



City Research Online

City, University of London Institutional Repository

Citation: Haynes, D. and Robinson, L. (2015). Defining User Risk in Social Networking Services. *Aslib Journal of Information Management*, 67(1), pp. 94-115. doi: 10.1108/AJIM-07-2014-0087

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: <https://openaccess.city.ac.uk/id/eprint/6228/>

Link to published version: <http://dx.doi.org/10.1108/AJIM-07-2014-0087>

Copyright: City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

Reuse: Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.



Defining User Risk in Social Networking Services

Journal:	<i>Aslib Journal of Information Management</i>
Manuscript ID:	AJIM-07-2014-0087.R1
Manuscript Type:	Research Paper
Keywords:	social networking services, social media, regulation, risk, privacy

SCHOLARONE™
Manuscripts

Peer Review

Defining User Risk in Social Networking Services

Abstract

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

Design: 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 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 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: A risk-based view of regulation of personal data on SNSs has not been attempted in such a comprehensive way before.

Keywords: social networking services; social media; regulation; risk; privacy; information privacy; personal data

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 & 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 social media (Dutton & 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):

1
2
3 *By better understanding the threats to privacy, researchers and developers can construct*
4 *countermeasures to mitigate the risks, and users can take informed steps towards protection*
5 *their personal information*

6 This paper sets out to identify the risks to individual SNS users and to develop a model of risk that
7 can be applied more widely to internet use and social media as they continue to evolve. The
8 research questions were:
9

- 10 • What are the risks to individuals that are associated with personal data on SNSs?
- 11 • Is there an existing typology of individual risk that adequately covers SNSs?
- 12 • Can a model of risks to users be used to differentiate between possible regulatory
13 responses?
14

15 Regulation is one area where an up-to-date and relevant model of risk could contribute to improved
16 protection of users. Risk-based regulation has emerged as a dominant approach in Europe and the
17 UK in the last few decades. Baldwin, Cave and Lodge (2012, p.83) suggest that *“Regulation can be*
18 *seen as being inherently about the control of risks...”*. This is a view supported by Hutter (2006,
19 p.205): *“...regulation has come to be defined as controlling and also as a way of managing risks”*.
20

21 *Methodology*

22 In order to address these questions, this research was based on a systematic review of the literature,
23 and a survey of information professionals in the UK. Modelling techniques were used to develop a
24 concept of risk that is relevant to internet use and, more specifically, to SNSs. The literature review
25 identified general risk typologies which were analysed in terms of: their applicability to SNSs; their
26 focus on risk to individuals; and their ability to distinguish between types of risk to individuals.
27

28 A survey of library and information service (LIS) professionals in 2014 provided insight into the
29 perceived importance of different risk categories (Appendix A). This sector was chosen because it is a
30 well-developed professional group representing users (many LIS staff act as intermediaries), and
31 who are information literate and are therefore likely to be exposed to a wide range of online
32 scenarios. It is also a cohesive group with a track record of active use of social media (Cooke & Hall
33 2013). The survey was directed at UK users of SNSs using a filter question at the start of the survey
34 to exclude non-UK users. This was cross-checked against the location of the IP Address of the device
35 accessing the survey and logged by SurveyGizmo. The survey objective was to identify the range of
36 risks to which users are exposed and to gain some insight into the perceptions of risk and priorities
37 for managing risk. The survey was based on purposive sampling directed at LIS professionals in the
38 UK, using a variety of forums (listed in Appendix B) to generate a snowball effect (David & Sutton
39 2011, p.232). Participants were encouraged to publicise the survey through their own professional
40 and personal networks.
41

42 A model of risks was developed from an analysis of the consolidated lists of risks identified in the
43 survey and the literature. A typology was developed which formed the basis of a model of personal
44 risk in SNSs. The event and consequence of each risk was analysed to identify the relationship
45 between the risks and to develop a definitive set of outcomes which might have the potential as a
46 tool to evaluate different regulatory approaches.
47

48 *Privacy and risk*

49 Information privacy is an important aspect of any discussion about personal data on SNSs. The
50 volume of personal data available on SNSs puts it firmly in the category of ‘big data’. It has been
51 suggested that when dealing with big data *“the change of scale leads to a change of state”* and that
52 *“this transformation not only makes protecting privacy much harder, but also presents an entirely*
53 *new menace: penalties based on propensities”* (Mayer-Schönberger & Cukier 2013, p.151). For
54 instance, where security agencies try to prevent terrorist acts by pre-empting them, individuals are
55 targeted and may be arrested or have their movements restricted without being convicted of any
56 crime. Another problem is ‘fetishizing’. This is a common fallacy identified elsewhere (Hansson
57
58
59
60

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:

- User identification – unique identifiers, cookies and other forms of user identification
- Adware, spyware and malware conduct covert data logging and surveillance
- Deep packet inspection (DPI)
- Pervasive geo-location technology: an emerging threat to Internet privacy
- Data processing and facial recognition
- Internet surveillance technology

