A Regulatory Model for Personal Data on Social Networking Services in the UK

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.

Keywords

Regulation; data protection; social networks; privacy

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).

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 Baldwin, Cave and Lodge 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. Figure 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 2,300 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.

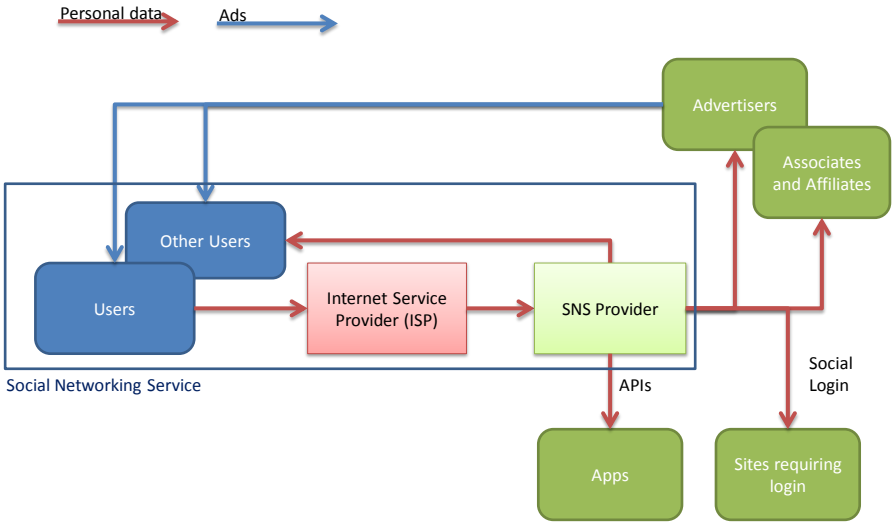

FIGURE 1 - RELATIONSHIP BETWEEN DIFFERENT AGENTS IN AN SNS

3.4 Lessig's Model of Internet Regulation

Reidenberg (1998) in his model of regulation identified the following characteristics of internet regulation:

> Lex Informatica has three sets of characteristics that are particularly valuable for establishing information policy and rule-making in an Information Society. First, technological rules do not rely on national borders. Second, Lex Informatica allows easy customization of rules with a variety of technical mechanisms. Finally, technological rules may also benefit from built-in self-enforcement and compliance-monitoring capabilities.

This led to the development of a new model of regulation that, while acknowledging the importance of statutory legislation based on Law, considers other modes of regulation namely: Norms, Market and Code (Lessig, 2006) shown in Figure 2.

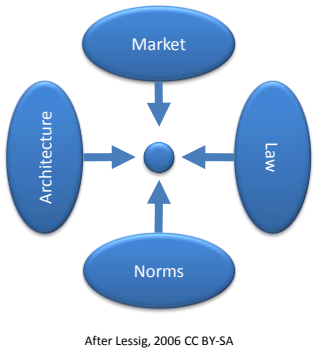

FIGURE 2 - LESSIG'S MODALITIES OF INTERNET REGULATION

Although Lessig's model has become a major reference point of analysis of different regulatory modes, other technology commentators such as Schmidt and Cohen (2013, p. 66) have described alternatives based on: corporate, legal, societal and personal responses to privacy and security needs. Each of Lessig's regulatory modes is considered in turn before a new model is proposed.

3.4.1 Law

In the UK the Data Protection Act 1998 is the main focus for statutory regulation of access to personal data. This in turn is based on the EU's Data Protection Directive (95/46/EC), which at the time of writing was due to be superseded by the General Data Protection Regulation in 2018. It is also dependent on: the Human Rights Act 1998, which enshrines the right to privacy (Figure 3); the Communications Act 2003, which regulates some aspects of data communications via the internet; and the Consumer Protection Act 1987, which establishes a self-regulating framework for the advertising industry and affects the digital advertising companies that operate in association with SNSs.

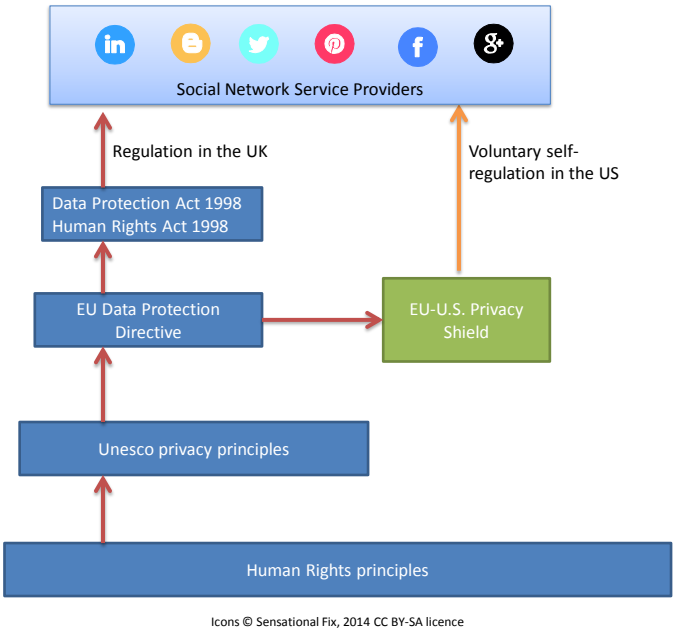

FIGURE 3 - LEGISLATIVE REGULATION IN THE UK

Lessig (2006) does not make the distinction between law and self-regulation. Even when considering legislative frameworks such as the Data Protection Act or advertising and consumer law in the UK, it is difficult to avoid self-regulation as a major component of the regulatory landscape. It also does not take account of the self-imposed commitments that SNS providers make in their privacy policies and terms and conditions of service. It could be argued that privacy policies are a type of 'code' in that they reflect the architecture of a system, however they are also an agreement between user and provider, and may be partially covered by contract law.

3.4.2 Norms

Lessig (2006) describes situations where users contravene accepted behaviour standards and are ostracised online. Users' behaviour and expectations can serve as a powerful regulatory force. This can be applied to SNS and specifically to regulation of access to personal data on SNSs. An earlier survey of LIS professionals in the UK suggested that users should have some responsibility for their own online safety (Haynes & Robinson, 2015). This is a theme that has also been picked up by the Information Commissioner's Office (ICO, 2015). Reports in the press indicated that users' expectations have a powerful effect on SNS providers. Cases such as the Facebook beacon device led to a strong reaction from users that resulted in its withdrawal because of its intrusive nature (Story & Stone, 2007). The feature automatically tracked purchases made online and effectively publicised this information. Boyd (2010) also suggests that norms operate within groups of connected individuals and that certain types of personal information are not revealed beyond the group. Wider social norms about abuse on social media have been covered prominently in the press and this suggests that there are implied standards of acceptable behaviour which when contravened elicit a strong response beyond that of the law (BBC News, 2013b).

All this points to the idea that social norms are an important factor in regulating SNSs (Rodrigues, 2010, p. 238). The effects of individual behaviour may be governed by collectively-held views of acceptable behaviour, but is only noticed at a market level when large numbers of users respond to breaches of norms:

> *Similarly, the power of individual reputation and online social norms can go a long way towards preventing the abuse of personal information among users of social-networking sites.*

Rodrigues goes on to highlight the importance of regulating the market to counter the natural monopolies that networks tend to create. He advocates lowering switching costs so that users are not penalised for transferring their accounts to alternative social networking sites. This is one of the new provisions in the GDPR (European Council, 2016).

3.4.3 Architecture or 'Code'

The way in which systems are designed and the options presented to users are an expression of 'code'. This is about the system's architecture and the way in which it controls access to personal data. At the first level is the amount of personal data gathered by SNSs. This varies significantly – SNSs such as Facebook and LinkedIn offer the opportunity to share very detailed personal information whereas services such as Twitter work on the basis of a minimal profile (up to 160

characters long). The second consideration is what is the minimum amount of personal data required for users to register with an SNS and, supplementary to this, whether real names or aliases are acceptable. This has led to controversy where networks such as Google+ have tried to impose the 'real names' requirements on users or where Facebook initially refused to accept preferred names for transvestites or transitioning transsexuals (Boyd, 2012; Lee, 2014). At the third level is the range of privacy options or settings offered by SNSs.

Lessig (2006) deals with technical architecture as an instrument of regulation. This is an approach that has been taken up by a number of regulatory authorities, initially in Canada and latterly in the UK and the EU as 'privacy by design' (Cavoukian, 2012; Information Commissioner's Office, 2008; Rubinstein & Good, 2013). Code also includes other technology based solutions for managing user identities online or for blocking ads and cookies so that online behaviour is not actively tracked by someone else.

Lessig's (2006) model of 'Code' can be extended to include the architecture of the networks and communications services as well as the electronic ecosystem within which they exist. This means that technology-based privacy and identity protection software as well as anti-spyware software are part of regulation by code. As well as the SNSs themselves, there are independent solutions that are available as add-ins to browsers, for instance, to supress cookies and to isolate Trojans and other software designed to capture sensitive data such as passwords and account details. This wider view of code as a regulatory instrument is important when considering the different agents involved.

3.4.4 Markets

Leading regulatory experts have a lot to say about regulation of market, but little is said about the use of markets to regulate an industry (Baldwin et al., 2012). Market effects are recognised, but the emphasis of regulatory bodies is to introduce rules that make the markets operate in a way that the regulators consider desirable.

The growth of internet communities and interactions has allowed the effective development of market-driven regulation. This can be seen in social pressure on providers to comply with market expectations. For instance, changes in the Facebook privacy settings without full consultation with users led to an outcry and pressure to retract (BBC News, 2011). This may be because of the implicit threat that legislators may respond with new regulations to address the concerns of their voters. Lessig's (2006) treatment of the market can be seen as a manifestation of user norms or as a response to legislation. If norms, then where a sufficient number of users feel strongly about a service and they respond, they operate as a market.

4 Results

The interview respondents provided information about their perceptions of regulation of access to personal data on SNSs. The Lessig model was used as the framework for identifying regulatory activity. This was done in semi-structured interviews (see Appendix A).

4.1 Regulatory Effectiveness

4.1.1 Views about Data Protection Legislation

There was a degree of support for the data protection principles in the Data Protection Act 1998 by respondents, because it sets a standard. The application of the eight data protection principles is seen as a flexible and appropriate way of protecting personal data:

> *Interestingly the* […] *key principles have proved relatively flexible and when combined with the Privacy and Electronic Communications Regulation (PECR) have created an environment in the UK where people are very comfortable.*
>
> Chris Combemale, DMA
>
> *I think the principles are valid now. There is obviously a debate about 'the internet has moved on and we didn't have Facebook in 1998 so therefore we need to reform things', but the principles of the DPA exist well and good now.*
>
> Nick Stringer, IABUK

By setting a standard for good handling of personal data, the DPA is seen as being effective. It affects the behaviour of companies that use or collect personal data and helps them to make their privacy policies more transparent:

> *They probably have quite an effective deterrent effect for any legitimate business.*
>
> Toby Stevens, Enterprise Privacy Group
>
> *I guess that because the kind of providers we are working with, who are tending to look at it* [tScheme] *as a mainstream business (BT, the Post Office or the banks), they tend to have a healthy respect for the Data Protection Act and the Information Commissioner's Office and therefore go out of their way almost to do things in a way that they believe is correct.*
>
> Richard Trevorah, tScheme

A good test of its effectiveness is to compare the situation with regions where there is no equivalent of Europe's data protection legislation:

> *However what I always compare this to is the counter-factual, which is the US. So a system where you have a total absence of rules governing the private sector and there you can see the effect the EU rules are actually having an impact in practice insofar as there is a minimum non-negotiable level of protection available for individuals, and companies will respect that.*

Orla Lynskey, LSE

4.1.2 Self-Regulation

There was general support for self-regulation, not only from the digital advertising industry but also from the professional bodies:

> *…there is a lot of feeling that self-regulation and adverse publicity is stronger way of enforcing people's privacy than over-regulation which can clearly affect competitiveness.*
>
> Peter Harris, BCS

The Direct Marketing Association thought that self-regulation of the advertising industry works well in comparison with self-regulation of the press, for instance:

> *In marketing and advertising it works very well. The ASA has been particularly effective and when they announce their adjudication that people have over-stepped the mark, it tends to be quite well respected.*
>
> Chris Combemale, DMA

Self-regulation was also seen as a preferable alternative to statutory regulation. For instance, a representative of the cryptographic industry has made the following case:

> *This is a new industry and it will kill the industry if you get too heavy-handed, and we don't quite know where the market is going. 'Why don't you work with us to come up with best practice processes and we, the industry, will self-regulate according to those standards. If you're happy those standards are appropriate, it should be good enough'. That was basically the initial remit of tScheme as an industry body to police the self-regulation.*
>
> Richard Trevorah, tScheme

Toby Stevens of the Enterprise Privacy Group suggested that self-regulation needs to be very focused, with clearly-defined regulatory mechanisms to be effective. He went on to suggest that a bond paid by members of the industry would act as a way of rapidly responding to complaints and penalising offending companies:

> *Self-regulation is only going to work where it is sector specific. It only means anything if all the significant players in one space say 'Yeah, we'll sign up to this'* […] *I've not seen any evidence of a self-regulation mechanism that has teeth. An effective self-regulation mechanism would be identity assurance. For example, you have to deposit funds, a bond, like the travel industry, so that when there is a failure,*

the regulator can dip into that deposit to fix things. […] *Without that sort of mechanism I don't think self-regulation can be meaningful.*

The social network providers also regulate the way in which brands use personal data they have downloaded via APIs by applying contract law:

Each of the brands that we engage with has to have a contractual arrangement with those network service providers. It's basically the social networks protecting (in their language) their users' data. […] *For example, Facebook will happily let you have access to the data on the customers that they have in the social network because they have published a bunch more* [profiles] *than anyone else. You get 52 different elements of information on an individual from postings. But if you're going to use that information for advertising, they throw a flag on the play and they won't let you do it.*

Russell Loarridge, Janrain

A key aspect of self-regulation is the application of privacy policies and terms of service provided by the SNSs for their users. Having a policy that makes clear to users their rights and obligations is important. Ultimately they are enforced by contract law, although there may be some dispute about which jurisdiction holds sway.

Some have also started responding to the need for greater transparency so that users can make informed decisions about how their personal data is used:

I also think we need to look at how social media systems work, especially how they change their terms and conditions. They can change these quite significantly and quite often. This can be very confusing for people. They could do more to give people clearer choices at the appropriate times and better control mechanisms thorough nice clear simple yes-no choices. I think people sometimes feel overwhelmed and that they don't really control who sees their information and what happens to it. Information-based firms need to do more to calm that anxiety, through being transparent, offering choices and using information in line with their users' expectations.

Iain Bourne, ICO

You have the fundamental starting point, data protection law is based on consent. I would argue that would also mean informed and meaningful consent and that you don't get informed and meaningful consent from asking someone to sign a privacy

policy that is longer than the theory of relativity, that was written by lawyers for lawyers.

Nick Pickles, Bigbrotherwatch

Many SNS providers are US-based and have relied on the EU-US Safe Harbor self-regulatory arrangements to demonstrate compliance with the Data Protection Directive. The Safe Harbor arrangement was ruled invalid by the European Court of Justice in 2015, although service providers still have access to other methods (such as contracts and robust procedures) to demonstrate compliance with the legislation in Europe (Haynes, 2015a). The introduction of the EU-U.S. Privacy Shield in 2016 to some extent replaces the Safe Harbor arrangements (European Commission, 2016).

4.1.3 Technology and Design

Technology plays an increasingly important role in regulating access to personal data on social media. Cookie blocking software can be used as apps or add-ins on many browsers to identify and highlight cookies and allow users to block them selectively or comprehensively. The Ghostery software is one example of this. The European Interactive Digital Advertising Alliance (EDAA) also offers a utility via the www.youronlinechoices.eu website to block cookies.

Ad blocking software can also be installed to prevent pop-up ads from appearing on websites. This type of software is increasingly being adopted by users, a point that was noted:

Social media users and others are slowly but surely getting more assertive and more critical in terms of how people use their information and that they do find some forms of advertising intrusive. A good example is 'beacon marketing', where your social media 'friends' are informed automatically of goods you've purchased on an e-commerce site. The fact that so many people are using ad blocking services is a bit of a worry I'd have thought, if my business model relied on advertising.

Iain Bourne, ICO

Software designed for computer security and dealing with malware also includes anti-tracking technologies that delete or suppress cookies as one of a number of security features. There are also services such as Mydex and Janrain, which provide ways of sharing personal data in a more controlled manner, so that the user has a choice about who sees what. Trust frameworks such as tScheme can be applied to such services to indicate to users that data-sharing is compliant with a stated policy.

Privacy by design is one of the elements of the Information Commissioner's Office (ICO) to improve privacy protection.

A lot of the greatest advances that have been made in privacy by design and privacy enhancement have been by the big tech firms. They don't want all that personal data sloshing around; it's expensive; it's a liability. I think it is important to realise that

they are not the 'baddies' in that sense, they are maybe developing the cures for some of these problems.

Iain Bourne, ICO

This is an approach that is supported by the industry:

The nice route with identity assurance is using federation and privacy by design principles. That type of approach is able to compartmentalise; it will allow you to minimise the data leakage between these domains, so that you can anonymously assert information. It moves us into an attribute rather than an identity economy. I think the solution is actually assurance rather than identity.

Toby Stevens, Enterprise Privacy Group

4.1.4 User Behaviour

Market responses and individual behaviour are both manifestations of individual attitudes about what is acceptable. In effect users regulate online advertising either by the decisions they take as individuals (for instance to determine how much personal data they will share on social media), or by the cumulative effect of their collective behaviour (using alternative services if they do not like what's going on).

The issue of user awareness has arisen in previous surveys and this is seen as one of the most effective ways of protecting users. As Guy Daines of CILIP (the Chartered Institute of Library and Information Professionals) said:

What we are really talking about here is information behaviour, in how people use information in their work and also in their personal life. It is about instilling the idea about responsible use. […] *It's about changing the culture about being careful about privacy.*

It is also about personal responsibility:

The consumers who register on these sites don't read the small print about what they are allowing the brands to do with their data.

Russell Loarridge, Janrain

From the early days of SNSs commentators were calling for greater investment in user education, specifically in response to the use of advertising beacon technology (Gray, Zeggane, & Maxwell, 2008). The collective behaviour of users can become regulation by the market, or 'mode' in Lessig's categorisation of regulatory modalities. For instance, if a significant proportion of users start to leave a service, the service may respond in a way that addresses user dissatisfaction. As one respondent put it:

> *the only reign-in on those organisations is the damage to their brand if they did something stupid*
>
> Russell Loarridge, Janrain

Research by the Future of Privacy Forum in the United States *"to assess the communication efficacy of behavioral advertising disclosures on the web"* found that disclosure statements and icons increase the comfort of active internet users when confronted with ads on third-party websites (Hastak & Culnan, 2010).

Others maintain that user behaviour is probably the best regulator:

> *It has got to a point where to what extent do they* [SNSs] *have to start deliberately showing me wrong adverts, because if they were right all the time, consumers would go 'Hang on a minute, they* ***do*** *know everything about me'. It's the 'creepy line' (phrase used by Google and the NY Times). That creepy line is probably the better regulator than either self-regulation or legal regulation.*
>
> Nick Pickles, Bigbrotherwatch

Iain Bourne of the ICO argued that regulation probably works because of the concern of SNS providers about loss of market:

> *If you look at the way that groups of social media users grouped together to campaign against changes to privacy policies, changes to practices, it's really interesting. There is evidence that some of the social networking sites* [are] *changing the way they do advertising, because of pressure from their own users…You see this more in the US I'd say but I think it will happen more in the EU as well. Maybe user power is having more influence than regulation in some areas.*
>
> Iain Bourne, ICO

5 Discussion and Conclusion

5.1 A Revised Model of Regulation of Personal Data on SNSs

Lessig (2006) has shaped the nature of the debate about regulation of the internet, firstly by conceptualising the idea that the architecture of systems (Code) is one way of regulating, and by identifying four modes of regulation. Since his initial work in the early days of the Internet and again in the early years of this century at the point when social media started to take off, many new services have been launched and mobile apps have become pervasive. His model is largely applicable to online social networking services and provided a useful starting point for an investigation of the nature of regulation of access to personal data on online SNSs (Haynes, 2015b). Revisiting the model through an investigation of the literature, surveys of data protection professionals and interviews with key informants has shown that self-regulation has become a very

important strand of the regulatory landscape. Lessig makes very little reference to self-regulation in his book, Code 2.0 and when he does it is applied to users regulating their behaviour online (an aspect of norms) and to self-governance of the internet (Lessig, 2006, pp. 97, 394). This first interpretation is supported by Cooke (2004, p. 36) who suggests that self-regulation is a form of 'norm-based governance'.

Earlier commentators on regulation have identified self-regulation as a significant method of regulation, even while pointing out its limitations (Cannataci & Bonnici, 2003; Spinello, 2002). Park (2014) provides a more detailed analysis of self-regulation based on a review of 398 commercial websites in the United States. Although he sees it as insufficient for ensuring data protection on its own, he recognises it as a significant form of regulation. Self-regulation by an industry can apply if there are suitable sanctions for non-compliance such as expulsion from a group with consequent loss of credibility and market share. Park's argument is that there is no evidence that companies which publish privacy policies (an expression of self-regulation) are any better at protecting privacy than those that do not.

Surrogate regulation or co-regulation, where the responsibility for regulating a professional group or industry is vested in a professional or trade body, can also be effective (Hans-Bredow Institut, 2006). Membership of the body becomes a condition of being allowed to trade. This can be seen with the established professions and some sectors in the UK (such as civil engineers, lawyers, doctors and architects). This approach takes the burden of regulation away from the state and the costs of regulation are borne by the regulated individuals or industry.

In this study representatives industry bodies such as the Direct Marketing Association as well as the regulator, the ICO, and the campaign group, Bigbrotherwatch recognised self-regulation as a regulatory method, although they differed on how effective it was as a way of protecting users' personal data on SNSs.

Lessig acknowledges the interdependence of different regulatory modes. For instance, markets regulate largely by availability and price and this in turn is affected by social norms and by the legislative environment. As such regulation by the market, as Lessig describes it, is an expression of the activity of suppliers. If pricing is the main mechanism by which markets operate, the model breaks down for SNSs where the monetary value and cost to consumers of services is difficult to determine. The social media services tend to be free at the point of delivery and the costs are carried by advertisers. This causes a divorce between the interests of users and the drivers for the market. If the services are indirectly paid for by the industry, the market response will be determined ultimately by industry rather than users. An alternative model is required to reflect the wider interests of users. The proposed new model, acknowledges the importance of the market as a regulator but sees it as an expression of social norms. 'Norms' covers both individual behaviour and attitudes and collective behaviour as seen in the market responses to services. The behaviour of suppliers is covered in both self-regulation and code – the way in which services are delivered. Indeed Mitchell (1996, pp. 111, 147) talks about code and norms, but does not include markets in his commentary on regulation of cyberspace.

Another problem with the concept of regulation by the market, is that the market is the object of regulation, not the method.

Regulation by the state is the starting point for an analysis of regulation (Baldwin et al., 2012). A preliminary survey of users and data protection officers suggested that there is some scepticism about the effectiveness of the Data Protection Act as a means of regulating access to personal data on social networks (Haynes, 2011). This was borne out by interviews with regulators and industry experts reported here. Although some respondents found it to be effective, many considered that the legislation alone was insufficient. Several respondents saw other modes such as self-regulation, user education, and technology as important elements in the protection of personal data. Nevertheless legislation is a key element in any model of regulation of SNSs.

Figure 4 shows the proposed model of regulation of access to personal data on SNSs, compring four modes of regulation:

1. Legislation
2. Self-regulation
3. Code
4. Norms

This proposed model of regulation builds on Lessig's (2006) idea that there are four modalities for regulating the Internet. It attempts to cover a major omission in the lack of a category for self-regulation. The model also makes a stronger connection between 'Norms' and collective user behaviour which Lessig treats separately as 'Markets'. This new model also recognises that legislation affects self-regulation which is usually manifest in privacy policies and in industry codes of practice. These codes of practice may themselves by governed by legislation or they may be industry-driven. The way in which enterprises design and deliver SNSs (Code) is itself a form of self-regulation.

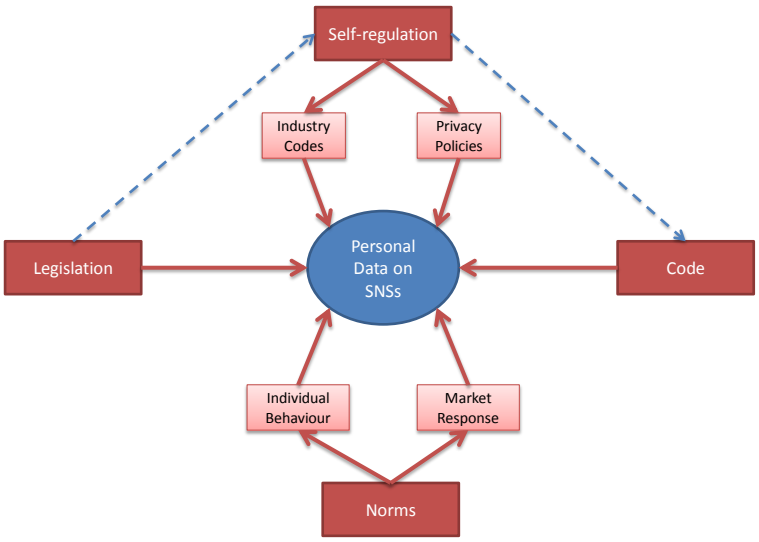

FIGURE 4 - REGULATING ACCESS TO PERSONAL DATA - NEW MODEL

5.2 Significance

This research set out to explore the relationship between different modes of regulation of access to personal data and to develop a model that reflects the current regulatory landscape. It highlighted the importance of self-regulation. In the context of 'light-touch' government this is a theme that very topical. A realistic model of regulation is required in order to be able to evaluate regulatory effectiveness. The absence of self-regulation in Lessig's original model of Internet regulation was a major omission.

The introduction of the General Data Protection Regulation (GDPR) has also highlighted regulatory issues with the emphasis on individual firms to police their own activity. This is particularly the case with the self-reporting of data breaches, although likely to be backed up with stiff penalties for organisations that do not follow the regulation. A number of commentators have highlighted risk based regulation as characteristic of the European regulatory landscape (Haythornthwaite, 2006; Hutter, 2005; Swedlow, Kall, Zhou, Hammitt, & Wiener, 2009). This is something that seems to be borne out from the wording of the GDPR which refers throughout to "risk to the rights and freedoms of natural persons" (European Council, 2016). A regulatory model based on risk analysis will help to provide an informed view about the effectiveness of the GDPR when it is implemented across the European Union in 2018.

