Protection of Children in Social Network Sites in Malaysia and Spain: A Comparative Legal Analysis

JAWAHITHA SARABDEEN
Assistant Professor
Faculty of Business and Management
University of Wollongong in Dubai
UNITED ARAB EMIRATES
jawahithasarabdeen@uowdubai.ac.ae http://www.uowdubai.ac.ae

MARIA DE-MIGUEL-MOLINA
Assistant Professor
Management Department
Universidad Politécnica de Valencia
SPAIN
mademi@omp.upv.es http://www.upv.es

Abstract: - The open nature of the social network sites facilitates many opportunities for children but also makes them vulnerable for abuses from various parties. Obscenity, hate speech, and indecent contents that are not suitable for children are very common in the social network sites. The Malaysian and Spanish government regulates these contents as they regulate the contents in other traditional mass media. For the purpose of regulatory compliance most social networks do not allow children under 13-14 to access their services. However, the technology that controls this restriction can easily be evaded and the service providers are still uncertain how to label contents appropriate to child access. Both Governments and corporations agree that control is insufficient and so companies embark on self-regulation of themselves through Codes of Conduct. The objective of this paper is to compare how far the regulation and self-regulation protect children in social networks sites and what need to be done to improve the effectiveness of regulation. The paper compares social networks in Malaysia and Spain to find strengths and opportunities that could enrich regulation of social networks in both countries.

Key-Words: - Online, protection, children, social network, regulation, data, privacy, security

1 Introduction
Social networks are online services provided through the Internet that allows users to generate a public profile. The social networks facilitate capturing of personal data and information of the users while providing with tools to interact with other users [1]. Social Networks are also accessible via mobile devices (Tuenti, Facebook, Keteke, and others). Around the world, children and young people are using the Internet for social interaction. But given the unregulated nature of those services, their protection can be difficult. Many of the sites which are very popular among young people collect vast amounts of personal information for sales and marketing purposes. Children rarely read the privacy policies of websites they visit so they are often unaware of their legal rights. In 1989, the United Nations General Assembly adopted the International Convention on the Rights of the Child, declaring that states would respect and ensure the rights of children, including the right to the protection of their privacy. Since that time, Data Protection and Privacy Commissioners of Europe have grown increasingly concerned over the online encroachment into the private lives of children. At the same time, Commissioners have recognized that an education-based approach combined with data protection regulation is one of the most effective methods of addressing the issue [2]. At the 30th International Conference of Data Protection and Privacy Commissioners in October 2008, a Resolution on Children’s Online Privacy [2] warned the potential risks to the privacy of Social Networks users as information on each profile is available to the user community. The lack of protection makes it easy to copy all types of personal information from these profiles and leak this information outside of the network when indexed by search engines. The Data Protection Authorities stressed the need to make an information campaign and involve both public and private parties in order to prevent various risks associated with the use of social networks. The suppliers of services for social networks among others were recommended to adopt measures relating to information control, security, profile eliminations, promote the use of pseudonyms, prevent mass data profile downloads by third parties and guarantee that...
user data can only be explored by external search engines with consent.

In 1998, the Federal Trade Commission of USA developed the Children’s Online Privacy Protection Act (COPPA, 2000) which requires the Commission to enact rules governing the online collection of personal information of children under 13 [3]. Firms have to make reasonable effort (taking into consideration the available technology) to ensure that before personal information is collected from a child, one of the child’s parents receives notice of the operator’s information practices and consents to those practices. Through this practice the children will be informed whether the content they wish to access is suitable for their age group.

This research paper explores the level of protection provided for children of Social Networks in Malaysia and Spain [5]. Besides the legislative protection the paper also will look into the self-regulatory measures taken by the industries in these countries.

2 Methodology
The paper studies the issue of children protection on social networks (SN) by comparing the legislative and regulatory framework of Malaysia and Spain. This study helps to find out the differences or similarities between two countries which have diverse legal systems and cultural frameworks.

