International Journal of Information Management 36 (2016) 872–882

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

A regulatory model for personal data on social networking services in the UK

David Haynes*, David Bawden, Lyn Robinson

Department of Library and Information Science, City University London, Northampton Square, London EC1V 0HB, United Kingdom

ARTICLE INFO

Article history:
Received 21 October 2015
Received in revised form 4 May 2016
Accepted 13 May 2016

Keywords:
Regulation
Data protection
Social networks
Privacy

ABSTRACT

Widespread use of online social networking services (SNSs) exposes users to a variety of risks. This study examines the UK's Data Protection Act 1998 (DPA) and considers the wider regulatory landscape in the UK. Although based on EU legislation, the DPA has shortcomings in enforcement and in regulating global services using national legislation. Lessig's model of internet regulation was used as a starting point to examine the alternative regulatory mechanisms that apply to personal data on SNSs. Interviews with industry experts highlighted self-regulation as a major influence on the behaviour of users and SNS providers. This has been incorporated into a new model of regulation that applies to SNSs. The resulting model has identified the following modes: law (statutory legislation), self-regulation (privacy policies and self-regulation of the online advertising industry), code (the way services are designed and their system architecture), and norms (expressed as user behaviour and collectively as market behaviour). The paper concludes that this new model of regulation is needed to adequately describe the current regulatory landscape as it applies to social media. This may form a better basis for evaluation of regulatory effectiveness in the future.

1. Introduction

1.1. Background

Increasing use of online social networking services (SNSs) has raised concerns about the ways in which personal data is exposed to general view and the risks that can result (Haynes & Robinson, 2015). SNSs are used in a variety of ways and contexts. For instance, Facebook is a largely social and leisure network but increasingly is being used for campaigning and marketing. LinkedIn is a largely professional network. Twitter has many communities for live-streaming of events (from natural disasters, to conferences, parties and festivals) and news, and for some professional and academic material, as well as keeping up with friends and feeding on celebrity gossip. A new generation of ephemeral services such as Whatsapp and Snapchat are used for instant messaging and status updates.

These services are largely free of charge to users and the network providers gain revenue mostly from selling personal data profiles to advertisers. Although this personal data is aggregated and to some extent anonymized, there are concerns about de-anonymization of data and about online behavioural advertising and its potential intrusiveness (Christiansen, 2011; De Lima & Legge, 2014; Litvínov, 2013; Scott, 2013). There is also increasing concern about the risks that users face when their data is shared with third parties or used in unexpected ways (Denham, 2009). Butler (2011) showed that periodic modifications to Facebook's privacy policy meant that users did not know what settings applied to their profiles. Two reports in the New York Times highlighted the risks associated with the introduction of new features that impact on privacy (Helft & Wortham, 2010; Story & Stone, 2007). Web beacons provided third party sites with details of purchases by Facebook members, which were automatically posted on friends' newsfeeds. This led to an outcry about invasion of privacy and the setting change was reversed.

Wider concerns raised by the regulatory authorities and campaigning groups have focused on dangers posed by exposing personal details on SNS profiles. Cases of burglary, home invasion, threats and actual physical violence have all been attributed to abuse of personal data on SNSs (BBC News, 2013a; McDonald, 2013; Roberts, 2010). There have been tragic cases of bullying that have led to self-harm or even suicide (Blake, 2015; Cox, 2014; The Moscow Times, 2015; Wakefield, 2014). Other commentators have also considered the risks to children of grooming, bullying and abuse via social media (Livingstone, 2013; Slavtcheva-Petkova, Nash, & Bulger, 2015; Staksrud & Livingstone, 2009).

* Corresponding author.
E-mail addresses: david.haynes@city.ac.uk (D. Haynes), d.bawden@city.ac.uk (D. Bawden), l.robinson@city.ac.uk (L. Robinson).

http://dx.doi.org/10.1016/j.ijinfomgt.2016.05.012
0268-4012/

One response to these risks is to regulate access to personal data. For instance, in the United Kingdom (UK) the Data Protection Act 1998 (based on the European Data Protection Directive 95/46/EC) provides some remedy against these risks.

Lessig (2006) devised a model of regulation of the internet which identifies: law, code, norms and market as regulatory modes. This model was analysed by Cooke (2004) and is developed further in this paper to reflect the current regulatory landscape for SNSs in the UK. Other commentators have considered the application of Lessig's model in countries such as Singapore and Brazil, as well as the European Union (Jiow, 2013; Lynskey, 2012; Medeiros & Bygrave, 2015).

