Social Network Sites and Protection of Children: Regulatory Framework in Malaysia, Spain and Australia

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, Spanish and Australian government regulate 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, Spain and Australia to find strengths and opportunities that could enrich regulation of social networks in those countries.

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

1 Introduction

Social networks are online services provided through the Internet that allow 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 [1]. 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 involving 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:

1. to adopt measures relating to information control, security, profile eliminations,
2. to promote the use of pseudonyms,
3. to prevent mass data profile downloads by third parties, and
4. to 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 [4].

The social network sites like Myspace, Face book and Linkedin in response to the demand of regulators and public provide the option in profile privacy setting to allow the users to manage their privacy. My space through search news feeds and wall allows the user to exert control over the user's face book and social ads. It also provides options to publish or not to publish stories. But it is to be noted that most of the social network sites collect personal information. For example, Face book collect personal information provided by the users and by the system as the users interact the web. However, Linkedin privacy policy clearly states that it follows the EU Privacy Framework and it certifies to meet the strict privacy guidelines of the EU. All relationships are mutually confirmed and any access to information will be consented. Its members are required to provide personal information as registration process and the site also collects information through the website and the customer service website. However, the technical information like web log, cookies, IP addresses and linkage to personal information will not be shared with any other third party without consent. It is interesting to note that the policy of Myspace makes a distinction between registration data and other profile information. It states that the site is the data collector in case of registration data but not on the profile information. Profile data include interests, hobbies etc. [4].

The data available under Social Network are categorised into 5 types:

1. service data: it is given as basic information to get registered as SNS member
2. disclosed data: this data are posted by a user on his pages for example photograph and messages.
3. entrusted data: they are posted on others' pages. The data is same as what is posted in disclosed data but the data subject does not have control over it.
4. incidental data: these types of data are posted by others that talk about a user. It is same as disclosed data. The data subject has no control over them and neither he created them.
5. behavioural data: these types of data are collected by the SNS about one's habits and his association [5].

Even if there are various terms and technologies that are specified or used by the social network sites to provide protection of children and other users, the children often neither understand the technology features nor read the terms. Therefore there is a high possibility that they disclose most of the private data exposing themselves to possible privacy violation by third parties. Thus the legislatures are trying to provide regulatory framework to balance the business interest for collection of data and private right over their data. However, mal practices and unawareness of the existing principles cause various violation .This research paper explores the level of protection provided for children of Social Networks in Malaysia, Spain and Australia [6]. Besides the legislative protection the paper will also 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 frame work of Malaysia, Spain and Australia. This study helps to find out the differences or similarities between the three countries which have diverse legal systems and cultural frameworks.

The premise of the 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 and Australia (Anglo, jurisprudential model) [7], the paper 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 under18 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 (As the draft is kept under Official Secret Act, only secondary data will be analysed here). The redrafting was considered as necessary since it was felt that the Bill 1998 which followed UK legislation on personal data protection was not acceptable as it was not adequate, complex and onerous. The government decided to adopt the Safe Harbor Model with modifications as it was thought that it will suit better for the Malaysian circumstances.

The Safe Harbor Model is said to be flexible and not onerous on the data user to get pre-consent on all types of data before collection or holding or use [9]. Further, it is believed that the new draft will satisfy the data subject, the user as well as the requirement of EU directive on the adequacy of law concerning the protection of personal data. This Bill proposes to cover any personal data directly relating to living individuals and it regulates person, body of persons, corporation and government who collect, use or disclose personal data. In this respect, there is no difference between the Bills 1998 and 2001. However, the new Bill by providing different sets of data principles to private and public entities differs from the 1998 Bill. The obvious difference under the new Bill is that the private sector is required to follow seven principles as in Safe Harbor unlike the nine principles provided in the old Bill. The new principles are:

Notice Principle: It requires the data user to inform the data subject the purpose of data collections, contact details of data user, the types of third party, the data to be disclosed and the information about the limitation of its use.

Choice Principle: Allows the individual to opt out to other purpose for which the data was not originally collected or subsequently authorized by the data subject.