Information governance is another important theme that has developed over recent years. Many organisations, increasingly aware of the threats that there are to their information assets, are developing comprehensive information governance frameworks. These include measures for information security and risk management and depend on clear lines of responsibility and accountability. The widespread use of social media in the workplace has introduced new risks, which need to be managed. An understanding of regulation will help to inform the debate about

information governance and raise awareness of the approaches that are available to information managers.

5.3 Further work

The proposed regulatory model described here is based on an analysis of regulation of access to personal data rather than the wider 'internet regulation' model proposed by Lessig. The model is in effect a hypothesis built up by considering personal risks associated with use of online social networking services and considering the regulatory mechanisms available.

Research of this type has limitations and there is scope for further development and refinement of this regulatory model. During this investigation it was not possible to secure interviews with representatives of the SNS providers. The digital advertising bodies were used as surrogates for the SNS providers and further work is needed to obtain the views of SNS providers directly. Future research could focus on the views of SNS providers about the proposed model of regulation and to find out whether it reflects their perception of the regulatory pressures that they experience.

The next step is to validate the model by consulting different groups of stakeholders: users, SNS providers, regulators, advertisers. In order to validate the hypothesis using a 'grounded theory' approach, it would be important not to consult the same people that were consulted during the hypothesis construction (Charmaz, 2006; Glaser & Strauss, 1967). This presents a potential problem in the case of the regulators, as there is only one data protection regulator in the UK. As a representative of the ICO was interviewed during the development of this model, it would be necessary either to interview a different person from the ICO, or to consult an official from the European Data Protection Supervisor's office instead.

The model has been developed to reflect the regulatory landscape that applies to SNSs used in the UK and to some extent in Europe. However it could be tested for applicability in other markets such as the United States, where there is a very different regulatory framework. Recent developments in China, Russia and Brazil to protect citizens' personal data (especially against transfer overseas) suggests a growing perception that a legislative approach to information privacy is required (Chen & Sun, 2014; Determann, Bekeschenko, Perevalov, & Wood, 2015; Medeiros & Bygrave, 2015). To some extent this may be a response to Snowden's NSA revelations, and it would be worth exploring this further (Greenwald, 2013; Haynes, 2015a).

An alternative line of investigation would be to consider risks from a corporate perspective. For instance, what are the risks faced by organisations that use social media for promotional and campaigning activities? Under the Defamation Act 2013 website hosts are responsible for anonymously-posted defamatory statements and this changes the regulatory landscape. Some examples of corporate risks associated with social media are already under investigation elsewhere (Haynes, 2016).

Finally, this research plugs into a wider consideration of regulation on the internet. Further work could be undertaking to consider copyright, intellectual property and censorship issues in addition to the privacy issues covered here.

Legislation Cited

Communications Act, UK 2003

Consumer Protection Act, UK 1987

Data Protection Act, UK 1998

Decision on Strengthening the Protection of Online Information (Online Information Decision), Standing Committee of the National People's Congress, People's Republic of China, 2012

Defamation Act, UK 2013

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) *Official Journal L 281*, 23.11.1995, pp.31-50

Federal Law No. 242-FZ dated July 21, 2014 "On Introducing Amendments to Certain Legislative Acts of the Russian Federation with regard to Personal Data Processing in Information and Telecommunications Networks."

General Data Protection Regulation. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM (2012) 11 final, 2012/0011 (COD), Brussels, 25 January 2012

Human Rights Act, UK 1998

Marco Civil da Internet 2014 (Lei No. 12,965), Brazil

References

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

BBC News. (2011). Facebook U-turns on Phone and Address Data Sharing. BBC. Retrieved September 16, 2012, from http://www.bbc.co.uk/news/technology-12214628

BBC News. (2013a). Arrests Made in Brian Holloway's Trashed House Party. *BBC News*. Retrieved February 11, 2014, from http://www.bbc.co.uk/news/world-us-canada-24293414

BBC News. (2013b). Professor Mary Beard: "Why I Shamed Twitter Troll." Retrieved November 19, 2014, from http://www.bbc.co.uk/news/uk-23502792

Blake, J. (2015). Ask.fm owners "considered shutting down" social network. *BBC Newsbeat*. Retrieved April 9, 2015, from http://www.bbc.co.uk/newsbeat/31249209

Bond, R. (2010). Data Ownership in Social Networks - a very personal thing. *Privacy and Data Protection*, *11*(1), 1–5.

Boyd, D. (2010). The Future of Privacy: how privacy norms can inform regulation. In *32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 29 October 2010*. Jerusalem.

Boyd, D. (2012). The Politics of “Real Names”. *Communications of the ACM*, *55*(8), 29–31.

Butler, E. (2011). Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content. *Human Communication*, *14*(1), 39–55.

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

Cavoukian, A. (2012). Privacy by Design [Leading Edge]. *IEEE Technology and Society Magazine*, *31*(4), 18–19.

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

Chen, H., & Sun, S. (2014). What the Consumer Protection Law Means for Foreign Businesses. *China Law & Practice*, *28*(1), 43.

Christiansen, L. (2011). Personal Privacy and Internet Marketing: an impossible conflict or a marriage made in heaven? *Business Horizons*, *54*(6), 509–514.

Cooke, L. (2004). *Regulating the Internet: policy and practice with reference to the control of Internet access and content (PhD Thesis)*. Loughborough University.

Cox, C. (2014). Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosecutions and Effective Laws. *Jurimetrics: The Journal of Law, Science & Technology*, *54*(3), 277–302.