1.2. Objectives

This paper sets out to map the nature of regulation of access to personal data on SNSs. It is focused on the European regulatory framework as it applies in the UK and incorporates national, international and global responses to issues of privacy and protection of personal data.

This paper develops a conceptual model to describe the regulatory modes that apply to protection of personal data on online SNSs. One of the purposes of regulation is to reduce risk (Baldwin, Cave, & Lodge, 2012; Hutter, 2006). The model focuses specifically on reduction of risk to users and looks at the nature of the risks that users face. This can be characterized by the degree of personalization of the data and its sensitivity in terms of perceived or actual harm that arises from misuse.

2. Methods

An 'interpretivist' approach, as suggested by Weber and others is used to gain a fuller understanding of the different regulatory modes and their interaction with SNS use (Outhwaite & Turner, 2007; Weber, 1970).

A literature review was conducted using EBSCOhost and the ISI Web of Knowledge and by tracking citations to identify scholarly works on regulation of the internet and specifically of SNSs.

A model of regulation based on Lessig's (2006) modes of regulation was developed to take into account the subsequent development of social media and SNSs in particular. Face-to-face and telephone interviews were conducted with ten respondents representing industry and professional groups as well as regulators, academics and industry experts. The industry groups represented the interests of advertisers and SNS providers. The user perspective was represented by CILIP, and, to some extent, the Information Commissioner's Office (ICO). Respondents were asked to identify what they thought were the key issues that needed to be addressed in regulating access to personal data and their views on existing approaches to regulation. The interviews were recorded, transcribed and sent to the interviewees for checking and permission to quote. They were analysed using NVivo10 to code responses and identify emergent themes. See Appendix A for a list of the respondents and the questions asked during the semi-structured interviews. Some of the questions were directed at specific groups. The following topics were explored:

- Attitudes to risk associated with social networks, usage of social media and view on effectiveness of different types of regulation of access to personal data.
- View of current regulatory measures, with a specific focus on legislation.
- View of regulators and what they perceive to be the challenges for future regulation of access to personal data.

3. Theory

3.1. Definition of regulation

Baldwin, Cave and Lodge's (2012, pp. 2–3) definition of regulation is significant in acknowledging that it goes beyond "control exercised by a public agency over activities that are valued by a community". In one of their definitions they state:

> . . .that regulation may be carried out not merely by state institutions but by a host of other bodies, including corporations, self-regulators, professional or trade bodies, and voluntary organizations. [Regulation can be seen:]
>
> As a specific set of commands . . .
>
> As deliberate state influence . . .
>
> As all forms of social or economic influence . . .

3.2. What is being regulated?

Regulation can be viewed in terms of who is being regulated. For instance, is it the industry, their agents, or the consumers that are being regulated? The Data Protection Act 1998 focuses on the responsibilities of the data controller who can in some cases be seen as representing the SNS provider. Part of the problem arises in the definition of data controller, whether it is the user who puts up a personal profile on an SNS or the service provider (Bond, 2010).

It could also be argued that activities are being regulated rather than individuals and organisations (Baldwin et al., 2012, pp. 2–3). For instance, exchange and use of personal data could be subject to self-regulation (in privacy policies), legislation (as with the Data Protection Act 1998) or by code (as with data encryption to protect against unauthorised access to personal data).

3.3. Who are the players?

In order to understand how personal data is used in the context of SNSs, it is necessary to identify the players or agents involved in gathering, distributing and processing that data. Fig. 1 shows how personal data and advertising data flows between the different agents.

Users and their contacts (other users) are grouped together as the advertisers may not necessarily distinguish between them. Users provide personal data to their SNS provider via an ISP (Internet Service Provider). The ISP is included because as an agent it may be subject to regulation or to legal action by other agents. The SNS provider may make personal data available to associates and affiliates or to advertisers, who may be affiliated organisations or third parties. Previous studies have shown that affiliates can number in the hundreds or even thousands, depending on what definition of affiliate is used. An investigation of the top 50 internet services showed that some providers were part of groups with up to 2300 subsidiaries (Gomez, Pinnick, & Soltani, 2009).

Personal data is also relayed to other users as an activity log ('X has just updated their profile', or 'X has just made friends with Y'), either directly or via groups that they have in common.

The advertisers then push tailored advertisements to targeted users. In doing so they may use tracking technologies to monitor internet behaviour and to build up profiles of individual users. This can be used with a registration system or login to a service provided by the advertising company to create identifiable (i.e. not anonymised) personal data.