Received 11 July 2014
Revised 15 October 2014
Accepted 14 November 2014

Defining user risk in social networking services

David Haynes and Lyn Robinson
Department of Library and Information Science, City University London, London, UK

Abstract

Purpose – The purpose of this paper is to identify the risks faced by users of online social networking services (SNSs) in the UK and to develop a typology of risk that can be used to assess regulatory effectiveness.

Design/methodology/approach – An initial investigation of the literature revealed no detailed taxonomies of risk in this area. Existing taxonomies were reviewed and merged with categories identified in a pilot survey and expanded in purposive sample survey directed at the library and information services (LIS) community in the UK.

Findings – Analysis of the relationships between different risk categories yielded a grouping of risks by their consequences. This aligns with one of the objectives of regulation, which is to mitigate risks.

Research limitations/implications – This research offers a tool for evaluation of different modes of regulation of social media.

Practical implications – Awareness of the risks associated with use of online SNSs and wider social media contributes to the work of LIS professionals in their roles as: educators; intermediaries; and users of social media. An understanding of risk also informs the work of policy makers and legislators responsible for regulating access to personal data.

Originality/value – A risk-based view of regulation of personal data on social media has not been attempted in such a comprehensive way before.

Keywords Social media, Risk, Regulation, Privacy, Social networking services

Paper type Research paper

Introduction

Background and context

Users of social networking services (SNSs) make personal information available to social network providers in exchange for "free at the point of use" services. This personal information is voluntarily provided by users, and is usually covered in the terms and conditions of service or is gathered by service providers who track online behaviour using agents such as "cookies". Making personal data available to a wide audience exposes users to risk. Although there have been attempts to enumerate some of these risks, which are described below, there has not been a comprehensive review of the risks or any attempt to develop a model of user risk in the context of SNSs. There is a tension about the relative importance of individual and social factors in the study of information behaviour (Bawden and Robinson, 2013). This is apparent in the individual response to social media and the way in which different interest groups regulate access to personal data.

An Oxis survey suggested that contrary to popular perceptions, users are becoming more aware of privacy as a concern on the internet, especially when it comes to using

The authors acknowledge with thanks the contribution of survey participants and interview respondents who give their time generously. They also acknowledge the comments and feedback provided by colleagues at City University London and by members of the wider research community.

Aslib Journal of Information Management
Vol. 67 No. 1, 2015
pp. 94-115

2050-3806
DOI 10.1108/AJIM-07-2014-0087

social media (Dutton and Blank, 2013). A comprehensive review of Facebook research in the social sciences recognised the need for researchers to analyse the risks associated with Facebook use (Wilson *et al.*, 2012, p. 216):

> By better understanding the threats to privacy, researchers and developers can construct countermeasures to mitigate the risks, and users can take informed steps towards protection their personal information.

This paper sets out to identify the risks to individual SNS users and to develop a model of risk that can be applied more widely to internet use and social media as they continue to evolve. The research questions were:

RQ1. What are the risks to individuals that are associated with personal data on SNSs?

RQ2. Is there an existing typology of individual risk that adequately covers SNSs?

RQ3. Can a model of risks to users be used to differentiate between possible regulatory responses?

Regulation is one area where an up-to-date and relevant model of risk could contribute to improved protection of users. Risk-based regulation has emerged as a dominant approach in Europe and the UK in the last few decades. Baldwin *et al.* (2012, p. 83) suggest that "Regulation can be seen as being inherently about the control of risks […]". This is a view supported by Hutter (2006, p. 205): "[…] regulation has come to be defined as controlling and also as a way of managing risks".

Methodology

In order to address these questions, this research was based on a systematic review of the literature, and a survey of information professionals in the UK. Modelling techniques were used to develop a concept of risk that is relevant to internet use and, more specifically, to SNSs. The literature review identified general risk typologies which were analysed in terms of: their applicability to SNSs; their focus on risk to individuals; and their ability to distinguish between types of risk to individuals.

A survey of library and information service (LIS) professionals in 2014 provided insight into the perceived importance of different risk categories (Appendix 1). This sector was chosen because it is a well-developed professional group representing users (many LIS staff act as intermediaries), and who are information literate and are therefore likely to be exposed to a wide range of online scenarios. It is also a cohesive group with a track record of active use of social media (Cooke and Hall, 2013). The survey was directed at UK users of SNSs using a filter question at the start of the survey to exclude non-UK users. This was cross-checked against the location of the IP Address of the device accessing the survey and logged by SurveyGizmo. The survey objective was to identify the range of risks to which users are exposed and to gain some insight into the perceptions of risk and priorities for managing risk. The survey was based on purposive sampling directed at LIS professionals in the UK, using a variety of forums (listed in Appendix 2) to generate a snowball effect (David and Sutton, 2011, p. 232). Participants were encouraged to publicise the survey through their own professional and personal networks.

A model of risks was developed from an analysis of the consolidated lists of risks identified in the survey and the literature. A typology was developed which formed the basis of a model of personal risk in SNSs. The event and consequence of each risk was analysed to identify the relationship between the risks and to develop a definitive set of outcomes which might have the potential as a tool to evaluate different regulatory approaches.

Privacy and risk

Information privacy is an important aspect of any discussion about personal data on SNSs. The volume of personal data available on SNSs puts it firmly in the category of "big data". It has been suggested that when dealing with big data "the change of scale leads to a change of state" and that "this transformation not only makes protecting privacy much harder, but also presents an entirely new menace: penalties based on propensities" (Mayer-Schönberger and Cukier, 2013, p. 151). For instance, where security agencies try to prevent terrorist acts by pre-empting them, individuals are targeted and may be arrested or have their movements restricted without being convicted of any crime. Another problem is "fetishizing". This is a common fallacy identified elsewhere (Hansson, 2004), where because the picture provided by big data is so compelling, it becomes the over-riding factor in making a decision or judgement.