(Mendel et al. 2012, pp.39–49)

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)
- 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
3. Harvesting and use of personal data on social networks by advertisers

(Nissenbaum 2010)

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 & 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*

1
2
3 *respect to something that humans value” (Aven & Renn 2009, p.2). From the regulatory sphere a*
4 *working definition is: “...risk is usually defined as the probability of a particular event (or hazard)*
5 *occurring and the consequent severity of the impact of that event” (Baldwin et al. 2012, p.82).*
6

7 For the purposes of this paper risk is defined as an uncertain event which has an adverse impact on
8 an activity or outcome. Applied here, risk is an event of unknown probability of occurrence involving
9 personal data on an SNS that has a negative impact on that person. For instance, an individual’s data
10 might be copied for the purposes of fraud, resulting in that individual suffering financial loss.
11

12 13 14 **Typologies of Risk in the Literature**

15 *A general typology of risk*

16 Some early commentators have attempted to identify risks associated with the use of SNSs
17 (Rosenblum 2007). However going back to more general approaches to risk identification provides a
18 wider picture. There can be a distinction between physical and social risks which can be integrated
19 (Macgill & Siu 2005, pp.1108–1110). Tulloch (2006, pp.132–133) adopts a social approach to risk:
20

21 *Thus, it seems clear that current research is positively engaged with the construction of self-identities*
22 *in conditions of risk that these frequently take account of the reflexive concern for dialogic*
23 *negotiation within and between everyday 'lay voices' and professionals, and that by and large this*
24 *work ... embeds 'wider social understanding' analysis in quite traditional understandings of the*
25 *'otherness' of age, gender, sexual preference, class, and (dis)ability.*
26

27 Swedlow and associates’ (2009, p.237) research into risk and regulation is based on the
28 “construction of a universe of nearly 3,000 risks...over a thirty-five year period”. This provides a
29 comprehensive view of the types of risk that exist generally and is used as a starting point for
30 identifying and categorising the risks faced by SNS users. Some of these risks would arise directly
31 from misuse of data; others are related to the data held about individual history, behaviour and
32 preferences. The following categories from this ‘universe’ of risks might be applicable to social media
33 and specifically to SNSs:
34

35
36 **Crime and violence** – There have been a number of court cases where revealing personal
37 data of individuals on social media has exposed them to threats of violence or to harassment
38 (Agate & Ledward 2013)

39 **Recreation** – A great deal of use of social networks is for recreation rather than professional
40 purposes and it could be argued that the other risks associated with social media fall into
41 this category
42

43 **War, security and terrorism** – With the WikiLeaks revelations starting in 2010 and the NSA
44 scandal in 2013 the press has paid particular attention to the security aspects of personal
45 information (Leigh & Harding 2011; BBC News 2012; Greenwald 2013). The risks to users are
46 two-fold. The first is that identifying information on social networks may be used to victimise
47 or persecute an individual by a state or terrorist organisation. The second is that an
48 individual’s identity may be stolen for use by terrorists or by state security agencies and in
49 doing so potentially expose them to harm
50

51 **Political, social and financial** – Political, social and financial harm can arise from identity
52 theft. For example, if sufficient biometric data is available on a users’ profile it may be
53 possible to set up a false identity to gain access to credit or to purchase products with no
54 intention of paying. The individual whose identity has been stolen may be pursued for
55 payment and may even be liable for debts and costs incurred through the fraud
56
57
58
59
60

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

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

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

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

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
- 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 1 shows these risks grouped into nine main headings.

-Take in Table No. 1-

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:

Cyber-bullying

1
2
3 Privacy breaches
4 Reputational damage
5 Assault on personal dignity
6

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

9 *Risks associated with geo-location data*

10 Geo-location data is an increasingly important part of the delivery of SNSs. By allowing their location
11 to be uploaded by mobile service providers and applications providers, users benefit from enhanced
12 services such as location of nearby restaurants, identification of friends in the vicinity and local
13 maps. However there are also concerns about the risks that users are exposed to when their location
14 data is available. This is a problem that the European Commission is well aware of (Article 29
15 Working Party 2013).
16

17 A number of mechanisms by which geo-location data is gathered or can be reconstructed have been
18 identified. These raise some concerns about the resulting loss of privacy (Andrienko & Andrienko
19 2012). Andrienko and colleagues (2013) go on to enumerate the ways in which geo-location data is
20 gathered:
21

- 22 • Whenever a mobile device is in use it sends a signal to the service provider. However the
23 provider can send a silent text message to force active communication without alerting the
24 user
25
- 26 • Call data records are another source of geo-location data, which came to prominence in the
27 NSA revelations in 2013 and these can give time-based data on movements (Greenwald
28 2013)
- 29 • Signal strength data can be used to triangulate the position of a mobile device
- 30 • Users often consent (not always in an informed way) to their location being identified by
31 apps providers or the mobile service provider for enhanced services. This data might be
32 associated with the user ID which has obvious privacy implications
- 33 • Anonymous location data seems to provide better protection, although the authors show
34 how identity and even time-based movement data can be reconstructed
- 35 • Some non-location data such as accelerometer data, which is freely available from some
36 devices, can be used to deduce the location with a reasonable degree of accuracy
37