De Lima, D., & Legge, A. (2014). The European Union’s approach to online behavioural advertising: Protecting individuals or restricting business? *Computer Law & Security Review*, *30*(1), 67–74.

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

Determann, L., Bekeschenko, E., Perevalov, V., & Wood, I. (2015). Keep Russian Data in Russia and Out of Clouds? *Computer & Internet Lawyer*, *32*(6), 1–8.

European Commission. (2016). EU-U.S. Privacy Shield - Factsheet. Retrieved April 28, 2016, from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

European Council. General Data Protection Regulation (DRAFT) - 5419/16 (2016). EU.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: strategies for qualitative research*. New York: Aldine de Gruyter.

Gomez, J., Pinnick, T., & Soltani, A. (2009). *Know Privacy*. Berkeley CA: University of California Berkeley, School of Information.

Gray, T., Zeggane, T., & Maxwell, W. (2008). US and EU Authorities Review Privacy Threats on Social Networking Sites. *Entertainment Law Review*, *19*(4), 69–74.

Greenwald, G. (2013, June 6). NSA Collecting Phone Records of Millions of Verizon Customers Daily. *The Guardian*. London.

Hans-Bredow Institut. (2006). *Study on Co-Regulation Measures in the Media Sector. Final Report*. Brussels: European Commission.

Hastak, M., & Culnan, M. J. (2010). Online Behavioral Advertising “Icon” Study: summary of key results. *Future of Privacy Forum*, *25*.

Haynes, D. (2011). Social Networks in the Workplace - some data protection issues. *Free Pint*, (1 December 2011).

Haynes, D. (2015a). End of Safe Harbour isn't the End of the World – let's hope its successor is better. *The Conversation*. Retrieved October 14, 2015, from https://theconversation.com/end-of-safe-harbour-isnt-the-end-of-the-world-lets-hope-its-successor-is-better-48841

Haynes, D. (2015b). *Risk and Regulation of Access to Personal Data on Online Social Networking Services in the UK*. City University London.

Haynes, D. (2016). Risk and Social Media (DRAFT). *Business Information Review*, *(in press)*.

Haynes, D., & Robinson, L. (2015). Defining User Risk in Social Networking Services. *Aslib Journal of Information Management*, *67*(1), 94–115.

Haythornthwaite, R. (2006). *The Regulation of Risk : setting the boundaries* (Vol. 16). Bath: University of Bath.

Helft, M., & Wortham, J. (2010). Facebook Bows to Pressure over Privacy. *New York Times*. Retrieved November 13, 2014, from http://www.nytimes.com/2010/05/27/technology/27facebook.html

Hutter, B. M. (2005). *The Attractions of Risk-based Regulation: accounting for the emergence of risk ideas in regulation*. *Vol. 33*. London: LSE, Centre for Analysis of Risk and Regulation.

Hutter, B. M. (2006). Risk, Regulation and Management. In J. Taylor-Gooby, Peter; Zinn (Ed.), *Risk in Social Science* (pp. 202–227). Oxford: Oxford University Press.

ICO. (2015). Online Safety. Retrieved October 20, 2015, from https://ico.org.uk/for-the-public/online/social-networking/

Information Commissioner's Office. (2008). *Privacy by Design*. Wilmslow: ICO.

Jiow, H. J. (2013). Cyber Crime in Singapore: An Analysis of Regulation based on Lessig' s four Modalities of Constraint. *International Journal of Cyber Criminology*, *7*(1), 18–27.

Lee, D. (2014). Drag Queens in Facebook Name Row. *BBC News Online*. Retrieved February 5, 2015, from http://www.bbc.co.uk/news/technology-29175102

Lessig, L. (2006). *Code* (2nd ed.). New York; London: BasicBooks.

Litvínov, A. V. (2013). The Data Protection Directive as applied to Internet Protocol (IP) Addresses: uniting the perspective of the European Commission with the jurisprudence of Member States. *George Washington International Law Review*, *45*(3), 579–610.

Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *Zer*, *18*(35), 13–28.

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

McDonald, T. (2013). Kids + Facebook = Home Invasion? *Business 2 Community*. Retrieved October 10, 2013, from http://www.business2community.com/facebook/kids-facebook-home-invasion-0618724

Medeiros, F. A., & Bygrave, L. A. (2015). Brazil's Marco Civil da Internet: Does it live up to the hype? *Computer Law & Security Review*, *31*(1), 120–130. doi:10.1016/j.clsr.2014.12.001

Mitchell, W. J. (1996). *City of Bits: space, place, and the infobahn*. Cambridge, MA: MIT Press.

Outhwaite, W., & Turner, S. P. (Eds.). (2007). *The SAGE Handbook of Social Science Methodology*. Los Angeles CA; London: Sage Publications.

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy and Internet*, *6*(4), 360–376.

Reidenberg, J. R. (1998). Lex Informatica: the formulation of information policy rules through technology. *Texas Law Review*, *76*(3), 553–584.

Roberts, L. (2010). Facebook Status Updates are "Burglary Risk." *BBC News Online*. Retrieved July 7, 2014, from http://www.bbc.co.uk/news/uk-england-birmingham-12062331

Rodrigues, R. (2010). Privacy on Social Networks: norms, markets and natural monopoly. In S. Levmore & M. C. Nussbaum (Eds.), *The Offensive Internet* (pp. 237–256). Cambridge, MA: Harvard University Press.

Rubinstein, I. S., & Good, N. (2013). Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal*, *28*(2), 1333–1413.