Disclosure Principle: Disclosure of personal data to third party must follow notice and choice principles if the transfer is for the similar purpose for which it was initially collected.

Security Principle: Security from loss, misuse, unauthorized access, unauthorized disclosure, amendment or destruction while collecting, using or disclosing personal data is a very important duty imposed on the data user under this principle.

Data Integrity Principle: When the data user collects, uses or discloses personal data, the data shall be relevant to the purpose. This principle further requires that any subsequent disclosure or use must be compatible with the original purpose.

Access Principle: Enforcement Princ Allows access to data subject to correct, amend or delete where the personal data is inaccurate. This data principle is not applicable where it is proven that the burden or expense of providing access is greater than the risk to the individual privacy or where it is shown that allowing access will lead to disclosure of other individual's data where the individual concerned did not consent to such access or where such access is regulated by law.

Enforcement Principle: This principle requires that the data user should provide clear transparent mechanism to ensure compliance of data principle and in the event of non-compliance recourse for affected individual must be expressed unequivocally.

Public sectors, under the new Bill, are only required to comply with three major principles:

1. The principles of collection, use and disclosure as required by law,
2. Right to access by written law, and
3. Responsibility to protect personal data.

The reason for relaxation given to public sector under the Bill is that privacy in the public sector is adequately regulated through Official Secrets Act 1972, section 4 of Statistics Act 1965, section 19 of National Land Code and section 139 of Consumer Protection Act 1999. Additionally, the data subjects are indirectly protected in public sector through administrative measures and disciplinary legislation[10].

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:

a) 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.
b) It is also not clear how the regulatory body is going to be constituted, what are the functions, power and restrictions.
c) 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.
d) It does not provide protection for public record information.
e) 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 [Item 5.0 Part 1 of the Code]. 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 [Item 8.0 Part 2 of the Code] . 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 (AECEM-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 [14].

5 Australian Regulation & Self-Regulation

Australia provides protection for children's privacy through various legislation and self-regulatory mechanisms. The Privacy Amendment Act 2000 was extended to private organisations through Privacy Amendment (Private Sector) Act 2000.The Privacy Amendment Act 2000 covers personal information or opinion that can identify a person that includes children. The approach in the Act reflects at least three conditions of the Commonwealth government:

1. Legislation reserves its limitation. Law generally develops much more slowly than the new technologies. This can severely limit the effectiveness of law in practice;
2. The legislation is inconsistent with the government's notions of "steering not rowing". It is believed that the law has the potential to stifle innovation and reduce freedom of choice; and
3. Though Australia is part of global economy, it is a relatively small player and is hardly in a position to set the rules, except perhaps at a marginal level.

Thus the 2000 Act only introduced a co-regulatory approach. The co-regulatory approach introduced under this law is intended to foster industry-developed codes, but the codes will be underpinned by legislation that will establish key privacy principles that will serve as a default framework in the absence of industry codes. As a rule, most organisations in the private sector will be required to either adopt a code or comply with the legislative privacy principle. The legislation seeks to set reasonable consistent privacy standards. Meanwhile it tries to give businesses the flexibility to develop an approach to privacy protection that is relevant to their day-to-day practice and that meets community expectation about the handling of personal information.

The Act requires organisation and private sectors to develop their own codes of conduct regarding privacy, which will then be approved by the Federal Privacy Commissioner. The Commissioner can revoke a code. The code can include its own complaint handling mechanism, if it does, it must provide for the appointment of a code adjudicator to determine complaints. It is believed that a code that incorporates complaints handling mechanism can give industry a sense of ownership. If a code does not provide for a complaint handling mechanism, the Office of Federal Privacy Commissioner will handle complaints and the Commissioner will be the code adjudicator [15]. The National Privacy Principles (NPPs) which were introduced by this Act aim to deliver, *inter alia*, promotion of greater openness between social network service providers and network users regarding the handling of personal information. They cover the whole information lifecycle from

