act.

The Section 36 exemption depends on who is defined as the data controller. It could be argued that if an SNS provider is managing, aggregating and selling access to personal data that they become the data controller. This is especially the case where data is gathered passively from users or where there is limited opportunity to provide informed consent on usage of personal data. This contradicts the stipulation that the exemption applies to: "*personal data processed by an individual only for the purposes of that individual's personal, family or household affairs*".

One analysis of the application of the Data Protection Act to SNSs suggests that the definition of a data controller is ambiguous when applied to SNSs. Comparison of legislation in Sweden, Germany, Canada, Australia and the UK provide varying views on this. Some SNS providers explicitly state

the scope of the definition of a data controller in relation to their own services (Garrie & Wong, 2010).

The Section 32 exemption is more problematical "*processing ... undertaken with a view to the publication by any person of any journalistic, literary or artistic material*" – in that any postings made by a user or indeed by other users could be viewed as journalism and covered by the right to freedom of expression. Again however, there is considerable personal data on many SNS user profiles that is not directly contributed by users and could therefore not be described as journalistic. This paper would therefore argue that personal data held on a SNS does not qualify for the exemptions in Sections 32 and 36 of the Data Protection Act and is therefore not exempt from the provisions of the Act.

Woods describes the tension between freedom of expression and privacy in SNSs. For instance the use of SNS postings by the media may conflict with the intention of users that content they post will not be widely distributed. Wider distribution of user-generated content could be seen as a tort of misuse of private information. It may also be seen as infringing on the right to a private life enshrined in the Human Rights Act (Woods, 2012). The Press Complaints Commission excludes "*user-generated and non-edited material*" from the Code's remit in online publications (Press Complaints Commission, 2012).

Jurisdiction for the service

This study focuses on self-regulation as embodied in the privacy Policies published by the 10 most popular SNSs available to English-speakers in the United Kingdom. These services are all global in scope and may result in personal data being held and processed in other jurisdictions. The privacy policies refer to the following jurisdictions. Two SNS providers warn of the consequences of extraterritoriality: "*Badoo is a global website operating through servers located in a number of countries around the world, including the United States. If you live in a country with data protection laws, the storage of your personal data may not provide you with the same protections as you enjoy in your country of residence*." Ning states: "*If you use the Ning Platform from the European Union, or any other region with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal data to the United States. The United States does not have the same data protection laws as the European Union and other regions*." The following table shows how some of the service providers define jurisdiction:

Service	Jurisdiction and location of data
Badoo	*"This policy and any dispute or claim arising out of or in connection with it or its subject matter (including non-contractual disputes or claims) shall be are governed by and construed in accordance with English law."*
Bebo	*"Personally identifiable information collected in connection with your use of the Bebo Service may be transferred to, or stored in the United States, or other countries where Bebo or its parent, affiliates, subsidiaries or service providers maintain facilities ... By using the Bebo Service, you expressly agree to the transfer to the United States and elsewhere of your personally identifiable information.* *Any disputes arising from this Privacy Policy shall be governed by the laws of the State of California, and if you and Bebo cannot resolve such disputes, the matter shall be brought in and decided by the courts of the State of California."*
Google	*"Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information outside your own country.* *We will cooperate with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between Google and an individual."*
Ning	*"International Users. The Ning Platform is hosted in the United States. If you use the Ning Platform from the European Union, or any other region with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal data to the United States. The United States does not have the same data protection laws as the European Union and other regions. By providing Personal Information under this Privacy Policy, you consent to the use of Personal Information in accordance with this Privacy Policy and the transfer of your Personal Information to the United States."*
Twitter	*"Irrespective of which country that you reside in or create information from, your information may be used by Twitter in the United States or any other country where Twitter operates."*

Safe Harbor and TRUSTe

As a member of the European Union, UK users are afforded protection under the European Data Protection Directive, enacted in the UK as the Data Protection Act 1998 and associated statutory

instruments and regulations (*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*, 1995). In order to allow freedom of movement of data between the United States and the European Union a Safe Harbor agreement has been signed. This is a voluntary, self-certifying code which is available for view on the United States Federal Department of Commerce website. Previous analysis of Safe Harbor registrations suggests that not all the provisions of this framework are complied with and that there is therefore a question about its effectiveness in ensuring the rights of individuals to effective data protection. The table below shows the fairly standard statement of compliance with Safe Harbour:

Service	Safe Harbor provisions
Bebo	*"Bebo adheres to the EU Safe Harbor framework as set forth by the Department of Commerce regarding the collection, use, and retention of data transferred from the European Union."*
Facebook	*"Safe harbour. Facebook complies with the EU Safe Harbor framework as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. As part of our participation in the Safe Harbor, we agree to resolve all disputes you have with us in connection with our policies and practices through TRUSTe. To view our certification, visit the U.S. Department of Commerce's Safe Harbor website at: https://safeharbor.export.gov/list.aspx"*
Google	*"Enforcement. Google complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Google has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Google's certification, please visit the Safe Harbor website."*
Google+	*"Google adheres to the U.S. Safe Harbor privacy principles. For more information about the Safe Harbor framework or our registration, see the Department of Commerce's web site."*
LinkedIn	*"LinkedIn Corp participates in the EU Safe Harbor Privacy Framework as administered by the United States Department of Commerce as a data controller,*

Service	Safe Harbor provisions
	and has self-certified our privacy practices as consistent with U.S.-E.U. Safe Harbor principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, Data Integrity and Enforcement."
Ning	*"Ning complies with the EU Safe Harbor framework as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. Information regarding the E.U. Safe Harbor Framework can be found at http://export.gov/safeharbor."*
Orkut	*"Google adheres to the US Safe Harbor privacy principles. For more information about the Safe Harbor framework or our registration, see the Department of Commerce's web site."*

A further line of investigation will be to view the Safe Harbor registrations of the SNSs reviewed here and to discover the extent to which they comply with the data protection principles laid down in the European Directive.

LinkedIn and Ning both specifically mentioned TRUSTe as an independent certification agent. The TRUSTe website provides the following information (3 January 2012):

SNS Provider	TRUSTe Service Used
LinkedIn	Dispute Resolution EU Safe Harbor Seal Web Privacy Seal
Ning	EU Safe Harbour Seal Trusted Cloud

The EU Safe Harbor Seal by TRUSTe verifies compliance with the Safe Harbor framework operated by the US Department of Commerce and replaces the self-certification provision in the framework. Dispute resolution is another service that directly relates to privacy protection and the safe harbour provisions. LinkedIn refers users to this service in its privacy policy.

References

Angwin, J., & Mcginty, T. (2010). Personal Information Exposed Via Biggest U.S. Websites - Protect Your Privacy - WSJ.com. *Wall Street Journal*. Retrieved September 16, 2012, from http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html

Applause Store Productions Ltd. & Anor v Raphael. (2008). Retrieved from http://www.bailii.org/ew/cases/EWHC/QB/2008/1781.html

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research, 12*(1), 1–11. doi:10.1080/13669870802488883

BBC News. (2011). Facebook U-turns on phone and address data sharing. BBC. Retrieved September 18, 2012, from http://www.bbc.co.uk/news/technology-12214628

Bickerstaff, R. (2009). *Towards a Commons Approach to Online Privacy for Social Networking Services – a " Privacy Commons "* (p. 24pp).

Blank, G. (2010). Trust and the Internet : 2003-2009. *OxIS Workshop, London 5 October 2010* (p. 19pp). Oxford: Oxford Internet Institute.

Bogdanor, V. (2009). *The new British Constitution* (p. 319). Oxford: Hart Publishing.

Bonneau, J., & Preibusch, S. (2009). The Privacy Jungle : On the Market for Data Protection in Social Networks. *Workshop on the Economics of Information Security, 2009* (p. 45pp).

Boudreaux, C. (2011). Social Media Policies in Social Media Management Handbook (Editors: N Smith and R Wollan) (pp. 273–285). Hoboken, NJ: Joh Wiley.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: who cares? *First Monday*, *15*(8), 2pp. Retrieved from (www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 11.

Brady, H. E., & Collier, D. (Eds.). (2004). *Rethinking social inquiry : diverse tools, shared standards* (p. 362). Lanham, Md. ; Oxford: Rowman & Littlefield. Retrieved from Table of contents http://www.loc.gov/catdir/toc/ecip0416/2004008240.html

Buckley Owen Cooke, L., Matthews,G., B. (2012). Information Policymaking in the United Kingdom: The Role of the Information Professional. *Journal of Information Policy*, *2*(0). Retrieved from http://jip.vmhost.psu.edu/ojs/index.php/jip/article/view/82

Cannataci, J., & Bonnici, J. P. M. (2003). Can Self-regulation Satisfy the Transnational Requisite of Successful. *International Review of Law, Computers & Technology*, *17*(1), 51–61.