Schmidt, E., & Cohen, J. (2013). *The New Digital Age. Reshaping the future of people, nations and business*. *NPQ: New Perspectives Quarterly* (Vol. 30). London: John Murray.

Scott, E. M. (2013). Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a trans-Atlantic browser-based opt-in for behavioral tracking the right solution? *Pacific McGeorge Global Business & Development Law Journal*, *26*(1), 285–313.

Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Information, Communication and Society*, *18*(1), 48–62.

Spinello, R. A. (2002). *Regulating cyberspace : the policies and technologies of control*. Westport, Conn. ; London: Quorum Books.

Staksrud, E., & Livingstone, S. (2009). Children and Online Risk: powerless victims or resourceful participants? *Information, Communication & Society*, *12*(3), 364–387.

Story, L., & Stone, B. (2007). Facebook Retreats on Online Tracking. *New York Times*. Retrieved February 4, 2015, from http://www.nytimes.com/2007/11/30/technology/30face.html

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

The Moscow Times. (2015). Russian Truck Driver Who Killed Elderly Cyclist Commits Suicide. *The Moscow Times*. Retrieved April 9, 2015, from http://www.themoscowtimes.com/news/article/518777.html

Wakefield, J. (2014). Cyberbullies: How best to tackle online abuse? *BBC News Online*. Retrieved July 7, 2014, from http://www.bbc.co.uk/news/technology-26121199

Weber, M. (1970). *From Max Weber: essays in sociology*. (H. H. Gerth & C. W. Mills, Eds.). London: Routledge & Kegan Paul.

Appendix A – Interview Questions

The following individuals were interviewed in the period March-April 2014:

Organisation	Contact name	Date	Type of interview
Bigbrotherwatch	Nick Pickles, Director	17 Apr 2014	Face-to-face
British Computer Society	Peter Harris, Chair, Information Privacy Expert Panel	3 Mar 2014	Telephone
CILIP	Guy Daines, Head of Policy	6 Mar 2014	Face-to-face
Direct Marketing Association	Chris Combemale, CEO	3 Apr 2014	Face-to-face
Enterprise Privacy Group	Toby Stevens	1 Apr 2014	Face-to-face
Information Commissioner's Office	Ian Bourne	19 Mar 2014	Face-to-face
Internet Advertising Bureau, UK	Nick Stringer, Director, Regulatory Affairs	11 Mar 2014	Face-to-face
Janrain	Russell Loarridge	8 Apr 2014	Telephone
London School of Economics	Orla Lynsky, Assistant Professor of Law	9 Apr 2014	Face-to-face
tScheme	Richard Trevorah	7 Apr 2014	Telephone

Introduction (for participants)

The purpose of this interview is to find out the views of respondents on the different ways in which access to personal data on social media is regulated in the UK. The study is part of a PhD research project exploring the relationship between personal risk and regulation of online social networking services and follows on from an online survey on risk perceptions among users.

This interview will consist of a series open questions covering:

- Current measures in place for protecting personal data on online social networking services
- Your views on the effectiveness of current measures
- Specific issues and problems associated with personal data
- Potential future measures, including proposed legislation

The interview is expected to last between 45 minutes and one hour in total. It will be recorded (audio recording) so that the notes can be accurately transcribed and analysed. We may need to contact you subsequently for clarification of any points arising from the interview. We will only do this with your permission.

This study is subject to the approval of the City University London, School of Informatics Research Ethics Committee. It is one of the University's requirements that all survey respondents should have consented to participation in the study before participating. [Make sure that the respondent has had a chance to read the participant guidelines and has signed the consent form before beginning the interview.]

Questions

Preliminaries

Interview with [Name] of [Organisation] on [Date]

Background about your regulatory role

Can you please explain your organisation's role in regulating access to personal data?

[Prompts]

- Code of practice – Training – Awareness
- Promotion of good practice
- Target audiences
- Written guidelines
- Current or due for update?

Views on risk

What do you think are the main risks that users are exposed to when they use online social networking services? [Prompt with a list of risks identified in previous surveys, if necessary]

Do you think that regulation reduces risks to individual users of social networks? In what ways?

Regulatory measures in place

What other measures that you are aware of are in place to protect social media users against misuse of their personal data?

[Service providers and advertisers] What measures does your organisation/industry take (have in place) to protect users against misuse of their data?

[SNS Providers and Advertisers] Do you subscribe to an industry code of practice?

- Who issues the code of practice? Do you have a contact?
- Do you have a copy of the code of practice that I can have?

Views on legislation

What is your view of the current Data Protection Act as a way of protecting people against misuse of personal data that they put up on online Social networking services?

- Do you think that the current legislation is effective?
- Do you think that it could be improved? If so, in what ways?

In your view, is this area over- or under-regulated? Why?

Are you familiar with the proposed European Data Protection Regulation currently under discussion?

- Do you think this is an improvement on the current legislation? Why?

Regulatory effectiveness

[Regulators and self-regulators] How do you assess regulatory effectiveness?

[Regulators and self-regulators] Do you think that risk could be used as a way of measuring regulatory effectiveness?

Responsibility for regulation

Who should have primary responsibility for protecting users against misuse of personal data that they put up on SNS profiles? [Prompt: users themselves, industry bodies, system designers, SNS providers, the government, others?]

Why?

Follow-up

May we quote you?

May we attribute any interview comments to you?

May we identify your organisation?

May we approach you again if any points need clarifying or if we need to follow up any aspect of this interview?

Can you suggest other people or organisations that you think should be consulted as part of this study? – Can I mention your name?

Thank you