collection to storage, maintenance, use and disclosure. Under the law, social network service providers can only collect information if the users have given consent. The users' consent can be reasonably considered as implied as long as it is clear to the network users the reason for the collection. It may be necessary to the service provider to advise them about how the information will be handled. The users will have access to the information collected. They may look at the information, obtain a copy of the information, take note of the information, listen to the information, and get an electronic copy of information stored on a computer system or a database. This Privacy Amendment Act 2000 gives individual a right to know on what information an organisation holds about and a right to correct that information if it is wrong. By this Act social network users like children have the right to know the reasons for collection of their personal information by private sector. They will also know the kind of information it holds about, the usage and the parties who will get the information. Patients can also make a complaint if they think that their information is not being handled properly. Some of the privacy principles like data security and data quality will be applied to organisations that already held data when the Privacy Amendment Act 2000 was implemented.

The collection principle states that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. The information collected must be of lawful and by fair means. At or before the time of collection, it must take reasonable steps to ensure that the individual is aware of:

a. the identity of the organisation and how the data will be collected,
b. the fact that he is able to gain access to the information,
c. the purposes for which the information is collected,
d. the organisations to which the organisation usually discloses information of that kind,
e. any law that requires collection, and
f. the consequences if all or part of the information is not provided.

The Privacy Amendment Act 2000 regulated the way private organisations can collect, use, keep, secure and disclose personal information. This gives a right to know why a private sector organisation is collecting one's personal information, what information it holds about him, how it will use the information and who else will have access to that data. The Act covers private sector "organisations" which include businesses with annual turnover of more than $ 3 million [16]. The Privacy Amendment Act 2000 exempts political parties, the media and small businesses as well as use and disclosure of employee records. Political parties are exempted from legislation for their activities in connection with an election, referendum, or other participation in the political process. Domestic use exemption allows the use of personal information related to personal, family or household affairs. Transfer of personal information between "related bodies corporate" is allowed to pool its personal data collections without the knowledge of its customers. However, there are restrictions as to the use and disclosure of this information. It is estimated that the small business exemption will leave up to 95% of the Australian business untouched by law. It is to be noted that small businesses will be subjected to the privacy principles if they collect or disclose personal information. It seems that exemption is not applicable if data is disclosed or collected for benefit, service or advantage. Besides the Privacy Amendment (Private Sector) Act 2000, the Telecommunications (Interception) Act 1979 protects privacy of public and private sectors by general prohibition on interception of communications passing over telecommunication systems. Freedom of Information Act 1982 gives individuals the right to access data about themselves that are held by a commonwealth body. The Act also provides for correction of data found to be incorrect.

Unsolicited Bulk Email or Spam is said to be one of the main causes of violation of right to privacy of internet users in general. The Act regulates spam mails too. According to the Coalition Against Unsolicited Bulk Email of Australia, spam is defined as any electronic mail message that is transmitted to a large number of recipients, and not explicitly and knowingly requested by some or all of those recipients [17]. Spam is expected to account for approximately 40% of all Internet email delivered in 2001[18]. An organisation subjected to the privacy principles has legal obligation to abide by the rules on unsolicited commercial e-mail. It requires organisation to collect
personal information only by lawful means [19]. In the case of unsolicited commercial e-mails, there may be a breach of privacy if the person does not get information about who has collected information about him, for what purpose. Information collection practice would be deemed unfair, depending on whether and how the spammer obtained a personal email address. Where a person has done business with an organisation and has asked it not to contact

him with marketing offers, the person could reasonably expect not to get any more offers. An online marketing must obtain opt in consent to use personal information for online marketing if that action is not related to primary purpose of collection and is not within the individual's reasonable expectations[19].

Along with the legislative framework three Content Codes of practice have been developed by the Internet Industry Association. Content Code 1 deals with ISP obligations in relation to general internet access. It is concerned with minimising access by children to unsuitable Internet material. For instance, certain contents are not available for children under 18 years of old without parents' consent. It also requires ISPs to encourage appropriate labelling of content which is likely to be considered unsuitable for children. In addition, the code requires ISPs to provide users with information about the supervision of children's access to the Internet. The code also requires ISPs to have procedures to deal with complaints from subscribers about unsolicited email that advertises Internet information [5]. Significantly, the code also requires ISPs to inform content providers "of their legal responsibilities, as they may exist under the Act or complementary State or Territory legislation in relation to Content which they intend to provide to the public via the Internet from within Australia". Content Code 2 deals with ISP obligations in relation to access to content hosted outside Australia. Specifically, the code provides that ISPs must provide filter technology at a reasonable cost. Content Code 3 deals with Internet content host (ICH) obligations. This Code is concerned to minimise the access of children to unsuitable material and so it replicates many of the provisions outlined in Content Code 1[20].

There are number of non-regulatory mechanisms available to protect childern. These include hotlines, filtering, rating systems and education and awareness. Many of these are overviewed in the *Safer Internet Action Plan (SIAP)* developed by the European Union as well as by the United Nations. Hotlines are one approach used to deal with inappropriate or unsuitable Internet content. Reference has already been made to filtering systems which can automatically restrict access to problematic sites according to general notifications, end-user selection or keywords. These filtering technologies are canvassed in a range of reports, and particularly by the Australian Broadcasting Authority. Rating systems allow content creators and/or third parties to classify content. This rating is then identified by the end-user's filtering system and access is determined accordingly. End-user education is another non-regulatory tool available to combat problem related to Social networl sites. In line with its emphasis on protecting children from harmful content, the Australian Broadcasting Authority has developed its "Cybersmart Kids Online" education tool for children. Other important 'net literacy' resources internationally include Childnet International and "Quality Information Checklist"[20].

Besides the above, Good Practice to educators, principles and directors introduced by Ministry of Education well specify the Cyber-safety Guidelines. It seeks to ensure children's good behaviour and safety irrespective of the fact whether they are online or offline. The provisions applies to staff members and children accessing online services in any schools and training centres that come within its jurisdiction. The policy addresses the issues like: Access and security, User identification and passwords, Appropriate behaviours. This includes the prohibitionof cyber buying and image exchange and acceptable use agreement [21].

The analysis of the legislation, guidelines and policies show that the social network sites operators are data controllers and they have legal obligations. Network sites like Facebook, Myspace cannot escape legal responsibilities as they:

a) provide means for the processing of user data,
b) provide services related to user management such as registration and deletion of account, and
c) use user data such as the personal information in advertisements [5].

Data controller has more responsibility than processor. They should provide clear identity about them while privacy-friendly default setting and privacy warnings for the users and warnings about privacy implication should also be given. The Act 2000 gives exception to household use but this exception will not be available if an SNS user acts on behalf of an organisation or corporation or uses for commercial, political or charitable goals.

6 Comparative Analysis

Some regulatory principles are common in Malaysian, Spanish and Australian legislation. Age of majority is fixed as 18 years in all three countries. However, Spanish legislation has established two different groups of children: one until 13 years and the other up to 14 years. In this regard 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 protects children. Malaysia has endeavoured for 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.

Australia in regulating the private sector prefers to do in a co-regulatory fashion which allows the industries to create their own privacy code that needs to be approved by the Privacy Commissioner. In addition there are other regulation and guidelines that monitor the collection and use of personal data. Recently the Australian Government introduced internet filter to protect children and through this filtering system it is planned to blacklist websites that violates the specified rules. Even if the initiatives were criticised but it could bring benefit in protecting the children from privacy intruders [22].

All these three countries have different regulations controlling adult contents to children. There are no restrictions 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 all these three 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.

7 Conclusion

The analysis shows that there are regulation and self-regulation in the three countries that address the issue of protection of children in social network sites. 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. Australia has a very comprehensive system of regulation and self regulatory mechanism that seek to protect children's privacy. 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. Many users are either unaware of privacy options offered to the sites or the privacy features did not conform with the expectations and experience of privacy they brought to the sites. Therefore privacy control should be easily mapped on the user's understanding and the social network sites' default setting should protect privacy. There should be no process of information sharing and the users should be given the option of opt-in rather than opting-out.

8 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:

[1] Study on data privacy and security in the Social Networks Sites (Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online). *Spanish Data Protection Agency (AGPD and INTECO)*, pp. 1-159, *https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf*

[2] 30th International Conference of Data Protection and Privacy Commissioners. Strasbourg, 17 October 2008, *Draft Resolution on Children's Online Privacy*, *https://www.agpd.es/portalweb/privacyconfere*

nce2009/documentacion/common/childrens_online_privacy_en.pdf

[3] *Children's Online Privacy Protection Act (COPPA)*, Federal Trade Commission USA: 2000, http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm

[4] Newman. A. L., and Bach. D., Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States, *Governance*, 17 (3), 2004, pp. 387–413.

[4] Jennifer Barrigar, Social network site privacy: a comparative analysis, The office of the privacy commission of Canada, *www.priv.gc.ca,* Feb 2009

[5] Out-law.com, Social Networking Giants are subjected to EU Data Protection Laws, 22 June 2009.

[6] Google Trends, *http://trends.google.com/websites*, 2009

[7] Mattei, U., and Monti, A., Comparative Law & Economics. Diritti, Regole, Mercato, Economia pubblica ed analisi economica del diritto. *XV Conferenza SIEP*. 2003, Società italiana di economia pubblica, *http://www-1.unipv.it/websiep/wp/291.pdf*

[8] Mattei, U., Comparative Law and Critical Legal Studies, in *The Oxford Handbook Of Comparative Law*, M. Reimann and R. Zimmermann eds., Oxford University Press, 2006, pp. 816-832, *http://works.bepress.com/ugo_mattei/32*

[9] Multimedia Super Corridor, *http://www.msc.gov.my,* 31 December, 2006.

[10]Nor, M., e-Privacy in the New Economy, *National Conference Management Science and Operations Research 2003*, Vol. 2, pp. 242-244.

[11]Reidenberg, J.R., E- Commerce and Trans-Atlantic Privacy, *Houston Law Review*, No. 38, 2001, p. 745.

[12] European Union: Proposal for a Decision Of The European Parliament And Of The Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies COM (2008) 106 final, *http://ec.europa.eu/information_society/activities/sip/docs/prog_2009_2013/decision_en.pdf*

[13]Spanish E-commerce Federation Code (FECEM), *http://www.confinazaonline.org*

[14]Code Of Conduct For Mobile Operators Designed To Encourage Responsible Use By Underage Persons Of Electronic Content Services Supplied Via Mobile Telephone Networks in Spain. Safer mobile use (Safer Internet Programme, *http://ec.europa.eu/information_society/activities/sip/index_en.htm,http://uk.sitestat.com/gsm/gsmworld/s?spain_en&ns_type=pdf&ns_url=http://www.gsmworld.com/gsmeurope/documents/eu_codes/spain_coc_0308.pdf*

[15]Malcolm Crompton, Privacy Amendment (Private Sector) Act 2000, December, 2001, *www.privacy.gov.au.*

[16]Caslon.com, Caslon Analytics Profile: Australian Privacy Regimes 2006, *http://caslon.com.au/austprivacyprofile3.htm.*

[17] Coalition Against Unsolicited Bulk Email, Spam, *http://www.caube.org.au/whatis.htm.*

[18]Morrissey, B., "Spam Under the Tree", *http:www.internetnews.com.IAR/article.php/1561201.URLs,* 4 June 2006.

[19] Guidelines to the NPP. 2.1 (c), September 2001.

[20]Australian Human Rights Commission, Internet Regulation in Australia, October 2002, *http://www.hreoc.gov.au/racial_discrimination/cyberracism/regulation.html#16*

[21] Ministry of Education and Children Services, Cyber-Safety Keeping Children Safe in the Connected World: Guidelines for Schools and Preschool, June 2009, *www.decs.sa.gov.au/docs/documents/1/cybersafetykeepingchildre.pdf.*

[22] SPPA, Inquiry into the sexualisation of children in the contemporary media environment, 17 April 2008