A UNESCO report identified a range of privacy issues associated with the internet. While these are not expressed as risks they could lead to users being exposed to risks. The issues identified are (Mendel *et al.*, 2012, pp. 39-49):

- user identification – unique identifiers, cookies and other forms of user identification;
- adware, spyware and malware conduct covert data logging and surveillance;
- deep packet inspection;
- pervasive geo-location technology: an emerging threat to internet privacy;
- data processing and facial recognition; and
- internet surveillance technology.

Anderson (2013) talks about the difficulty of applying technical "quick fixes" to complex social systems. This can lead to mismatches between users' expectations and the behaviour of SNSs. He identifies a number of scenarios to illustrate this:

- attacker re-posted private entries which included sensitive information in a more public forum;
- permissive default privacy settings;
- changes to privacy settings by SNS provider without consent of users. This means that formerly private friends lists are exposed to public view;
- apps developers harvesting personal data to third-party advertisers and data aggregators (in breach of terms of reference); and
- cautious users unwilling to expose themselves to risk and thus being severely limited in what they can do.

He goes on to point out that the big differences in power between service providers and users, effectively mean that users have little choice or control over their own data once they sign up to SNSs.

Nissenbaum (2010) identifies three types of privacy issue in social media:

(1) individuals post information about themselves, which later gets them into trouble, with an employer, for instance;

(2) posting information about other people, often without their explicit permission can cause problems. Even where there are remedies, such as removing tags from photos, the photos may still remain on the system; and

(3) harvesting and use of personal data on social networks by advertisers.

Defining risk

Risk is an elusive concept based on the notion of uncertainty sometimes expressed in terms of the probability of an adverse event occurring. Commonly used definitions of risk as "a situation involving exposure to danger" or "the possibility that something unpleasant or unwelcome will happen" are not very specific and need to be pinned down (Pearsall and Hanks, 1999, p. 1602). The international standard on risk management starts with an even more general definition "effect of uncertainty on objectives" and goes on to say that "An effect is a deviation from the expected – positive and/or negative". The Standard does eventually provide a more specific definition: "Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence" (British Standards Institution, 2010). However risk is more widely understood to be an event with a negative outcome, in other words, a threat: "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 and Renn, 2009, p. 2). From the regulatory sphere a working definition is: "[…] risk is usually defined as the probability of a particular event (or hazard) occurring and the consequent severity of the impact of that event" (Baldwin *et al.*, 2012, p. 82).

For the purposes of this paper risk is defined as an uncertain event which has an adverse impact on an activity or outcome. Applied here, risk is an event of unknown probability of occurrence involving personal data on an SNS that has a negative impact on that person. For instance, an individual's data might be copied for the purposes of fraud, resulting in that individual suffering financial loss.

Typologies of risk in the literature

A general typology of risk

Some early commentators have attempted to identify risks associated with the use of SNSs (Rosenblum, 2007). However going back to more general approaches to risk identification provides a wider picture. There can be a distinction between physical and social risks which can be integrated (Macgill and Siu, 2005, pp. 1108-1110). Tulloch (2006, pp. 132-133) adopts a social approach to risk:

Thus, it seems clear that current research is positively engaged with the construction of self-identities in conditions of risk that these frequently take account of the reflexive concern for dialogic negotiation within and between everyday "lay voices" and professionals, and that by and large this work […] embeds "wider social understanding" analysis in quite traditional understandings of the "otherness" of age, gender, sexual preference, class, and (dis)ability.

Swedlow and associates' (2009, p. 237) research into risk and regulation is based on the "construction of a universe of nearly 3,000 risks […] over a thirty-five year period".

This provides a comprehensive view of the types of risk that exist generally and is used as a starting point for identifying and categorising the risks faced by SNS users. Some of these risks would arise directly from misuse of data; others are related to the data held about individual history, behaviour and preferences. The following categories from this "universe" of risks might be applicable to social media and specifically to SNSs:

(1) Crime and violence – there have been a number of court cases where revealing personal data of individuals on social media has exposed them to threats of violence or to harassment (Agate and Ledward, 2013).

(2) Recreation – a great deal of use of social networks is for recreation rather than professional purposes and it could be argued that the other risks associated with social media fall into this category.

(3) War, security and terrorism – with the WikiLeaks revelations starting in 2010 and the NSA scandal in 2013 the press has paid particular attention to the security aspects of personal information (Leigh and Harding, 2011; BBC News, 2012; Greenwald, 2013). The risks to users are twofold. The first is that identifying information on social networks may be used to victimise or persecute an individual by a state or terrorist organisation. The second is that an individual's identity may be stolen for use by terrorists or by state security agencies and in doing so potentially expose them to harm.

(4) Political, social and financial – Political, social and financial harm can arise from identity theft. For example, if sufficient biometric data are available on a users' profile it may be possible to set up a false identity to gain access to credit or to purchase products with no intention of paying. The individual whose identity has been stolen may be pursued for payment and may even be liable for debts and costs incurred through the fraud.

(5) Social risks may include ostracism because of private information being made available inadvertently to a wider audience than intended. For example, expression of views that are not compatible with a community's mores (whether it be a religious group, a political party or an ethnically-based group) may lead to some kind of sanction or even expulsion from that group.

(6) Human disease/health – mental health falls under this category. Cases where vulnerable young people have been driven to suicide because of harassment and bullying are an extreme example of this (Wakefield, 2014). Less extreme, but nonetheless distressing, may be social isolation and associated depression. Even an affront to an individual's self-esteem and confidence is a potential threat to mental well-being.

(7) Occupational – Some employers admit that they search the social media profiles of potential employees and take the results into account in their recruitment decisions (Rosenblum, 2007, p. 46). It is also an issue for employees who use social media in their private lives to express their views. If an employer deems this to be detrimental to their business or incompatible with their views, it could result in disciplinary action or even dismissal.

(8) Consumer products – consumer products are associated with advertising and this is one of the major areas of concern of many users (Rosenblum, 2007,

pp. 46-47). Behavioural advertising depends on tracking online browsing behaviour and sites visited in order to deduce the interests of the user and target them with advertising for products that they are likely to be interested in. The impact on users could be described in terms of nuisance caused or possible social isolation.