Cavazza, F. (2010). The Social Medial Landscape 2011. Retrieved September 16, 2012, from http://www.fredcavazza.net/2010/12/14/social-media-landscape-2011/

Charles Booth Online Archive. (n.d.).*London School of Economics*. Retrieved September 18, 2012, from http://booth.lse.ac.uk/

Charmaz, K. (2006). *Constructing grounded theory : a practical guide through qualitative analysis*. London: Sage.

Christiansen, L. (2011). Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven? *Business horizons*, *54*(6), 509–514. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=25914006&site=ehost-live

Clapperton, G. (2009). *This is social media: tweet, blog, link and post your way to business success* (p. 180). Chichester, UK: Capstone.

Collins, R. (2006). Internet Governance in the UK. *Media culture and Society*, *28*(3), 337–358.

Comm, J. (2010). *Twitter Power 2.0: How to dominate your market one Tweet at a time* (p. 268). Hoboken, NJ: John Wiley & Sons, Inc. / Business.

Communications Act (2003). Retrieved from http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf

Computer Misuse Act (1990). Retrieved from http://www.legislation.gov.uk/ukpga/1990/18

Connolly, C. (2008). *The US Safe Harbor - Fact or Fiction ? (2008) Version* (p. 18pp). Prymont, NSW, Australia. Retrieved from http://www.galexia.com/public/research/articles/research_articles-pa07.html

Constitutional Reform Act (2005).

Data Protection Act (1998).

Delbridge, R., & Kirkpatrick, I. (1994). Theory and Practice of Participant Observation. In V. J. Wass & P. E. Wells (Eds.), . Aldershot, Hants, England ; Brookfield, Vt.: Dartmouth.

Denham, E. (2009). *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.* (p. 113pp). Ottawa.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Pub. L. No. Directive 2009/136/EC (2009). OJ L 337, 18.12.2009, p. 11–36.

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 (1995). Official Journal L 281 , 23/11/1995 P. 0031 - 0050.

Dry, S. (2007). *Fishermen and forecasts : how barometers helped make the metrological department safer in Victorian Britain*. *Discussion paper ; no. 46* (p. 30). London: London School of Economics and Political Science, Centre for Analysis of Risk and Regulation.

Dutton, W. H., & Blank, G. (2011). Next Generation Users: The Internet in Britain. Oxford Internet Survey 2011 Report. Oxford, UK: Oxford Internet Institute. Retrieved from http://microsites.oii.ox.ac.uk/oxis/

Feldman, D. (1989). The Nature of Legal Scholarship. *The Modern Law Review*, *52*(4), 498–517. Retrieved from http://www.jstor.org/stable/1096178

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining Risk. *Policy Sciences*, *17*(2), 123–139. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=16854183&site=ehost-live

Freedom of Information Act (2000).

Galperin, E. (2011). How to Disable Facebook's Facial Recognition Feature. Retrieved January 3, 2012, from www.eff.org/deeplinks/2011/06/how-disable-facebooks-facial-recognition-feature

Garrie, D. B., & Wong, R. (2010). Social networking: opening the floodgates to "personal data." *Computer and Telecommunications Law Review*, *16*(6), 167–175.

Glaser, B. G. (1978). *Theoretical sensitivity : advances in the methodology of grounded theory*. Mill Valley Calif: Sociology Press.

Glaser, B. G., & Strauss, A. L. (1966). The Purpose and Credibility of Qualitative Research. *Nursing Research*, *15*(1), 56–61.

Glaser, B. G., & Strauss, A. L. (1967). *The Discoveryof Grounded Theory: strategies for qualitative research*. Transaction Publishers.

Gomez, J., Pinnick, T., & Soltani, A. (2009). *KNOW PRIVACY* (p. 44pp). Berkeley, CA.

Google Privacy Policy: Main Findings and Recommendations. (2012). (p. 9pp). Paris.

Great Britain. Better Regulation Commission. (2006). *Risk, responsibility and regulation - : whose risk is it anyway?* (p. 55). London: Better Regulation Commission.