38 The description of these mechanisms helps to highlight how easy it is for geo-location data to be
39 gathered without the knowledge or understanding of the user, and how this information is available
40 to service providers, mobile operators and apps providers.
41

42 **Risks Identified in the Survey**

43 The survey of UK-based LIS professionals ranked risks to provide an indication of priorities. The score
44 is a weighted calculation. In Table 2 the item with the highest score is ranked first. In each case the
45 score is the sum of all weighted rank counts:
46

47 -Take in Table No. 2-

48 'Identity theft' and 'Strangers being able to see sensitive personal details' both had high scores in the
49 ranking. Identity theft can itself expose users to other risks such as fraud (ranked 4) and one of the
50 consequences can be financial loss. For instance, if a user's identity is used to apply for a loan or
51 credit facilities, the victim may be left with the liability to pay back the loan.
52

53 'Strangers being able to see sensitive personal details' ranked much more highly than 'Friends, family
54 and colleagues being able to see sensitive details'. There is a dual risk of strangers seeing personal
55 details – firstly as a means to commit fraud, and secondly because it exposes users to discrimination
56
57
58
59
60

1
2
3 by potential or actual employers, for instance. Additional comments from users were concerns
4 about reputational damage and loss of face. Personal information may be exposed by the actions of
5 others, such as when friends mention an individual or tag photographs or other entries with their
6 names (Thomas et al. 2010).
7

8 Some of the risks may have consequences that are more to do with social awkwardness or
9 annoyance rather than loss of money or physical threat. For instance, targeting by advertisers may
10 be irritating rather than life-threatening. Potentially there is the loss of face if another person makes
11 assumptions about an individual on the basis of advertising that appears on a screen. There is also
12 the inconvenience of screen clutter and slowing down of browsers if there is a lot of graphics or
13 moving images to download.
14

15 **A consolidated model of risk**

16 *Developing a typology of risk*

17 Consolidation of these risk categories yields a typology of risk related to use of SNSs. However not all
18 these risks are related to access to personal data, but relate to intellectual property, security and
19 organisational issues.
20

21 Three approaches to devising a typology of risk for this domain were considered. Risks can be
22 categorised by:
23

- 24 Risk event
- 25 Stakeholder affected
- 26 Consequence
- 27
- 28

29 *Risk event*

30 A risk consists of an event, for which there is a degree of uncertainty about whether it will occur
31 AND the consequence or outcome should it occur. The first part of this definition is the 'risk event'.
32 Risks can be categorized according to a universal set of risks such as those identified by researchers
33 at Duke University and Northern Illinois University (Swedlow et al. 2009). These are based on risk
34 events or threats. This categorisation does not take into account severity, or impact, or which
35 stakeholders are affected.
36

37 Some threats or risks could fall under more than one heading. For instance, identity theft could be
38 under 'Crime and Violence', if it leads to fraud and eventual financial loss to the individual whose
39 data was 'stolen'. It could also be under 'War Security and Terrorism', where identity theft (the same
40 event) results in a different outcome – a terrorist using an alias to escape detection, for instance. It
41 could be argued that this might expose an individual to even greater harm such as the loss of liberty
42 or even loss of life.
43

44 *Stakeholder affected*

45 Risks can be analysed in terms of the stakeholders. In a pilot investigation prior to the survey the SNS
46 stakeholders were identified as: users, service providers, advertisers, employers, and government.
47 However because this study is considering the risks associated with allowing access to personal data
48 on SNSs, it is not surprising that the majority of risks will primarily affect users. Indeed a preliminary
49 analysis of the risks identified to date (Table 1) bears this out. Apart from work-related risks which
50 primarily affect employers, the remaining risks all have some direct impact on users.
51

52 Although main risks are faced by users, release of personal data can have a negative impact on
53 employers by damaging reputations or exposing them to legal action or prosecution. There might be
54 wider risks to government or society if personal data is misappropriated and used for terrorist
55 activities or economic sabotage, for instance. Many of the risks to employers of using SNSs in the
56 workplace are not related to access to personal data. They include issues such as: time wasting,
57
58
59
60

1
2
3 security breaches, copyright, and libel where staff members post inappropriate materials on an SNS
4 site during work hours or on a site with a strong presence by or association with the employer.

5
6 The other side of the argument is determining who benefits from access to personal data.
7 Advertisers, and those that pay them or whom they pay, benefit directly from accessing personal
8 data, consolidated or not. Indirectly government benefits because of increased tax revenue from the
9 resulting economic activity. Potentially users also benefit – because of more tailored experience of
10 services and targeted advertising – presumably some value is perceived otherwise no-one would
11 follow the links and there would be no point in advertisers using this as a method of gaining new
12 custom.