(9) Related risks – a number of the general risks identified are not core to SNS use but may be associated with it in some way. For example, the following would also affect the political, social and financial risks faced by individual users:

- alcohol, tobacco, and other drugs;
- medication and medical treatment;
- toxic substances; and
- human disease/health.

In all of these cases the risk is associated with information about these activities being available on personal profiles via social networks. So for instance an indication of previous problems with drug abuse may prejudice employment prospects, and health problems revealed online may affect insurance premiums.

Other risk typologies

Other researchers looking at the internet have provided more relevant categories of risks that might be associated with use of social media (McDonald, 2013; Farr, 2013; Solovic, 2013; Mann, 2009). These can be broken down into risk events and associated consequences. Table I shows these risks grouped into nine main headings.

Risks identified in European Union legislation

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"(European Economic and Social Committee, 2010). It identified the concerns about "the risks of the illegal and abusive use of SNS, which rides roughshod over a number of basic human rights". It identified threats to individuals (particularly to children) and more generic risks that happen to users of SNSs. Risks that might be relevant in the workplace include:

(1) cyber-bullying;

(2) privacy breaches;

(3) reputational damage; and

(4) assault on personal dignity.

As well as hazards associated with geo-tagging, and facial recognition technologies, spreading of viruses via social media was also identified.

Risks associated with geo-location data

Geo-location data are an increasingly important part of the delivery of SNSs. By allowing their location to be uploaded by mobile service providers and applications providers, users benefit from enhanced services such as location of nearby restaurants, identification of friends in the vicinity and local maps. However there are also concerns about the risks that users are exposed to when their location data are available.

Risk title	Description
External threats	
Identity theft	Includes tax-related identity theft. This risk may lead to other consequences such as wrongful arrest or financial loss
Phishing	Fraudulent link or site entices personal information form the user
Malware link	Link to malware (may be embedded in a direct message or attachment) which may result in external monitoring of passwords, or disruption to computer operations
Hijacking of profile	Hijacking of personal site, profile or page could cause embarrassment or inconvenience. Could be a form of bullying as well
Targetting by official bodies	
Loss of liberty	Arrest and prosecution for a crime that the user did not commit (identity theft)
Prosecution and recrimination	Prosecution or recrimination for posting offensive comments on social media. Offender's personal data becomes available to the authorities
Physical harm	
Kidnapping and extortion	Personal information revealing whereabouts, regular travel routes, or activities that leave users open to extortion
Domestic violence	Abusive individuals pursuing former partners
Stalking, harassment and cyberbullying	
Cyber-bullying and trolling	Offensive comments made by colleagues – cyber-bullying and victimisation, ostracism, denigration, flaming, trolling
Inappropriate comments by colleagues	Sexual harassment, sexual solicitation
Harassment	Unwanted attention from other users, cyber-stalking, offensive comments, hate campaigns, silent calls, threats from another user
Targetting by criminals	
Picture of home and possessions shared	Making the user a target for burglars
Home address published	Making the user a target for home invasion
Financial loss	Liability for bills incurred by fraudster (identity theft)
Scams	Often a form of phishing, where the user is required to provide additional personal information (such as bank account details) or where the user is encouraged to send money to the fraudster. This category includes the following scams: dating, work at home, investment, utility, money transfer, weight loss, fake cheques, mystery shopper, debt relief, pay-in-advance credit, lotteries and sweepstakes, miracle cures, imposter, penny auctions, technical support
Discrimination	
Sharing genetic information	Denial of health or life insurance, Discrimination during recruitment
Loss of opportunities	Refusal of a job or a place at university because of material on a personal profile page
Loss of financial facilities	Refusal of credit or benefits because of information revealed on personal profile. Bad credit rating
Work-related risks	
Contravening company policy	Leading to disciplinary action or dismissal
Psychological harm	
Financial records shared	Causing embarrassment with work colleagues and friends
Sharing of genetic information	Invasion of privacy of blood relatives

Table I.
Personal risks associated with SNSs

(*continued*)

Risk title	Description
Release of account details to relatives or executors	Loss of dignity in death. Distress caused to relatives when details not revealed
Loss of privacy	Disclosure of private information
High school pictures shared	Causing embarrassment, doxing, outing
Advertising	
Persistent advertising	Continual, persistent advertising causing nuisance
Spam	Unwanted marketing, junk mail, sales calls, text messages, invitations to connect that contain spam pointed on someone's network update, discussion group spam

Table I.

This is a problem that the European Commission is well-aware of (Article 29 Working Party, 2013).

A number of mechanisms by which geo-location data are gathered or can be reconstructed have been identified. These raise some concerns about the resulting loss of privacy (Andrienko and Andrienko, 2012). Andrienko *et al.* (2013) go on to enumerate the ways in which geo-location data are gathered:

- whenever a mobile device is in use it sends a signal to the service provider. However the provider can send a silent text message to force active communication without alerting the user;
- call data records are another source of geo-location data, which came to prominence in the NSA revelations in 2013 and these can give time-based data on movements (Greenwald, 2013);
- signal strength data can be used to triangulate the position of a mobile device;
- users often consent (not always in an informed way) to their location being identified by apps providers or the mobile service provider for enhanced services. This data might be associated with the user ID which has obvious privacy implications;
- anonymous location data seems to provide better protection, although the authors show how identity and even time-based movement data can be reconstructed; and
- some non-location data such as accelerometer data, which is freely available from some devices, can be used to deduce the location with a reasonable degree of accuracy.

The description of these mechanisms helps to highlight how easy it is for geo-location data to be gathered without the knowledge or understanding of the user, and how this information is available to service providers, mobile operators and apps providers.

Risks identified in the survey

The survey of UK-based LIS professionals ranked risks to provide an indication of priorities. The score is a weighted calculation. In Table II the item with the highest score is ranked first. In each case the score is the sum of all weighted rank counts:
"Identity theft" and "Strangers being able to see sensitive personal details" both had high scores in the ranking. Identity theft can itself expose users to other risks such

Item	Score	Overall rank
Identity theft	1,934	1
Strangers able to see sensitive personal details	1,841	2
Targeting by advertisers	1,575	3
Victim of fraud	1,531	4
Discrimination by employer or potential employer	1,443	5
Targeting by criminals (e.g. so that they can burgle your home while you are away)	1,411	6
Friends, family or colleagues able to see sensitive personal details	1,297	7
Cyber-bullying or harassment (including stalking)	1,288	8
Targeting by official bodies or security agencies	980	9
Extortion or blackmail	628	10
Prosecution by authorities because of crime allegations	590	11
Physical violence or kidnapping	451	12

Note: Total respondents, 213

Table II.
Ranking of risks from a survey of LIS professionals

as fraud (ranked 4) and one of the consequences can be financial loss. For instance, if a user's identity is used to apply for a loan or credit facilities, the victim may be left with the liability to pay back the loan.

"Strangers being able to see sensitive personal details" ranked much more highly than "Friends, family and colleagues being able to see sensitive details". There is a dual risk of strangers seeing personal details – first as a means to commit fraud, and second because it exposes users to discrimination by potential or actual employers, for instance. Additional comments from users were concerns about reputational damage and loss of face. Personal information may be exposed by the actions of others, such as when friends mention an individual or tag photographs or other entries with their names (Thomas *et al.*, 2010).

Some of the risks may have consequences that are more to do with social awkwardness or annoyance rather than loss of money or physical threat. For instance, targeting by advertisers may be irritating rather than life-threatening. Potentially there is the loss of face if another person makes assumptions about an individual on the basis of advertising that appears on a screen. There is also the inconvenience of screen clutter and slowing down of browsers if there is a lot of graphics or moving images to download.

A consolidated model of risk

Developing a typology of risk

Consolidation of these risk categories yields a typology of risk related to use of SNSs. However not all these risks are related to access to personal data, but relate to intellectual property, security and organisational issues.

Three approaches to devising a typology of risk for this domain were considered. Risks can be categorised by:

(1) risk event;

(2) stakeholder affected; and

(3) consequence.

Risk event

A risk consists of an event, for which there is a degree of uncertainty about whether it will occur AND the consequence or outcome should it occur. The first part of this definition is the "risk event". Risks can be categorised according to a universal set of risks such as those identified by researchers at the Duke University and Northern Illinois University (Swedlow *et al.*, 2009). These are based on risk events or threats. This categorisation does not take into account severity, or impact, or which stakeholders are affected.

Some threats or risks could fall under more than one heading. For instance, identity theft could be under "Crime and Violence", if it leads to fraud and eventual financial loss to the individual whose data was "stolen". It could also be under "War Security and Terrorism", where identity theft (the same event) results in a different outcome – a terrorist using an alias to escape detection, for instance. It could be argued that this might expose an individual to even greater harm such as the loss of liberty or even loss of life.

Stakeholder affected

Risks can be analysed in terms of the stakeholders. In a pilot investigation prior to the survey the SNS stakeholders were identified as: users, service providers, advertisers, employers and government. However because this study is considering the risks associated with allowing access to personal data on SNSs, it is not surprising that the majority of risks will primarily affect users. Indeed a preliminary analysis of the risks identified to date (Table I) bears this out. Apart from work-related risks which primarily affect employers, the remaining risks all have some direct impact on users.

Although main risks are faced by users, release of personal data can have a negative impact on employers by damaging reputations or exposing them to legal action or prosecution. There might be wider risks to government or society if personal data are misappropriated and used for terrorist activities or economic sabotage, for instance. Many of the risks to employers of using SNSs in the workplace are not related to access to personal data. They include issues such as: time wasting, security breaches, copyright and libel where staff members post inappropriate materials on an SNS site during work hours or on a site with a strong presence by or association with the employer.

The other side of the argument is determining who benefits from access to personal data. Advertisers, and those that pay them or whom they pay, benefit directly from accessing personal data, consolidated or not. Indirectly government benefits because of increased tax revenue from the resulting economic activity. Potentially users also benefit – because of more tailored experience of services and targeted advertising – presumably some value is perceived otherwise no-one would follow the links and there would be no point in advertisers using this as a method of gaining new custom.

Consequence

The risks identified when the EU's Data Protection Directive was being developed can be divided into two categories: tangible risks; and intangible risks (Lynskey, 2012):

(1) Tangible risks:
    - discrimination;
    - identity theft;

- abuse of power by the state; and
- physical harm.

(2) Intangible risks:

- the chilling effect;
- the feeling of helplessness; and
- the apprehension of future harm.

This grouping moves towards the idea of categorising risks by their consequences rather than by the nature of the risk event. This can be further refined by concentrating on consequences to users specifically (see Table III). This provides a means of quantifying the risks, banding them in risk severity categories, or at least a relative ranking.

Although this is a useful model, one event could lead to several different consequences. For instance loss of personal data (an event) could lead to harassment (consequence) or fraud (consequence). One consequence could also have several different causes. For example, financial loss could be as a result of following up inappropriate advertising, or it could be because of identity theft, or because of discrimination by prospective employers who have gained access to personal profiles.

A further complication is that a consequence such as cyber-bullying arising from exposure of sensitive data to an inappropriately wide group, could itself lead to further

Consequence	Risk events or threats that leads to the consequence
Self-harm	Cyber bullying
	Exposure of sensitive personal data to wider view
	Inappropriate advertising to susceptible individuals or groups
Loss of self-esteem	Cyber bullying
	Exposure of sensitive personal data to wider view
Social isolation	Cyber bullying
	Exposure of sensitive personal data to wider view
Financial loss (e.g. job or insurance costs)	ID theft leading to fraud and financial loss
	Discrimination in employment or during recruitment because of content of SNS profile (e.g. activities, views or past history – membership of a particular group, or health)
	Higher insurance premiums because of perception of greater risk based on SNS profile (Health, exposure to hazards, risky behaviour)
	Use of personal data to target for crime – e.g. burglary during holidays or robbery based on recent purchases
	Cost of inappropriate purchases made under advertising pressure
Loss of liberty – e.g. injustices because of mistaken identity	ID theft leading to mistaken identification as a terrorist
	Inappropriate use of personal data by security services to profile and target potential terrorists
Violence against the person	Targeting individuals for stalking
	Using personal data to get at a target for revenge, robbery, stalking (Rosenblum, 2007, p. 47)
Nuisance	Appropriation of personal data (aggregated or identifiable) by advertisers

Table III.
Analysis of risks by their consequences to users

consequences such as self-harm, loss of self-esteem and social isolation.

From the early days of SNSs researchers have identified different standards of behaviour on the internet as a potential source of risk: "This artificial sense of the anonymity of Net communications leads people to actually lower their inhibitions, and to feel protected from the consequences of their speech" (Rosenblum, 2007, p. 45).

Discussion

A risk model for SNSs

Any categorisation is to some extent arbitrary and so it is necessary to identify what criteria are used to select an appropriate approach. Very few commentators in this area have explicitly selected one or other of the three approaches discussed in this paper – analysis by: risk event; stakeholder; or consequence. For the purposes of this study the key consideration is whether this allows differentiation of risks in terms of possible regulatory responses.

Swedlow *et al.* (2009) analysed by risk event using categories that are too general for this study. The majority of relevant risks that they have identified, fall into a single category – political, social and financial risks. The categories defined do not deal very well with the consequences of risk events such as: harassment; nuisance; loss of dignity; or invasion of privacy.

The stakeholder approach is used by other researchers focusing on risks specifically associated with SNS use from an employer's perspective (Langheinrich and Karjoth, 2010). They go beyond the scope of this study by including risks associated with company information as well as general exposure on social networks. However they identify many relevant risks and this coupled with other analyses that focus on the user perspective, results in a list of risks based on stakeholder groups. This offers a method for investigating the effects of regulation (Ellison and Boyd, 2013). The same event (e.g. sharing personal data with advertisers) may have quite different effects on each group. For instance, making personal data available to the partners of an SNS provider may be good for advertisers and some consumers, and bad for other users (especially those not looking to purchase).

There are two main problems with the stakeholder approach. The first is that the majority of risks associated with inappropriate access to personal data will directly affect the user. As this study is concerned with risks to individuals, this is not a good way of distinguishing between risks. The other problem is that the list is long and un-differentiated within these two main categories, with overlap and potential gaps in coverage.

The third approach analyses risk in terms of its consequences and this provides a smaller number of main headings under which risks can be grouped (see Table III). This approach also allows addition of a stakeholder aspect so that analysis by this criterion is also possible.

The survey brought in wider perspectives on what the risks to individuals were and how those risks interacted. Analysis of the risks identified and the relationships between those risks provides a clear distinction between risk events and their consequences. A map of the relationships between risks categories was developed (Figure 1) from the typology based on consequences of risks events (Table III). This allows the development of a model of risk relationships. The model emphasises the difficulty of defining limits around the definitions of each risk category, a pre-requisite for measuring or quantifying risk.

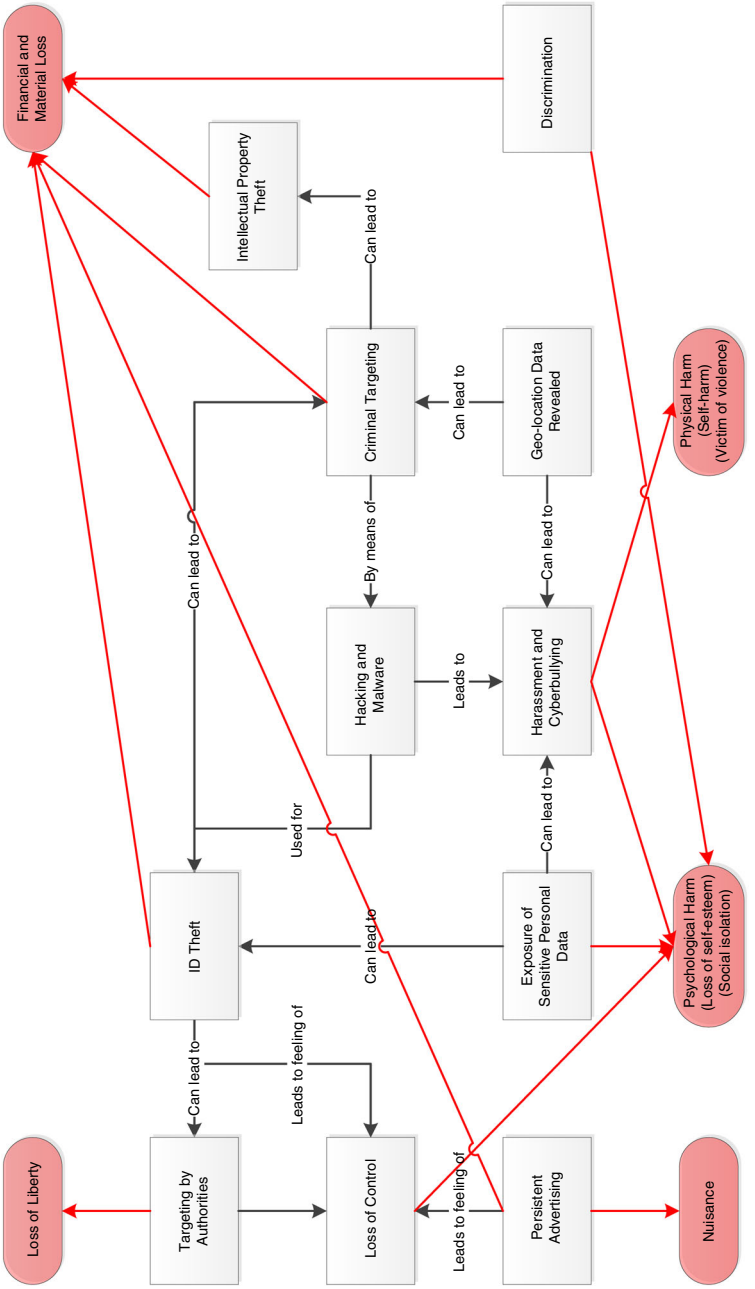

Figure 1.
Relationships between risk events and their consequences

The analysis of consequences produces a more complex picture than a simple listing (Table III) can reveal. One of the challenges of trying to analyse risk is that some consequences may themselves expose individual to new risks and therefore to other types of harm. The figure uses red arrows to point to the risk consequences and labelled black arrows to look at the relationship between underlying risks.