The premise of our study is the conclusion of recent works that highlight several risks for children while using ICT and social networks [1], [2]. Those studies underline that both regulation and self-regulation are important to protect children. Therefore, taking into account the different legal systems of Spain (French, normative model) and Malaysia (Anglo, jurisprudential model), we have analysed regulation and self-regulation that could protect children from Social Networks risks to compare them and find similarities and differences that could improve children protection.

3 Malaysian Regulation & Self-regulation
Children Content in Malaysia is governed by Child Act 2001, the Communications and Multimedia Act 1998, the Printing, and Presses and publications Act 1984. The Child Act 2001 defines a child as a person under 18 years of old. The printing Presses and Publications Act 1984 imposes some legal restrictions concerning possession, transmission or access of pornographic materials including child porn materials. Part IV of the Act 1984 entitled ‘Control of Undesirable Publication’ gives power to the relevant Minister to prohibit any publication containing material which is likely to be prejudiced to or is likely to be prejudicial to public or national interest. The Minister may prohibit the printing, production, reproduction, publication, sale, issue, circulation or possession of that publication. It is an offence under the Act 1984 for a person to produce, reproduce or publish prohibited publications as determined under section 7. Undesirable publication in section 7 means publications that consist of articles, photograph, writing, sounds, music, and statements in any manner which prejudice the societal well-being.

Section 211 of the Communications and Multimedia Act 1998 also regulates prohibited contents. It states that no content application service providers or other person using a content application service shall provide content which is obscene, false menacing or offensive character with intent to annoy, threaten or harass any person. These laws could be applied to contents that are transmitted, stored and used in the social network sites too. Anyone violating this will face criminal sanction.

However, Malaysian law does not have specific law concerning privacy rights. The absence of a law which specifically provides protection for personal data of an individual causes many problems. The introduction of a Personal Data Protection Act will be necessary. Due to various concerns over data privacy, Malaysian government had drafted the Personal Data Protection Bill in 1998. The Bill was intended to regulate the collection, possession, processing and use of personal data by the data user (individual, company, organization or government). Providing statutory protection for the individuals’ data was set to be its primary concern. With this initiative the Malaysian government sought to promote confidence among the users of Internet for various purposes [8]. The Bill was introduced to satisfy the increasing demand of the local and international community. The principles that need to be adhered to when collecting, holding, processing or using personal data are illustrated in section 4 of the Bill. It consists of 9 data principles. They are: the personal data shall be collected fairly and lawfully; purposes of collection of personal data; use of personal data; disclosure of personal data; accuracy of personal data; duration of retention of personal data; access to and correction of personal data; security of personal data; and information to be generally available.

The Bill remained as a draft till 2001. After the 9/11 catastrophe in USA, the government redrafted the 1998 Bill to reflect the rights of individuals and the companies, and the government's interest over the personal data.1 The redrafting was considered as necessary since it was felt that the Bill 1998 which

---

1 As the draft is kept under Official Secret Act, only secondary data will be analysed here.
The existing privacy legislation does not guarantee adequate protection. They cover only small portion of the issue on the whole segment of the right to privacy. These provisions in no way will be able to protect the privacy over the global dossier and as regards the protection of children’s personal data too the situation remains the same. Some of the obvious weaknesses of the new Bill are:

1. It is not clear how the voluntary self-regulation and enforcement under the Safe Harbor are to be addressed by providing a single regulatory body for the personal data protection under the Bill.
2. It is also not clear how the regulatory body is going to be constituted, what are the functions, power and restrictions.
3. Other written laws will prevail over this Bill to the extent of its inconsistency. The reason being is that the legislation is drafted to fill in the gaps concerning personal data protection which is not covered by available written law in the country.
4. It does not provide protection for public record information.
5. Protection is also exempted for any processing of personal data pursuant to “conflicting obligation” or “explicit authorization” of law [11].

