Regulating the Future

David Haynes

Department of Information Science, City University London, Northampton Square, London EC1V 0HB. Email: david.haynes.1@city.ac.uk

Abstract

Research into the regulation of social networking services (SNSs) reveals several possible approaches based on Lessig's model of Law, Mode, Market and Code as means of regulating the Internet. This paper explores some of the issues that arise from a detailed examination of national legislation in the UK coupled with a survey of user and employer perceptions of risk associated with personal data on SNSs. The paper suggests that a mixed mode of regulation is probably most appropriate, but envisages that politicians of the future will continue to be obsessed with trying to regulate the technology rather than people's behaviour.

Keywords: *Regulation; Internet; Social Networking Services; Legislation; Regulatory modes; Risk; Markets; Future.*

Introduction

Looking ahead 10 years, as the British Library did in 1989-90 to the impossibly distant future of the year 2000, a number of interesting predictions were made (Martyn 1990). CaTV was seen as the main medium for transmission of information, education and entertainment. X-Terminals would provide online access to databases and there was no Internet. Aslib's even more ambitious and wide-ranging future scan encompassed the present (just before 2000) to 100,000 years hence (Scammell 1999).

If we were to look at the accuracy of these predictions and the number that 'survive' future scrutiny one could develop a theory of 'half-lives' – i.e. after a certain period of time half the predictions are no longer true, as has been done for the persistence of facts (Arbesman 2012). If we were to turn this around and say that after 10 years 60% of the predictions made are true (a generous estimate probably), then after 50 years only about 8% of the predictions originally made would still be true. Making accurate predictions so far ahead in time is unrealistic, but may serve a purpose in helping us to shape the future.

The research reported here is about regulation and the ways in which this affects the delivery of information services (Haynes 2012). The focus is specifically on privacy and personal data and the tension between tailoring services to suit individuals and the risks to which users are exposed when they use online social networking services (SNSs) such as Facebook and LinkedIn. Clearly there is a problem when users enter into a relationship with an SNS provider, who then makes their personal details available to wider audiences. When a user signs up there is an implicit (actually explicit, if the EULAs are examined carefully) contract that in return for the 'free' services provided by the SNS, the service provider can use that personal data to generate income. For instance they can sell the data to advertisers and business partners. For a modest fee ($30,000 a year) you can buy access to the personal profiles of members of LinkedIn. Facebook provides a variety of services for companies who want to reach large numbers of customers. Cookies improve data quality but also invade the privacy of users.

In the news today we see the manifest frustration of politicians trying to regulate Google and Amazon so that, for instance, they pay their taxes, and (less good) so that they give up details of their customers to the security services. This reveals one of the major limitations of national regulation. It can be said that the Internet is a place (boyd 2008; Zittrain 2008; Lessig 2006). We even have seen a declaration of independence (Barlow 1996). In 50 years' time the Internet or its replacement may well have sovereignty and apply its own regulations to those who use it. The big regulatory issues will not go away – freedom of access to information, censorship, security, protecting individual rights such as privacy, protecting intellectual property rights – but they may be handled differently to the predominantly legislative approach we see today.

How do we regulate the Internet?

So we are faced with the challenge of regulating something that operates beyond national boundaries. This research sets out to look at the ways in which access to personal data on SNSs is regulated in the UK and to explore the role of risk. The early work consisted of a qualitative survey of users to get an understanding of the scope and range of risks that they perceive from use of SNSs such as Facebook, LinkedIn and Twitter. Lessig defined four modes of regulation of the Internet: Law, Mode, Market and Code (Lessig 2006). These four modes have been adapted to the regulation of SNSs and form the subject of this study: Law, Self-regulation, Code and User education.

Law

In looking at law, the research sets out to address the following questions: What are the rules? How did the rules come about? What is their effect? What can be changed? The last question led to speculation about possible futures and the intention is that this research should be part of the debate around future regulation of the information world. The research focused primarily on the Data Protection Act (Anon 1998).

The most obvious problem is one of enforcement – not only because most social media services are based outside Europe and often do not see European laws as being relevant, but also because the authorities themselves think that regulating SNSs is beyond their scope.

Self-regulation and co-regulation

Self-regulation is emerging as a real alternative to pure legislation. The development of privacy policies and the response of providers to the threat of legislation has resulted in changes to the behaviour of services such as Facebook and Google+. There are already self-regulatory regimes in place, such as Safe Harbor in the United States. However without adequate scrutiny, self-regulation lends itself to abuse or neglect (Connolly 2008).

One concern with current legislative development is the concept of the 'right to be forgotten' (Anon 2010a). In trying to deal with the persistence of personal data, the EU wants to provide a mechanism that allows individual users to have personal data removed from the internet. This fails to address the very real problem of control. Once something appears on an SNS, it can never truly be controlled: other users may have downloaded and stored the funny pictures; different file servers (distributed to ensure robustness of service) will have back-up copies of your profile; and the fact that data has been transmitted means that it will be stored on intermediate servers. Some of that traffic is likely to have been transmitted by satellite and with data leakage, you would need to be able to outrun and then intercept the carrier waves as they rush out into space. This is an example of a political response to technology that is poorly understood.

Within the European Union a co-regulatory approach is emerging, where a trade association of industry regulates its members, but uses guidelines based on legislation. Some commentators suggest that co-regulation will be used more widely rather that regulation purely by the state, or self-regulation (Woods 2012; Baldwin et al. 2012).

Code

Lessig suggests that the way in which information systems are designed and coded (i.e. the software) regulates their use. For example, password access, encryption and default privacy settings are all examples of how existing SNSs regulate access to personal data. In the future this might develop to allow automated intervention by powerful and intelligent agents originating from providers, consumers and governments, in a similar way to anti-malware software and services today.

User education

Regulators such as the Information Commissioner see user education as being an important component in managing access to personal data. As users become more familiar with the digital landscape they will develop a 'traffic sense' and instinctively know what constitutes safe and risky behaviour.

Conclusion

What is the best way forward? A preliminary survey of users and employers conducted in 2011 suggested that a mixed approach to regulation is better than legislation alone (Haynes 2012). In its recent

deliberations about the future of the data Protection Directive, the European Commission has itself signalled the following future areas of action (Anon 2010b):

- Notification of breaches
- Data minimisation (such as the 'right to be forgotten')
- Consent
- Measures for self-regulation and other non-legislative approaches
- Harmonisation of rules and processes

It is impossible to know the social, economic and technological context that the regulations will operate in, in 50 years' time. We have experienced a paradigm shift with the application of information technology and development of the Internet to our work and our daily lives (Kuhn 1970). Based on pointers from my research, here is a vision of the information world in 2063:

- Globalisation of information services – services will be beyond the jurisdiction of nation-states and are more likely to be under the control of corporations and informal networks of individuals
- International agencies have policing and enforcement powers for the digital world
- Competing intelligent agents automatically regulating digital systems – agents deployed by service providers, governments, corporate users and individuals to regulate which data (including personal data) is available to what system
- More self-regulation by service providers – with more sophisticated users and greater choice there will be greater pressure on service providers to offer stronger protections to users
- Tools to enhance market responses and regulate the service providers –e.g. user feedback used to block or restrict access to items or services
- Silver suited politicians will still continue to try and regulate the technology rather than the consequences of its misuse

References

Anon, 2010a. *A comprehensive approach on personal data protection in the European Union*, European Commission.

Anon, 1998. *Data Protection Act*, United Kingdom.

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

Arbesman, S., 2012. The half-life of facts : why everything we know has an expiration date,

Baldwin, R., Cave, M. & Lodge, M. eds., 2012. *Understanding regulation : theory, strategy, and practice*, Oxford: Oxford University Press.

Barlow, J., 1996. A declaration of the independence of cyberspace.

boyd, D., 2008. A Response to Christine Hine A. N. Markham & N. K. Baym, eds. *Internet inquiry: Conversations about method.*, pp.26–32.

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

Haynes, D., 2012. Access to Personal Data in Social Networks : measuring the effectiveness of approaches to regulation (Transfer report). City University London.

Kuhn, T.S., 1970. The structure of scientific revolutions. Second edition, enlarged., [Chicago ;: University of Chicago Press,.

Lessig, L., 2006. *Code : version 2.0 ; Lawrence Lessig*, New York; London: BasicBooks; Perseus Running, distributor.

Martyn, J., 1990. *Information UK 2000*, London ;;New York: Bowker-Saur.

Scammell, A., 1999. I in the sky : visions of the information future, London :: Aslib/IMI,.

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

Zittrain, J., 2008. The future of the Internet :and how to stop it, London: Allen Lane.

Author biography

David Haynes is a PhD Student at City University London. Since gaining an MSc in Information Science from City University some years ago, he has had a varied career as an information scientist, project manager and management consultant. He returned to City University in 2010 to investigate the relationship between risk, regulation and access to personal information on the Internet. He also teaches at City University and at the Centre for Archives and Information Studies (CAIS) at the University of Dundee.