13 14 *Consequence*

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

17 18 Tangible risks

- 19 • Discrimination
- 20 • Identity theft
- 21 • Abuse of power by the state
- 22 • Physical harm

23 24 Intangible risks

- 25 • The chilling effect
- 26 • The feeling of helplessness
- 27 • The apprehension of future harm

28
29
30 This grouping moves towards the idea of categorising risks by their consequences rather than by the
31 nature of the risk event. This can be further refined by concentrating on consequences to users
32 specifically (see Table 3). This provides a means of quantifying the risks, banding them in risk severity
33 categories, or at least a relative ranking.

34
35 -Take in Table No. 3-

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

41
42 A further complication is that a consequence such as cyber-bullying arising from exposure of
43 sensitive data to an inappropriately wide group, could itself lead to further consequences such as
44 self-harm, loss of self-esteem and social isolation.

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

50 51 **Discussion**

52 53 *A risk model for SNSs*

54 Any categorisation is to some extent arbitrary and so it is necessary to identify what criteria are used
55 to select an appropriate approach. Very few commentators in this area have explicitly selected one
56 or other of the three approaches discussed in this paper – analysis by: risk event; stakeholder; or
57
58
59
60

1
2
3 consequence. For the purposes of this study the key consideration is whether this allows
4 differentiation of risks in terms of possible regulatory responses.

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

9
10 The stakeholder approach is used by other researchers focusing on risks specifically associated with
11 SNS use from an employer's perspective (Langheinrich & Karjoth 2010). They go beyond the scope of
12 this study by including risks associated with company information as well as general exposure on
13 social networks. However they identify many relevant risks and this coupled with other analyses that
14 focus on the user perspective, results in a list of risks based on stakeholder groups. This offers a
15 method for investigating the effects of regulation (Ellison & Boyd 2013). The same event (e.g.
16 sharing personal data with advertisers) may have quite different effects on each group. For instance,
17 making personal data available to the partners of an SNS provider may be good for advertisers and
18 some consumers, and bad for other users (especially those not looking to purchase).

19
20 There are two main problems with the stakeholder approach. The first is that the majority of risks
21 associated with inappropriate access to personal data will directly affect the user. As this study is
22 concerned with risks to individuals, this is not a good way of distinguishing between risks. The other
23 problem is that the list is long and un-differentiated within these two main categories, with overlap
24 and potential gaps in coverage.

25
26 The third approach analyses risk in terms of its consequences and this provides a smaller number of
27 main headings under which risks can be grouped (see Table 3). This approach also allows addition of
28 a stakeholder aspect so that analysis by this criterion is also possible.

29
30 The survey brought in wider perspectives on what the risks to individuals were and how those risks
31 interacted. Analysis of the risks identified and the relationships between those risks provides a clear
32 distinction between risk events and their consequences. A map of the relationships between risks
33 categories was developed (Figure 1) from the typology based on consequences of risks events (Table
34 3). This allows the development of a model of risk relationships. The model emphasises the difficulty
35 of defining limits around the definitions of each risk category, a pre-requisite for measuring or
36 quantifying risk.

37
38 The analysis of consequences produces a more complex picture than a simple listing (Table 3) can
39 reveal. One of the challenges of trying to analyse risk is that some consequences may themselves
40 expose individual to new risks and therefore to other types of harm. The figure uses red arrows to
41 point to the risk consequences and labelled black arrows to look at the relationship between
42 underlying risks.

43
44 -Take in Figure No. 1-

45
46 This grouping of risks has allowed an inductive derivation of five categories of consequences to
47 users. Within each category, the contributing risks events are described.

48
49 **Nuisance** includes being bombarded with advertisements or users being inconvenienced by having
50 to go through extra steps to preserve their privacy. This could also include intrusion into private lives
51 by strangers, where no other direct harm is felt.

52
53 **Psychological harm** can result from exposure of private information and also from harassment and
54 cyberbullying. This can range from mild social embarrassment when personal information is
55 circulated to those that the data subject would not be comfortable with, through to victimisation
56 and threats. It can also result from a feeling of helplessness engendered by loss of control over who
57 has access to personal data.

1
2
3 **Financial and material loss** can arise from criminal targeting through or from fraud as a result of ID
4 theft. Active discrimination in the job market – for instance by religion, race, trade union activity or
5 sexuality, all of which may be inadvertently revealed on SNS profiles. Theft of intellectual property
6 via SNSs – especially where users are encouraged to post pictures, videos etc. could result in loss of
7 revenue (Rosenblum 2007, p.46). There have also been cases reported in the press of people
8 inadvertently advertising when they are away, making them targets for burglary or home invasions
9 (Roberts 2010; BBC News 2013).