Hammock, M. R., & Rubin, P. H. (2011). *Applications Want to be Free: Privacy Against Information*. Washington DC: Technology Policy Institute.

Hansson, S. O. (2010). Risk: objective or subjective, facts or values. *Journal of Risk Research*, *13*(2), 231–238. doi:10.1080/13669870903126226

Haufler, V. (2001). *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*. Washington, D.C.

Haythornthwaite, R. (2006). *The regulation of risk : setting the boundaries* (Vol. 16, p. 13). Bath: University of Bath.

Heffernan, S. (2011). UK financial reform post crisis: is more regulation the answer? In T. Green, CJ; Pentecost, EJ; WeymanJones (Ed.), *Financial Crisis and the Regulation of Finance* (pp. 193–211). Cheltenham: EDWARD ELGAR PUBLISHING LTD. Retrieved from http://0-apps.webofknowledge.com.wam.city.ac.uk/full_record.do?product=UA&search_mode=GeneralSearch&qid=6&SID=R232KJ2bpDa2lj3FCFM&page=1&doc=1

Heyvaert, V. (2011). Governing Climate Change: towards a new paradigm for risk regulation. *The Modern Law Review*, *74*(6), 817–844. Retrieved from http://ejournals.ebsco.com/direct.asp?ArticleID=463DB9C1BE77DEDDC276

Hjørland, B. (2002). Domain analysis in information science: Eleven approaches - traditional as well as innovative. *Journal of Documentation*, *58*(4), 422–462. doi:10.1108/00220410210431136

Home Office Draft Communications Data Bill, Cm8359 (2012). London: England and Wales.

Human Rights Act (1998). Retrieved from http://www.legislation.gov.uk/ukpga/1998/42

Hustinx, P. (2010). Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA). *Official Journal of the European Union*, *C*(147), 1–13.

Hutter, B. M. (2005). *The Attractions of Risk-based Regulation*. *Centre for Analysis of Risk and Regulation. Discussion Paper no. 33. March 2005*. Centre for Analysis of Risk and Regulation.

Johnson, B. (2010). Privacy is no longer a social norm says Facebook founder. The Guardian.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), 59–68. doi:10.1016/j.bushor.2009.09.003

LaRose, R., Lin, C., & Eastin, M. (2003). Unregulated Internet Usage: Addiction, Habit, or Deficient Self-Regulation? *Media Psychology*, *5*(3), 225–253.

Lessig, L. (2006). *Code : version 2.0 ; Lawrence Lessig* (Vol. 2nd, p. 410). New York; London: BasicBooks; Perseus Running, distributor.

Letter to Larry Page, Google from the European Privacy Authorities 16 October 2012. (2012). (p. 5pp). Brussels.

List of Social Networking Websites. (2011).*Wikipedia*. Retrieved December 29, 2011, from http://en.wikipedia.org/wiki/List_of_social_networking_websites

Liu, K., & Terzi, E. (2010). A Framework for Computing the Privacy Scores of Users in Online Social Networks. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, *5*(1), 1–30. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=22958522&site=ehost-live

Lofstedt, R., Bouder, F., Wardman, J., & Chakraborty, S. (2011). The changing nature of communication and regulation of risk in Europe. *Journal of Risk Research*, *14*(4), 409–429. doi:10.1080/13669877.2011.557479

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. doi:10.1287/isre.1040.0032

Mansell, R. (Workshop C. (2008). *Communication and Information: Towards a Prospective Research Agenda Report on a Workshop, UNESCO, Paris, 20-21 December 2007* (p. 32pp). Paris. Retrieved from

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/programme_doc_iamcr_report.pdf

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59*(2), 411–429. doi:10.1111/1540-4560.00071

McCullagh, K. (2009). Protecting "privacy" through control of "personal" data processing: A flawed approach. *International Review of Law, Computers & Technology*, *23*(1-2), 13–24. doi:10.1080/13600860902742562

McNeill, P. (2005). *Research methods* (Vol. 3rd ed.). London: Routledge.

Miller, D. (2011). *Tales from Facebook* (p. 218). Cambridge: Polity.

Moran, M. (2005). *Politics and governance in the UK* (p. 552). Basingstoke: Palgrave Macmillan.