This grouping of risks has allowed an inductive derivation of five categories of consequences to users. Within each category, the contributing risks events are described.

Nuisance includes being bombarded with advertisements or users being inconvenienced by having to go through extra steps to preserve their privacy. This could also include intrusion into private lives by strangers, where no other direct harm is felt.

Psychological harm can result from exposure of private information and also from harassment and cyberbullying. This can range from mild social embarrassment when personal information is circulated to those that the data subject would not be comfortable with, through to victimisation and threats. It can also result from a feeling of helplessness engendered by loss of control over who has access to personal data.

Financial and material loss can arise from criminal targeting through or from fraud as a result of ID theft. Active discrimination in the job market – for instance by religion, race, trade union activity or sexuality, all of which may be inadvertently revealed on SNS profiles. Theft of intellectual property via SNSs – especially where users are encouraged to post pictures, videos ,etc., could result in loss of revenue (Rosenblum, 2007, p. 46). There have also been cases reported in the press of people inadvertently advertising when they are away, making them targets for burglary or home invasions (Roberts, 2010; BBC News, 2013).

Loss of liberty is a dramatic consequence of personal data being made available on SNSs. This could be either as a result of exposure of criminal activity or being mistakenly identified as a criminal or terrorist (Strauß and Nentwich, 2013). Boasts about drug-taking on SNSs or evidence of location could be used as evidence of criminal activity. Profiling by security services and police are approximate tools that have led to targeting of innocent people with consequent loss of liberty, political persecution and financial loss.

Physical harm can be a consequence of criminal targeting – for instance during a robbery or a kidnapping. Personal data can reveal information about movements, routines and intent and therefore make it easier for criminals to target the individual. There are also concerns about personal information revealing the location of shelters for those escaping domestic abuse.

Conclusion

This research has identified risks that individual users of SNSs face as a result of revealing personal data on their profiles or through their online behaviour. Previous attempts to categorise risk have been too general to adequately describe the risk exposure of SNS users. Where there has been a focus on the risks associated with use of the internet or social media, they have tended to focus on a few specific aspects that were topical at the time. A consolidated list of risks reflected the perceptions of risk among a group of library and information professionals surveyed in the UK.

A list of risks does not, however, describe the relationship between different risk categories. This is important because of the strong interdependence between them.

A risk model that more accurately represents the potential threats to users and the consequences can be used as a tool for investigating different modalities of regulation. As much of current regulatory activity is risk based, this approach could provide a means of evaluating different regulatory approaches. For example, it might be possible to consider whether proposed changes in legislation tend to increase or reduce each of the risk categories in terms of probability of occurrence and severity of impact.

This up-to-date perspective on user risk is of potential utility to policy makers and decision makers. Legislators need a more nuanced tool than currently exists for evaluating proposed new laws or regulations. Service providers can consider the effect of different privacy settings and proposed new services on users, and systems designers have a tool that they can adopt to demonstrate that they are following "privacy-by-design" principles.

The risk model also provides a conceptual framework for trainers, educators and information intermediaries. These are all roles that are increasingly forming a part of the role of LIS professionals. Their role in modifying user behaviour by example and by user education could have a significant effect in helping users to derive the greatest benefit safely from SNSs and from social media generally.

References

Agate, J. and Ledward, J. (2013), "Social media: how the net is closing in on cyber bullies", *Entertainment Law Review*, Vol. 24 No. 8, pp. 263-268.

Anderson, J. (2013), "*Privacy Engineering for Social Networks*", Computer Laboratory, Cambridge, available at: www.repository.cam.ac.uk/handle/1810/244239 (accessed 7 December 2013).

Andrienko, G. and Andrienko, N. (2012), "Privacy issues in geospatial visual analytics", in Gartner, G. and Ortag, F. (Eds), *Advances in Location-Based Services, 8th International Conference on Location Based Services, 2011, Springer, Vienna, Heidelberg*, pp. 239-246.

Andrienko, G., Gkoulalas-Divanis, A., Gruteser, M., Kopp, C., Liebig, T. and Rechert, K. (2013), "Report from dagstuhl", *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 17 No. 2, p. 7.

Article 29 Working Party (2013), "WP29 opinion on apps on mobile devices", 00461/13/EN WP 202, Brussels, available at: www.huntonprivacyblog.com/wp-content/uploads/2013/03/wp202_en.pdf (accessed 4 March 2014).

Aven, T. and Renn, O. (2009), "On risk defined as an event where the outcome is uncertain", *Journal of Risk Research*, Vol. 12 No. 1, pp. 1-11.

Baldwin, R., Cave, M. and Lodge, M. (2012), *Understanding Regulation: Theory, Strategy, and practice*, 2nd ed., Oxford University Press, Oxford.

Bawden, D. and Robinson, L. (2013), "No such thing as society? On the individuality of information behavior", *Journal of the American Society for Information Science & Technology*, Vol. 64 No. 12, pp. 2587-2590.

BBC News (2012), "BBC news – Wikileaks revelations", *BBC News Online*, available at: www.bbc.co.uk/news/world-11863274 (accessed 7 July 2014).

BBC News (2013), "BBC news – arrests made in brian holloway's trashed house party", *BBC News*, available at: www.bbc.co.uk/news/world-us-canada-24293414 (accessed 11 February 2014).

British Standards Institution (2010), *BS ISO 31000:2009 Risk Management – Principles and Guidelines*, British Standards Institution, London.

Cooke, L. and Hall, H. (2013), "Facets of DREaM: a social network analysis exploring network development in the UK LIS research community", *Journal of Documentation*, Vol. 69 No. 6, pp. 786-806.

David, M. and Sutton, C.D. (2011), *Social Research: an Introduction*, SAGE, Los Angeles, CA.

Dutton, W.H. and Blank, G. (2013), Cultures of the internet: the internet in Britain, Oxford internet survey 2013, Oxford, available at: http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf (accessed 19 May 2014).

Ellison, E.B. and Boyd, D.M. (2013), "Sociality through social network sites", in Dutton, W.H. (Ed.), *The Oxford Handbook of Internet Studies*, Oxford University Press, Oxford, pp. 151-172.

European Economic and Social Committee (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), European Union: OJ (2010/C 128/12) 18 May, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:EN:PDF

Farr, C. (2013), "Can you trust Facebook with your genetic code?", *VentureBeat*, available at: http://venturebeat.com/2013/10/07/can-you-trust-facebook-with-your-genetic-code/ (accessed10 October 2013).

Greenwald, G. (2013), "NSA collecting phone records of millions of Verizon customers daily", *The Guardian*, available at: www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed 7 July 2014).

Hansson, S.O. (2004), "Fallacies of risk", *Journal of Risk Research*, Vol. 7 No. 7, pp. 353-360.

Hutter, B.M. (2006), "Risk, regulation and management", in Taylor-Gooby, J. and Peter, Z. (Eds), *Risk in Social Science*, Oxford University Press, Oxford, pp. 202-227.

Langheinrich, M. and Karjoth, G. (2010), "Social networking and the risk to companies and institutions", *Information Security Technical Report*, Vol. 15 No. 2, pp. 51-56.

Leigh, D. and Harding, L. (2011), *Wikileaks: Inside Julian Assange's War on Secrecy*, Guardian Books, London.

Lynskey, O. (2012), *Identifying the Objectives of EU Data Protection Regulation and Justifying its Costs,* PhD thesis, University of Cambridge, Lucy Cavendish College, Cambridge.

McDonald, T. (2013), "Kids + Facebook = home invasion?", *Business 2 Community*, available at: www.business2community.com/facebook/kids-facebook-home-invasion-0618724 (accessed 10 October 2013).

Macgill, S.M. and Siu, Y.L. (2005), "A new paradigm for risk analysis", *Futures*, Vol. 37 No. 10, pp. 1105-1131.

Mann, B.L. (2009), "Social networking websites: a concatenation of impersonation, denigration, sexual agressive solicitation, cyber-bullying or happy snapping videos", *International Journal of Law and Information Technology*, Vol. 17 No. 3, pp. 252-264.

Mayer-Schönberger, V. and Cukier, K. (2013), *Big Data: a Revolution That Will Transform How We Live, Work and Think*, John Murray, London.

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D. and Torres, N. (2012), *Global Survey on Internet Privacy and Freedom of Expression (Unesco Series on Internet Freedom)*, UNESCO Publishing, Paris.

Nissenbaum, H.F. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford, CA.

Pearsall, J. and Hanks, P. (Eds) (1999), *The New Oxford Dictionary of English*, Oxford University Press, Oxford.

Roberts, L. (2010), "BBC news – Facebook status updates are "burglary risk", *BBC News Online*, available at: www.bbc.co.uk/news/uk-england-birmingham-12062331 (accessed 7 July 2014).

Rosenblum, D. (2007), "What anyone can know: the privacy risks of social networking sites", *IEEE Security & Privacy*, Vol. 5 No. 3, pp. 40-49.

Solovic, S. (2013), "The social media dilemma: managing business benefits and personal risks", *Business 2 Community*, available at: www.business2community.com/social-media/social-media-dilemma-managing-business-benefits-personal-risks-0597574 (accessed 10 October 2013).

Strauß, S. and Nentwich, M. (2013), "Social network sites, privacy and the blurring boundary between public and private spaces", *Science and Public Policy*, Vol. 40 No. 6, pp. 724-732.

Swedlow, B., Kall, D., Zhou, Z., Hammitt, J.K. and Wiener, J.B. (2009), "Theorizing and generalizing about risk assessment and regulation through comparative nested analysis of representative cases", *Law & Policy*, Vol. 31 No. 2, pp. 236-269.

Thomas, K., Grier, C. and Nicol, D.M. (2010), "UnFriendly: multi-party privacy risks in social networks", in Atallah, M. and Hopper, N. (Eds), *Privacy Enhancing Technologies, 10th International Symposium, 21-23 July 2010*, Springer Verlag Berlin Heidelberg, Berlin, pp. 236-252.

Tulloch, J. (2006), "Everyday life and leisure time", in Taylor-Gooby, P. and Zinn, J. (Eds), *Risk in Social Science*, Oxford University Press, Oxford, pp. 117-139.

Wakefield, J. (2014), "BBC news – cyberbullies: how best to tackle online abuse?", *BBC News Online*, available at: www.bbc.co.uk/news/technology-26121199 (accessed 7 July 2014).

Wilson, R.E., Gosling, S.D. and Graham, L.T. (2012), "A review of facebook research in the social sciences", *Perspectives on Psychological Science*, Vol. 7 No. 3, pp. 203-220.

Appendix 1. Survey of LIS professionals' attitudes to SNSs in the UK

Social Networks, Risk and Regulation

Introduction

Hi there!

Thanks for following the link to this City University survey.

This short survey (no more than 15 minutes) seeks your views on the risks associated with online social networking. It specifically looks at the risks to users in the United Kingdom and the ways in which those risks might be managed. The survey is part of a PhD research study to compare different ways of regulating access to personal data gathered by online social networking providers.

Online social networking is based on web-accessible services, which allow users to connect with other users to form social or professional networks. This usually involves setting up a personal profile, which is visible to other users.

In line with City University's research policy, participation in this survey is voluntary. You have the right to withdraw from the survey at any time. Data gathered in this survey will be consolidated so that individual respondents cannot be identified. The data will be used for academic research purposes only. At the end of the survey there will be a consent statement which you will need to confirm before submitting the completed questionnaire.

David Haynes, February 2014

Before we begin we need to find out whether this survey is relevant to you. Where in the UK do you live?*

For the purposes of this survey, the United Kingdom comprises: England, Wales, Scotland and Northern Ireland. It does not include the Isle of Man or the Channel Islands.

( ) England

( ) Wales

( ) Scotland

( ) Northern Ireland

( ) I do not live in the United Kingdom

[Filter question. Non-UK responses terminated at this point]

Use of Social Networks

(1) Do you have an active profile on an online social networking service such as: Facebook, Twitter or LinkedIn?

Online social networks are web-accessible services, which allow users to connect with other users to form social or professional networks. This often means putting up a personal profile that is visible to other users.

( ) Yes
( ) No

(2) If you do use online social networking services, how often do you access them? Use the blank boxes to add the names of online social networks you regularly use, if they are not included in the list.

	Most days	Most weeks	Occasionally	Never
Facebook	( )	( )	( )	( )
Google+	( )	( )	( )	( )
LinkedIn	( )	( )	( )	( )
Twitter	( )	( )	( )	( )

Risks

An earlier survey identified a number of risks associated with use of online social networks. This has been followed up by an extensive literature survey. In this section we have identified the main risks reported so far. We would like your views on what you consider to be the most important risks.

For the purposes of this survey risk is defined as: "a event of unknown probability that has an adverse effect or consequence".

(3) Thinking about your own use of online social networks, how concerned are you personally about the following risks?
Please rank them, with the most important risk at the top.

Please note that this feature is not compatible with early versions of some browsers. If you have difficulty, you can list the risks in the response area for Q4 (the next question).

_____Cyber-bullying or harassment (including stalking)
_____Victim of fraud
_____Identity theft
_____Targeting by official bodies or security agencies
_____Targeting by advertisers
_____Targeting by criminals (e.g. so that they can burgle your home while you are away)
_____Discrimination by employer or potential employer
_____Friends, family or colleagues able to see sensitive personal details
_____Strangers able to see sensitive personal details
_____Physical violence or kidnapping
_____Extortion or blackmail
_____Prosecution by authorities because of crime allegations

(4) Are there any other risks associated with your personal data on online social networks that have not been included in the above list?

_____

Measures to manage risk

(5) Who you think should have primary responsibility for protecting your personal data on online social networks?

( ) **Government** (UK or European Union for instance)
( ) **Online social network providers** (e.g. Facebook, Twitter, LinkedIn, Google)
( ) **Advertisers** (who obtain profile data from online social network providers)
( ) **Users**
( ) **Other** (Please specify): _____

(6) To what extent do you agree or disagree with the following statements? These statements all refer to data about you, which is held by social networking services (SNSs) such as Facebook, Twitter or LinkedIn. We are interested in your views about who should be responsible for protecting your personal data.

	Strongly disagree	Disagree	Agree	Strongly agree
Current data protection **legislation is effective** for protecting my personal data	( )	( )	( )	( )
The **SNS providers should be responsible** for protecting my personal data without government interference	( )	( )	( )	( )
The **SNS providers should work with government** to protect my personal data	( )	( )	( )	( )
SNSs should be set up with **maximum privacy as the default** setting	( )	( )	( )	( )
My personal **profile should only be visible to those people or groups that I specify**	( )	( )	( )	( )
SNSs should be **designed with protection of personal data in mind**	( )	( )	( )	( )
There should be **no external regulation** of personal data on SNSs	( )	( )	( )	( )
As a user **I should be responsible** for my own online privacy	( )	( )	( )	( )

(7) Are there any further measures that you think should be in place to protect personal data gathered by online social networks?
Please give details below.

_____

Background information

Finally, to help us put the results of this survey into context, could you please answer the following quick questions:

(8) Which age range do you fall into?
( ) under 18
( ) 18-24
( ) 25-34
( ) 35-44
( ) 45-54
( ) 55-64
( ) 65+

(9) Gender
( ) Male
( ) Female

(10) Are you a member of the LIS profession (this includes: librarians, information scientists, knowledge managers, records managers, information managers, and archivists)?
Although this survey is primarily targeted at LIS professionals (including students), the results from all respondents will be included in the final analysis.
( ) Yes
( ) No

Consent form

In order to complete this survey we need your informed consent to store and process the data provided in your response. If you agree to your response being used, please answer 'Yes' to the question below. If you choose not to proceed, your response will be discarded.

I agree that my response to this survey can be used for academic research and retained for future academic study. My response will be aggregated so that my identity is not revealed in any publication of results.*
( ) Yes
( ) No

Consent check

Would you like to return to the survey consent form? If you click on 'No' this will confirm that you do not wish to participate in the survey and your response will be discarded.*

( ) Yes
( ) No

Future contact

If you are interested in the results of this survey or in participating in a follow-up study, please select the box(es) below:

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

[ ] I would be interested in participating in a follow-up study

My e-mail address is:

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 on to a third party.

_____

Thank You!

Thank you for completing this survey.

David Haynes

David Haynes is currently researching the relationship between risk and regulation of social networking services as part of his PhD studies at the Centre for Information Science at City University London. He can be contacted at: david.haynes.1@city.ac.uk

Appendix 2. Survey notices to LIS professionals in the UK

Discussion lists on JISCM@il

- LIS-LINK
- RECORDSMANAGEMENT-UK
- LIS-PROFESSION
- LIS-LIRG

LinkedIn Groups

- LIS research methods;
- information research;
- CILIP on LinkedIn;
- Information and Records Management Society Group;
- ISKOUK; and
- London Information and Knowledge Exchange.

Twitter

- Personal Twitter feed

About the authors

David Haynes is a Visiting Lecturer in Information Management at the City University, London where he is studying for a PhD in Information Science. He is researching the relationship between risk, regulation and access to personal data in social media. David Haynes is the corresponding author and can be contacted at: david.haynes.1@city.ac.uk

Dr Lyn Robinson joined the City University London in 2004. She is a Senior Lecturer in Information Science, and Programme Director for Library and Information Science and Computer Science.