10
11 **Loss of liberty** is a dramatic consequence of personal data being made available on SNSs. This could
12 be either as a result of exposure of criminal activity or being mistakenly identified as a criminal or
13 terrorist (Strauß & Nentwich 2013). Boasts about drug-taking on SNSs or evidence of location could
14 be used as evidence of criminal activity. Profiling by security services and police are approximate
15 tools that have led to targeting of innocent people with consequent loss of liberty, political
16 persecution and financial loss.

17
18 **Physical harm** can be a consequence of criminal targeting – for instance during a robbery or a
19 kidnapping. Personal data can reveal information about movements, routines and intent and
20 therefore make it easier for criminals to target the individual. There are also concerns about
21 personal information revealing the location of shelters for those escaping domestic abuse.

22 23 **Conclusion**

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

30
31 A list of risks does not, however, describe the relationship between different risk categories. This is
32 important because of the strong interdependence between them.

33
34 A risk model that more accurately represents the potential threats to users and the consequences
35 can be used as a tool for investigating different modalities of regulation. As much of current
36 regulatory activity is risk-based, this approach could provide a means of evaluating different
37 regulatory approaches. For example, it might be possible to consider whether proposed changes in
38 legislation tend to increase or reduce each of the risk categories in terms of probability of
39 occurrence and severity of impact.

40
41 This up-to-date perspective on user risk is of potential utility to policy makers and decision makers.
42 Legislators need a more nuanced tool than currently exists for evaluating proposed new laws or
43 regulations. Service providers can consider the effect of different privacy settings and proposed new
44 services on users, and systems designers have a tool that they can adopt to demonstrate that they
45 are following 'privacy-by-design' principles.

46
47 The risk model also provides a conceptual framework for trainers, educators and information
48 intermediaries. These are all roles that are increasingly forming a part of the role of library and
49 information service (LIS) professionals. Their role in modifying user behaviour by example and by
50 user education could have a significant effect in helping users to derive the greatest benefit safely
51 from SNSs and from social media generally.

References

- Agate, J. & 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*. Cambridge: Computer Laboratory, Available at: <http://www.repository.cam.ac.uk/handle/1810/244239> [Accessed December 3, 2013].
- Andrienko, G. et al. (2013), "Report from Dagstuhl", *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 17 No. 2, p.7.
- Andrienko, G. & Andrienko, N. (2012), "Privacy issues in geospatial visual analytics", In G. Gartner & F. Ortog (eds.), *Advances in Location-Based Services. 8th International Conference on Location Based Services, 2011, Vienna*. Heidelberg: Springer, pp. 239–246.
- Article 29 Working Party (2013), *WP29 opinion on apps on mobile devices. 00461 /13/EN WP 202*, Brussels, Available at: https://www.huntonprivacyblog.com/wp-content/uploads/2013/03/wp202_en.pdf [Accessed March 4, 2014].
- Aven, T. & 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. & Lodge, M. (2012), *Understanding regulation : theory, strategy, and practice* (2nd ed.), Oxford: Oxford University Press.
- Bawden, D. & 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 (2013), "BBC News - Arrests made in Brian Holloway's trashed house party", *BBC News*, Available at: <http://www.bbc.co.uk/news/world-us-canada-24293414> [Accessed February 11, 2014].
- BBC News (2012), "BBC News - Wikileaks revelations", *BBC News Online*, Available at: <http://www.bbc.co.uk/news/world-11863274> [Accessed July 7, 2014].
- British Standards Institution (2010), *BS ISO 31000:2009 Risk management — Principles and guidelines*, London.
- Cooke, L. & 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. & Sutton, C.D. (2011), *Social research : an introduction*, Los Angeles: SAGE.

- 1
2
3 Dutton, W.H. & Blank, G. (2013), *Cultures of the Internet: The Internet in Britain*. Oxford
4 *Internet Survey 2013*, Oxford, UK. Available at:
5 [http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.](http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf)
6 pdf.
7
- 8 Ellison, E.B. & Boyd, D.M. (2013), "Sociality through social network sites", In W. H. Dutton
9 (ed.) *The Oxford handbook of Internet studies*. Oxford: Oxford University Press, pp.
10 151–172.
11
- 12 European Economic and Social Committee (2010), *Opinion of the European Economic and*
13 *Social Committee on the "impact of social networking sites on citizens/consumers"*
14 *(own-initiative opinion) (2010/C 128/12)*, European Union: OJ (2010/C 128/12) 18 May
15 2010. Available at: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:EN:PDF)
16 [lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:EN:PDF).
17
18
- 19 Farr, C. (2013), "Can you trust Facebook with your genetic code?", *VentureBeat*. Available
20 at: <http://venturebeat.com/2013/10/07/can-you-trust-facebook-with-your-genetic-code/>
21 [Accessed October 10, 2013].
22
23
- 24 Greenwald, G. (2013), "NSA collecting phone records of millions of Verizon customers
25 daily", *The Guardian*. Available at: [http://www.theguardian.com/world/2013/jun/06/nsa-](http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order)
26 [phone-records-verizon-court-order](http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order) [Accessed July 7, 2014].
27
28
- 29 Hansson, S.O. (2004), "Fallacies of risk", *Journal of Risk Research*, Vol. 7 No. 7, pp.353–
30 360.
31
- 32 Hutter, B.M. (2006), "Risk, Regulation and Management", In J. Taylor-Gooby, Peter; Zinn,
33 (eds.) *Risk in Social Science*. Oxford: Oxford University Press, pp. 202–227.
34
- 35 Langheinrich, M. & Karjoth, G. (2010), "Social networking and the risk to companies and
36 institutions", *Information Security Technical Report*, Vol. 15 No. 2, pp.51–56.
37
38
- 39 Leigh, D. & Harding, L. (2011), *Wikileaks: inside Julian Assange's war on secrecy*, London:
40 Guardian Books.
41
- 42 Lynskey, O. (2012), *Identifying the Objectives of EU Data Protection Regulation and*
43 *Justifying its Costs (PhD Thesis)*. University of Cambridge, Lucy Cavendish College.
44
- 45 Macgill, S.M. & Siu, Y.L. (2005), "A new paradigm for risk analysis", *Futures*, Vol. 37 No.
46 10, pp.1105–1131.
47
48
- 49 Mann, B.L. (2009), "Social Networking Websites: a concatenation of impersonation,
50 denigration, sexual aggressive solicitation, cyber-bullying or happy snapping videos",
51 *International Journal of Law and Information Technology*, Vol. 17 No. 3, pp.252–264.
52
- 53 Mayer-Schönberger, V. & Cukier, K. (2013), *Big data : a revolution that will transform how*
54 *we live, work and think*, London: John Murray.
55
56
57
58
59
60

- 1
2
3 McDonald, T. (2013), "Kids + Facebook = Home Invasion?", *Business 2 Community*.
4 Available at: [http://www.business2community.com/facebook/kids-facebook-home-](http://www.business2community.com/facebook/kids-facebook-home-invasion-0618724)
5 [invasion-0618724](http://www.business2community.com/facebook/kids-facebook-home-invasion-0618724) [Accessed October 10, 2013].
6
- 7 Mendel, T. et al. (2012), *Global Survey on Internet Privacy and Freedom of Expression*
8 (*Unesco series on internet freedom*), Paris: UNESCO Publishing.
9
- 10 Nissenbaum, H.F. (2010), *Privacy in context : technology, policy, and the integrity of social*
11 *life*, Stanford, Calif.: Stanford Law Books.
12
- 13 Pearsall, J. & Hanks, P. (eds.) (1999), *The New Oxford Dictionary of English*, Oxford:
14 Oxford University Press.
15
- 16 Roberts, L. (2010), "BBC News - Facebook status updates are "burglary risk."", *BBC News*
17 *Online*. Available at: <http://www.bbc.co.uk/news/uk-england-birmingham-12062331>
18 [Accessed July 7, 2014].
19
- 20 Rosenblum, D. (2007), "What Anyone Can Know: The Privacy Risks of Social Networking
21 Sites", *IEEE Security & Privacy*, Vol. 5 No. 3, pp.40–49.
22
- 23 Solovic, S. (2013), "The Social Media Dilemma: Managing Business Benefits And Personal
24 Risks", *Business 2 Community*. Available at:
25 [http://www.business2community.com/social-media/social-media-dilemma-managing-](http://www.business2community.com/social-media/social-media-dilemma-managing-business-benefits-personal-risks-0597574)
26 [business-benefits-personal-risks-0597574](http://www.business2community.com/social-media/social-media-dilemma-managing-business-benefits-personal-risks-0597574) [Accessed October 10, 2013].
27
- 28 Strauß, S. & Nentwich, M. (2013), "Social network sites, privacy and the blurring boundary
29 between public and private spaces", *Science and Public Policy*, Vol. 40 No. 6, pp.724–
30 732.
31
- 32 Swedlow, B. et al. (2009), "Theorizing and Generalizing about Risk Assessment and
33 Regulation through Comparative Nested Analysis of Representative Cases", *Law &*
34 *Policy*, Vol. 31 No. 2, pp.236–269.
35
- 36 Thomas, K., Grier, C. & Nicol, D.M. (2010), "unFriendly: Multi-party Privacy Risks in
37 Social Networks", M. J. H. Atallah NJ (ed.), *Lecture Notes in Computer Science*, 6205,
38 pp.236–252.
39
- 40 Tulloch, J. (2006), "Everyday life and Leisure Time", In P. Taylor-Gooby & J. Zinn (eds.),
41 *Risk in Social Science*, Oxford: Oxford University Press, pp. 117–139.
42
- 43 Wakefield, J. (2014), "BBC News - Cyberbullies: How best to tackle online abuse?", *BBC*
44 *News Online*. Available at: <http://www.bbc.co.uk/news/technology-26121199> [Accessed
45 July 7, 2014].
46
- 47 Wilson, R.E., Gosling, S.D. & Graham, L.T. (2012), "A Review of Facebook Research in the
48 Social Sciences", *Perspectives on Psychological Science*, Vol. 7 No. 3, pp.203–220.
49
50
51
52
53
54
55
56
57
58
59
60

Acknowledgments:

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.

Biographical Details

David Haynes is a visiting lecturer in Information Management at 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.

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

For Peer Review

Table 1 – Personal risks associated with SNSs

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 from 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
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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Table 2 – Ranking of risks from a survey of LIS professionals

Item	Score	Overall Rank
Identity theft	1934	1
Strangers able to see sensitive personal details	1841	2
Targeting by advertisers	1575	3
Victim of fraud	1531	4
Discrimination by employer or potential employer	1443	5
Targeting by criminals (e.g. so that they can burgle your home while you are away)	1411	6
Friends, family or colleagues able to see sensitive personal details	1297	7
Cyber-bullying or harassment (including stalking)	1288	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

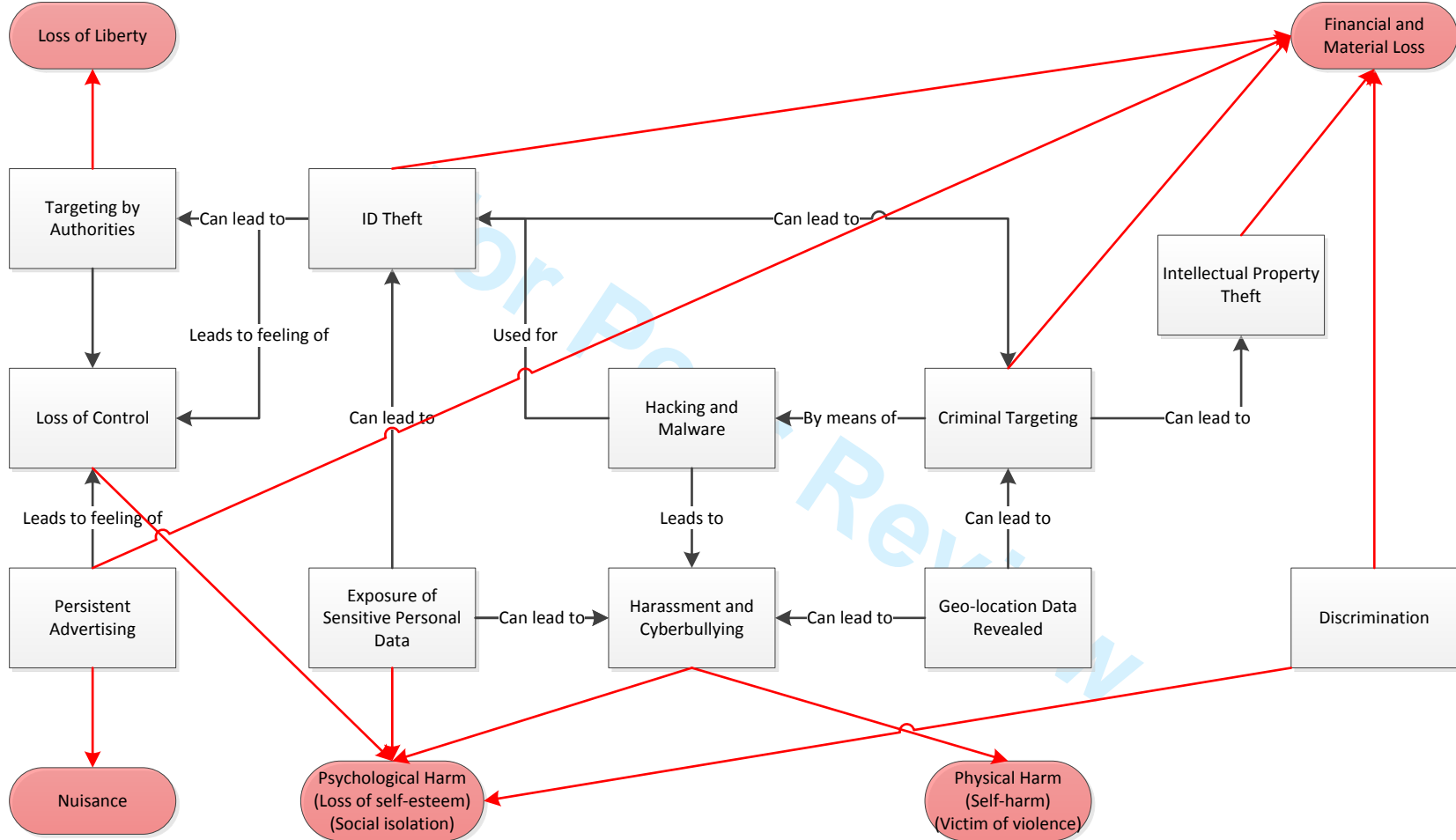
Total Respondents: 213

Peer Review

Table 3 – Analysis of risks by their consequences to users

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

Figure 1 – Relationships between risk events and their consequences



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47

Appendix A – 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Google+	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LinkedIn	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Twitter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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)

- 1
2
3 _____ Victim of fraud
4 _____ Identity theft
5
6 _____ Targeting by official bodies or security agencies
7
8 _____ Targeting by advertisers
9
10 _____ Targeting by criminals (e.g. so that they can burgle your home while you are away)
11 _____ Discrimination by employer or potential employer
12 _____ Friends, family or colleagues able to see sensitive personal details
13 _____ Strangers able to see sensitive personal details
14
15 _____ Physical violence or kidnapping
16
17 _____ Extortion or blackmail
18
19 _____ Prosecution by authorities because of crime allegations
20
21
22

23 **4) Are there any other risks associated with your personal data on online social networks**
24 **that have not been included in the above list?**
25
26 _____
27
28
29
30 _____
31

32 **Measures to manage risk**

33
34
35 **5) Who you think should have primary responsibility for protecting your personal data on**
36 **online social networks?**

- 37 **Government** (UK or European Union for instance)
38
39 **Online social network providers** (e.g. Facebook, Twitter, LinkedIn, Google)
40
41 **Advertisers** (who obtain profile data from online social network providers)
42
43 **Users**
44 **Other** (Please specify): _____
45
46
47

48 **6) To what extent do you agree or disagree with the following statements? These**
49 **statements all refer to data about you, which is held by social networking services (SNSs)**
50 **such as Facebook, Twitter or LinkedIn. We are interested in your views about who should be**
51 **responsible for protecting your personal data.**
52

	Strongly disagree	Disagree	Agree	Strongly agree
--	--------------------------	-----------------	--------------	-----------------------

53
54
55
56
57
58
59
60

1 2 3 4 5 6 7	Current data protection legislation is effective for protecting my personal data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8 9 10 11	The SNS providers should be responsible for protecting my personal data without government interference	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12 13 14 15 16	The SNS providers should work with government to protect my personal data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
17 18 19	SNSs should be set up with maximum privacy as the default setting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20 21 22 23 24	My personal profile should only be visible to those people or groups that I specify	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
25 26 27	SNSs should be designed with protection of personal data in mind	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
28 29 30 31	There should be no external regulation of personal data on SNSs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
32 33 34 35	As a user I should be responsible for my own online privacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

36
37
38
39
40
41
42
43
44
45
46
47
48

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.

49
50

Background information

51
52
53
54

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

55
56
57
58
59
60

8) Which age range do you fall into?

under 18

- 1
2
3 18-24
4 25-34
5
6 35-44
7
8 45-54
9
10 55-64
11 65+

12
13
14
15 **9) Gender**

- 16 Male
17
18 Female
19

20
21
22 **10) Are you a member of the LIS profession (this includes: librarians, information scientists,**
23 **knowledge managers, records managers, information managers, and archivists)?**

24 *Although this survey is primarily targeted at LIS professionals (including students),*
25 *the results from all respondents will be included in the final analysis.*

- 26
27 Yes
28
29 No
30
31
32
33

34
35 **Consent form**

36
37 **In order to complete this survey we need your informed consent to store and process the**
38 **data provided in your response. If you agree to your response being used, please answer**
39 **'Yes' to the question below. If you choose not to proceed, your response will be discarded.**
40
41

42
43
44 ***I agree that my response to this survey can be used for academic research and retained for***
45 ***future academic study. My response will be aggregated so that my identity is not revealed***
46 ***in any publication of results.****

- 47 Yes
48
49 No
50
51
52
53

54
55 **Consent check**
56
57
58
59
60

1
2
3 ***Would you like to return to the survey consent form? If you click on 'No' this will confirm***
4 ***that you do not wish to participate in the survey and your response will be discarded.****

5 Yes

6
7 No

11
12
13 **Future contact**

14
15 ***If you are interested in the results of this survey or in participating in a follow-up study,***
16 ***please select the box(es) below:***

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

18
19 I would be interested in participating in a follow-up study

20
21
22
23
24 **My e-mail address is:**

25 ***If you give your e-mail address it will only be used for the purposes you have***
26 ***indicated in this response and will not be passed on to a third party.***

28
29
30
31
32
33 **Thank You!**

34
35
36
37 **Thank you for completing this survey.**

38
39 **David Haynes**

40
41
42 ***David Haynes is currently researching the relationship between risk and regulation of***
43 ***social networking services as part of his PhD studies at the Centre for Information Science***
44 ***at City University London. He can be contacted at: david.haynes.1@city.ac.uk***
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Appendix B – 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
- London Information and Knowledge Exchange

Twitter

- Personal Twitter feed

Original Peer Review

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60