Muir, A., & Oppenheim, C. (2002). National information policy developments worldwide IV: Copyright, freedom of information and data protection. *Journal of Information Science*, *28*(6), 467–481. doi:10.1177/016555150202800603

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (1980). Paris.

Ofcom. (2009). *How people assess online content and services* (p. 59). London.

Office of Communications. (2008). *Social Networking: a quantitative and qualitative research report into attitudes, behaviours and use* (p. 92pp). London.

Opinion 2/2010 on online behavioural advertising, Pub. L. No. Opinion 2/2010 EC (2010). Article 29 Data Protection Working Party. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

Opinion of the European Economic and Social Committee on the "impact of social networking sites on citizens/consumers" (own-initiative opinion) (2010/C 128/12) (2010). OJ (2010/C 128/12) 18 May 2010. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:EN:PDF

Oppenheim, C. (2001). *The legal and regulatory environment for electronic information*. *An Infonortics in-depth briefing* (Vol. 4th, p. 266). Tetbury: Infonortics.

Outhwaite, W., & Turner, S. P. (Eds.). (2007). *The SAGE handbook of social science methodology* (p. 622). Los Angeles (Calif.) ; London: SAGE.

Press Complaints Commission. (2012). *Newspaper and Magazine Publishing in the U.K. Editors' Code of Practice* (p. 1). London. Retrieved from http://www.pcc.org.uk/assets/696/Code_of_Practice_2012_A4.pdf

Prince Albert v. Strange. (1849). Retrieved from http://www.bailii.org/ew/cases/EWHC/Ch/1849/J20.htm

Privacy by design. (2008). (p. 32pp). Wilmslow, Cheshire. Retrieved from www.ico.gov.uk/.../PRIVACY_BY_DESIGN_REPORT_V2.ashx

Ragin, C. C. (1994). *Constructing social research : the unity and diversity of method*. Thousand Oaks London: Pine Forge Press.

Ragin, C. C. (2000). *Fuzzy-set social science*. Chicago: University of Chicago Press.

Ragin, C. C., & Becker, H. S. (Eds.). (1992). *What is a case? : exploring the foundations of social inquiry*. Cambridge: Cambridge University Press.

Reay, I., Dick, S., & Miller, J. (2009). A large-scale empirical study of P3P privacy policies. *ACM Transactions on the Web*, *3*(2), 1–34.

Regulation of Investigatory Powers Act (2000).

Reidenberg, J. R. (1998). Lex Informatica: the formulation of ifnormation policy rules through technology. *Texas Law Review*, *76*(3), 553–584. Retrieved from http://reidenberg.home.sprynet.com/lex_informatica.pdf

Robinson, L. (2009). Information science: communication chain and domain analysis. *Journal of Documentation*, *65*(4), 578–591. doi:10.1108/00220410910970267

Room, S. (2007). *Data protection and compliance in context* (p. 274). Swindon: British Computer Society.

Rowlands, I., Eisenschitz, T. S., & Bawden, D. (2002). Frame Analysis as a Tool for Understanding Information Policy. *Journal of Information Science*, *28*(1), 31–38. doi:10.1177/016555150202800104

Schneier, B. (2010). A taxonomy of social networking data. *IEEE Security and Privacy*, *8*(4), 88.

Slattery, D., & Nellis, J. (2011). Rethinking the role of regulation in the aftermath of the global financial crisis: The case of the UK. *Panoeconomicus*, *58*(3), 407–423. doi:10.2298/PAN1103407S

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=67129829&site=ehost-live

Sobel, R. (2007). The HIPAA paradox: The privacy rule that's not. *Hastings Center Report*, *37*(4), 40–50.

Solove, D. J. (2007). *The future of reputation : gossip, rumor, and privacy on the Internet* (p. 247). New Haven, Conn. ; London: Yale University Press.

Spinello, R. A. (2006). *Cyberethics : morality and law in cyberspace* (Vol. 3rd). Sudbury, Mass. ; London: Jones and Bartlett Publishers. Retrieved from Table of contents http://www.loc.gov/catdir/toc/ecip064/2005033110.html

Study on Co-Regulation Measures in the Media Sector. Final Report. (2006). (p. 198pp).

Swedlow, B., Kall, D., Zhou, Z., Hammitt, J. K., & Wiener, J. B. (2009). Theorizing and Generalizing about Risk Assessment and Regulation through Comparative Nested Analysis of Representative Cases. *Law & Policy*, *31*(2), 236–269. doi:10.1111/j.1467-9930.2009.00296.x

Tavani, H. T. (2000). Privacy and Security. In D. Langford (Ed.), *Internet Ethics* (pp. 65–95). Basingstoke: Macmillan.

Teggart v TeleTech UK Ltd. (2012). Retrieved from http://www.bailii.org/nie/cases/NIIT/2012/00704_11IT.html

Tene, O., & Polonetsky, J. (2012). Symposium Issue - Privacy in the Age of Big Data: a time for big decisions. *Stanford Law Review Online, 64*(63), 63–69.

The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations (2010). Retrieved from http://www.legislation.gov.uk/uksi/2010/31/pdfs/uksi_20100031_en.pdf

The Data Protection (Notification and Notification Fees) (Amendment) Regulations (2009). Retrieved from http://www.legislation.gov.uk/uksi/2009/1677/pdfs/uksi_20091677_en.pdf

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations (2011). Retrieved from http://www.legislation.gov.uk/uksi/2011/1208/pdfs/uksi_20111208_en.pdf

The Privacy and Electronic Communications (EC Directive) Regulations (2003). Retrieved from http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf

The Transfer of Tribunal Functions Order (2010). Retrieved from http://www.legislation.gov.uk/uksi/2010/22/pdfs/uksi_20100022_en.pdf

The Treaty on European Union (1992). OJ C 83/13, 30.3.2010. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:EN:PDF

The Treaty on the Functioning of the European Union (1957). OJ C 83/56 30.3.2010.

Torriti, J. (2007). Impact Assessment in the EU: A Tool for Better Regulation, Less Regulation or Less Bad Regulation? *Journal of Risk Research, 10*(2), 239–276. doi:10.1080/13669870701217847

Treaty between the Member States of the European Communities and the Kingdom of Denmark , Ireland and the United Kingdom of Great Britain and Northern Ireland (1972).

Turrow, S. (2004). Bridging the Quantitative and Qualitative Divide. In H. Brady & D. Collier (Eds.), *Rethinking Social Inquiry: diverse tools, shared standards* (pp. 171–179). Lanham, Md. ; Oxford: Rowman & Littlefield.

Wacks, R. (2010). *Privacy : a very short introduction*. *Very short introductions ; 221* (p. 160). Oxford: Oxford University Press.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard law review, 4*(5), pp. 193–220. Retrieved from http://www.jstor.org/stable/1321160

Weber, R. H. (2002). *Regulatory models for the online world* (p. 207). The Hague ; London: Kluwer Law International.

Weiss, S. (2008). *The need for a paradigm shift in addressing privacy risks in social networking applications*. (S. D. FischerHubner P Zuccato, A Martucci,L., Ed.) (p. 171pp). Univ Frankfurt, D-60054 Frankfurt, Germany.: SPRINGER.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. doi:10.1111/1540-4560.00072

Wikipedia. (2011). List of virtual communities with more than 100 million users. Wikimedia Foundation Inc.

Wollan, R., Smith, N., & Zhou, C. (2011). *The social media management handbook : everything you need to know to get social media working in your business*. (R. Wollan & N. Smith, Eds.) (p. 328). Hoboken, N.J.; Chichester: Wiley; John Wiley distributor.

Woods, L. (2012). User Generated Content: Freedom of expression and the role of media in a digital age. In M. Amos, J. Harrison, & L. Woods (Eds.), *Freedom of Expression and the Media* (pp. 141–168). Leiden and Boston: Martinus Nijhoff under the auspices of the Clemens Nathan Research Centre.

Wu, T. (2010). *The Master Switch: the rise and fall of information empires* (p. 384). Atlantic Books.

Yassine, A., Shirehjini, A., Shirmohammadi, S., & Tran, T. (2012). Knowledge-empowered agent information system for privacy payoff in eCommerce. *Knowledge and Information Systems*, *32*(2), 445–473.

Your Personal Little Book about Protecting your Personal Information. (2009). (p. 22pp). Wilmslow. Retrieved from http://www.ico.gov.uk/upload/documents/youth/your_personal_little_book.pdf

Zittrain, J. (2008). *The future of the Internet :and how to stop it* (p. 342). London: Allen Lane.