It is alleged that the Malaysian new Bill embodied the weaknesses of Safe Harbor by minimizing restriction to the application of data protection principles and also by providing adequate redress mechanism to the victimized individuals against the data controller. How far the new legislation is going to provide protection for privacy is yet to be known to the public as the Bill is still kept under Official Secrets Act of Malaysia. There are 7 data
principles that are applicable to private sectors. These principles may control the abuse of personal data for business profitability. However, since the new draft is proposing “opt-out” system, level of protection guaranteed as compared to the Bill 1998 could be seen less. The other problem with the new draft is that the government agencies are exempted from the application of many data principles. As the government is the holder of huge amount of data including e-health data, how far this new law is going to protect personal data privacy is yet to be seen.

On the issue of self-regulation the Content Code was drafted by the Communications and Multimedia Content Forum under section 212 and 213 of the Communications and Multimedia Act 1998. This Code represents the views of the industry and sets out guidelines, good practice procedures and the standards of content disseminated to various audiences. The Code would be relevant to all online and mobile contents. Content is defined as “any sound, text, still picture, moving picture, other audio, visual presentation or any combination of the above which is capable of being created, manipulated, stored, retrieved or communicated electronically.” The prohibited contents under the Code are indecent content, obscene content, violence, menacing content, bad language, false content, children’s content, family value and people with disability. The classification specifically addresses the issue of children’s content. The special prohibition on children’s content addresses the issue of violence, safety, security and imitable acts. A content or service provider would be responsible when he has full knowledge of the substance of content and control over the substance of such content.

Therefore, Content Access Service Providers, Content Providers, Content Aggregates and Link Providers may be held responsible. The Code has some weaknesses that could affect the full utilization of the Code. Under the Code there is no mandatory reporting to the enforcement agencies and other regulating bodies on the illegal materials. The Bureau set up under the Code has no power to order imprisonment and it can only use reprimand, imposition of fines and removal of content or cession of the offending act.

4 Spanish Regulation & Self-Regulation
The use of communication technologies such as Social Networks is growing considerably among the children and offers greater opportunities and participation, interactivity and creativity but it also places them in risks of abuse and misuse. Thus it is inevitable to introduce measures to promote the safe use of social network sites [12]. In this context, it may be appropriate to look at some of the provisions of Spanish laws to see the protection given against the abuse and misuse of children’s personal data.

The Data Protection Regulation 1720/2007 of 21st December has clarified and explained in its article 13 at what age we can consider that the children are mature enough to give their consent to the automated processing of their personal data and at which age this consent must be given through their legal representative. Children over 14 years of age are mature enough to be able to consent by themselves to the automated processing of their personal data (provided that it has been given with all the legal guarantees and for services appropriate to his or her age). Article 162.1 of the Civil Code also requires that the under age children must be represented by the legal representative.

The Organic Law 1/1982 of the Civil Protection Right honours personal and family privacy and establishes procedures to follow. It states the necessity of honouring one’s privacy and self-image plus it allows each person to keep his or her family information in person. It provides, however, the possibility of a mature minor to give consent to use, disclose or collect personal information which affects his honour, intimacy and self-image. In cases where the child does not have sufficient capacity to consent, the rule provides that consent will be given in writing by his legal representative who will be required to inform the prior consent to the prosecutor within eight days and if the public prosecutor objects, the judge could decide on the issue.

An additional criterion is mentioned in Organic Law 1/1996 of January 15 on Protection of Minors which partially amended the Civil Code and the Code of Civil Procedure. That provision recognises the child's right of privacy and provides for intervention of the Public Prosecutor in cases of dissemination of information or the use of images or names of the minors in the media that may involve an unlawful intrusion into their privacy, honour or reputation, or that is contrary to their interests. Also, it orders the parents or guardians and the authorities to protect these rights against possible attacks by third parties.

It is clear that social networks require a systematic and proper order as children under 14 years can access technologies that capture and reproduce information which affect their honour, privacy and image. Photographs of children proliferate on the Internet in their own spaces, even on pages linked to family and school activities. Those information can be used by malicious users to contact them and social networks are not to be able to control them neither they are in a position to control publications made by children who are users. They do not have appropriate
tools to ensure full identity of users, causing major difficulties in achieving effective protection of children. Some Agencies, as the Spanish Data Protection Agency, provide a series of recommendations to parents, highlighting among other recommendations, the need to train and educate both the parents and children. In addition, Law 34/2002 of July 11 on Services of Information Society and Electronic Commerce provides that in the case of websites accessible by minors, they should not integrate content that violate values that protect children and youth.

On the issue of self-regulation, some e-commerce sites signed the “Confidence Online Code”, a system of the Spanish Federation of E-commerce and Interactive Advertising (AECM-FECEMD) [13], which is part of the European Extra-Judicial Network (EEJ) of the European Commission. This system of self-regulation tries to increase consumer confidence in electronic commerce and interactive advertising. Few Social Networks have signed it because it is more focused on commerce. It could be better for Social Networks to adopt a similar Code called Mobile Operators Code which focuses on all kind of services [14]. The problem is that this code of content does not cover content exchanged between users on a person-to-person level. However, few of its measures can easily be adopted by Social Network Sites. They are:

1. not to market under their own brand content that has been classified as being for adult consumption without first offering adequate means of controlling access to such material;
2. to display a message warning of content classified as being not suitable for persons under the age of 18 in accordance with current Spanish social standards before offering access to such material;
3. to offer information on how to use social network services responsibly, including measures that can be taken by parents, carers and educators to ensure a responsible use by the children and young persons under their supervision; and
4. to collaborate with official security organisations and police forces in the fulfilment of their obligations regarding content prohibited under criminal law, with particular reference to content that is likely to have a negative effect on the personal development of children and youths.

5 Comparative Analysis
Some regulatory principles are common in both Malaysian and Spanish legislations. Adult age is fixed in 18 years so children are the same group in both countries. However, Spanish legislation has established two different groups of children: one until 13 years and other up to 14 years. In this sense Spanish legislation has a more extended regulation regarding children.

As for privacy right, Spain has developed this basic right since 1999 in accordance with its Constitution. The integration in the European Union made Spain to review Data Protection Act to adopt the corresponding European Directive. Thus Data Protection Regulatory was recently reviewed in 2007 that included article 13 which directly protect children. Malaysia has tried to approve its own Data Protection Act since 1998. The delay in passing the legislation will make the children’s data privacy vulnerable for abuses. The proposed legislation on data protection, however, does not follow the European model rather it proposed to follow the USA model of safe harbour.

Finally, both countries have different regulations controlling adult contents to children, there are no restriction in extending these regulations to social network sites. In addition to these regulations, there are self-regulatory mechanisms available for the better protection of children in social network sites. The self-regulatory mechanism seeks to cover gaps in the existing regulation. Thus the finding suggests that the two countries are very much concerned about protecting children and the legislation and self-regulatory initiatives can be used to prevent number of risks. However, updating of the current legislative framework together with proper implementation is inevitable for the protection of children in social networks.

6 Conclusion
This analysis shows that there are regulation and self-regulation in both countries that address the issue of protection of children. However, the areas of coverage differ as per their culture and legal system. The available legislative framework that is drafted to regulate offline activities of the children could be extended to cover the legal challenges faced by children in exposing them in social network activities.

Spain, due to its integration in the European Union, has many regulations regarding child privacy. However, the legislation does not help to police the social network sites effectively. The paper shows that besides regulation, the self-regulation could be the key to solve many of the problems as the companies themselves voluntarily adopt the code and try to build reputation as “safe sites”. The social network sites could form an international sector to have a uniform self-regulatory system to protect the children worldwide.
7 Acknowledgement
This paper has been developed in the frame of the Research Project conducted by Professor María de Miguel Molina and supported by Valencia Region Government (Spain): ‘M-MINOR: ICT Mobile Services and children protection’ (M-MENOR: la protección del menor de edad ante los Servicios de la Sociedad de la Información por telefonía móvil, con especial referencia a la Comunidad Valencia). Ref: GVPRE/2008/102.

References: