Copyright © 2011 International Journal of Criminal Justice Sciences (IJCJS) – Official Journal of the South Asian Society of Criminology and Victimology (SASCV) ISSN: 0973-5089 January – December Vol. 6 (1&2): 372–385

Emerging Platform for E-Crime: Issues of Social Networking Websites in India

Itisha Yadav[1] & Fathima Quraishi[2]
Dr. Ram Manohar Lohiya National Law University, Lucknow, India

Abstract

Ironically, the SNS (Social Network Services) which were conceived to develop a healthy relationship between netizens is used as a tracking device to follow the behaviour and actions of many. Very valuable information is exposed on these highly compromised platforms. There is also a perceived privacy threat in relation to placing too much personal information in the hands of large corporations. This paper elaborates upon issues such as safety implication, privacy, social capital, youth culture and education and legal implications. Additionally, the working of Social Networking Sites with law enforcement agencies and also the pigeonholes in the privacy policies of some social networking sites are carefully perused. Furthermore, four components of data protection and privacy regime of India, namely, (a) Constitution of India (b) The Information Technology Act, 2000 and the subsequent Amendment Act passed in 2008 and (c) Draft Reasonable Security Practices Rules, 2011, have also been deliberated upon.

Keywords: Social Networking Services; Privacy; Youth Culture; IT Act 2000.

Introduction

Social Networking Sites provide a virtual community for people to interact. People need to understand that it will get problematic for them if they reveal too much about their personal lives on a public forum. With the growing popularity of these sites, the volume of content has grown and has become very personal. People are nudged towards self-revelation by others which drastically affect privacy. This phenomenon is also called *herding*. The normal boundaries for selectively sharing information within predefined groups have slowly eroded.

Now that the social networking frenzy has reached a fever pitch, it marks a dynamic shift in the way that people connect, collaborate and communicate throughout the world. The reason for its quick growth is not the remarkable new technology, but because it strikes into the inherent need for humans to intermingle. The dawn of computers, the internet and web technologies meant that people were becoming standoffish in their

[1] Undergraduate in Law, Dr. Ram Manohar Lohiya National Law University, Sec- D1, LDA Colony, Kanpur Road Scheme, Lucknow – 226012, Uttar Pradesh, India. Email: freezememoriesin@gmail.com

[2] Undergraduate in Law, Dr. Ram Manohar Lohiya National Law University, Sec- D1, LDA Colony, Kanpur Road Scheme, Lucknow – 226012, Uttar Pradesh, India. Email: fatima_quraishi@hotmail.com

interactions. People worked remotely from their domiciles and experienced a dramatic reduction in the amount of true social interactions. Social networking has empowered people to connect with others in a way that satisfies the basic instinct to be social but on a scale that was previously unattainable (Brasser, 2010). Today, there are numerous social networking websites over the internet, like Facebook, Orkut, Twitter, Friendster, Myspace, Hi5, etc. These sites provide a platform for criminals to give effect to their activities. An example of criminal activity can be illustrated by a simple instance where there has been a dramatic migration of users from Orkut to Facebook, perhaps because Facebook offers more attractive features. Even though Orkut has become a bit outmoded amongst the online social networks, it still has inactive accounts of the people who were once active on it. These accounts contain personal information of the account holder. Although new privacy settings have been introduced, the inactive accounts do display the personal information, like name, gender, area of residence, birth date etc. according to the previously done privacy settings, which were not so adequate. Criminals can easily take advantage of the inactiveness of the account holders which could be harmful in a number of ways!

The potential harm of poor security measure on Social Networking Websites can be illustrated by a fairer comparison to online auction and shopping websites (e.g., Amazon.com, eBay). The content of these websites is more similar to social networking websites than search engines because monitoring is limited to the company's own website. As per eBay's Rules & Policies (n.d.), to put an item up for sale on eBay, a seller writes a description and uploads a picture; eBay takes measures to prevent fraudulent transactions, partly through identity verification by requiring a seller to use a PayPal account or credit card, which is appropriate because a seller must be over eighteen years to use eBay. This provides a buyer with judicial recourse for a fraudulent sale.

Notably though, fraud is a direct harm to eBay's business, and the measures taken against fraud are directly linked to the success of eBay as a business; a fraudulent transaction is an unsuccessful transaction. Comparatively, the harms associated with social networking websites are not as damaging to the website's business, and therefore there is less monetary incentive to address or prevent those harms. Additionally, one of the biggest differences between social networking websites and eBay is the type of harm encountered by their users. The information a user inputs into eBay is noticeably limited and different from the information a user puts on a social networking forum. On eBay, the information's focus is on the product, and on social networking websites, the information's focus is on the actual person. The very fact that the personal lives of people are publicly discussed on such forum makes it more susceptible to greater damage.

Privacy

Privacy involves the right to control one's personal information and the ability to determine how that information should be obtained and used. The volume and varying nature of transactions carried out on the net are such that the right to privacy must exist. "Right to Privacy" is an implied right under Fundamental Rights. The Constitution of India does not expressly recognize the right to privacy but at the same time this right has been spelt out by our Supreme Court from the provision of Article 21 which deals with the right to life and liberty. The Apex Court of India has reiterated the "Right to privacy" in many cases; however, its application vis-à-vis internet content has not yet been directly clarified by a judicial ruling.

a. Privacy and Data Protection

Privacy is closely related to Data Protection. An individual's details like name, address, interests, family, etc. are often available on various web sites. Passing on such information to interested parties can lead to invasion of privacy. In India, data protection is governed by The Information Technology Act. This legislation deals with the issues pertaining to data protection and privacy but not in unequivocal terms. These issues are covered in a piecemeal fashion under this Act.

The Information Technology (Amendment) Act, 2008 contains provisions which recognize privacy protection and few which encroach upon the privacy rights. The sections that recognize the privacy issues are Section 43A and Section 72A. However, Section 69 and Section 69B encroach upon the right to privacy (Aarora, 2009). These sections are well drafted when it comes to fraud cases which happen through or by social networking sites. We may note that the encroachment on the right of privacy could be in the interest of national security or likewise. These sections are condensed as follows.

Section 43A provides scope for introducing the definition of "Sensitive Personal Data or Information" (subject to notification), and also imposes a responsibility for "Reasonable Security Practice" to be followed by the data handlers. This section provides remedy to the person affected when wrongful loss is caused to him or wrongful gain is caused to another person at the expense of the confidentiality of the affected person. The victim of a breach of privacy is provided an antidote to claim compensation from the body corporate that has been negligent. And there is no upper limit for the compensation to be claimed which may even be in excess of Rs. 5 crores.

Another provision, Section 72A says that a person including an intermediary could be held liable if he discloses "personal information" which he accessed while providing services under a contract. The liability arises if the disclosure was made with an intention to cause or knowledge that he is likely to cause wrongful loss or wrongful gain to a person.

Conversely, Section 69 of the amended Act empowers the state to issue directions for interception, monitoring, decryption of any information through any computer resource. Section 69B empowers the Government the authority to monitor, collect traffic data or information through any computer resource for cyber security. In addition to the existing circumstances under the Information Technology Act, like in the interest of national security, sovereignty, public order etc., the Central Government may intercept /monitor any information transmitted through any computer resource also for investigation of any offence. The reason is that the dividing line between "Cyber Crime" and "Cyber Terrorism" is very thin. For example, a series of "Phishing Offences" may actually be part of a Cyber Terrorist's plan to "Destabilize the economy". Hence one cannot be expected to control Cyber Terrorism or Cyber Wars without controlling Cyber Crimes. There is widespread apprehension in the mind of legal experts that these provisions, giving blanket powers to the Government to intercept or monitor any information through any computer resource, would soon become a common practice and would grossly violate one's personal privacy as it is obvious that one's computer system contains very personal data and information and by virtue of this section, the Government would have unfettered right to intercept or peep into electronic communication of even bonafide persons. This can further be misused by ruling Government against their political adversaries, violating their privacy rights.

However keeping in mind the need of the hour where cyber terrorism is on the rise, the powers conferred by these sections are considered essential though the risk of abuse is evident and needs to be addressed. Cyber criminals may target a specific person or just any random individual. For example, on Facebook, by turning on the "public search" option, one makes his/her Facebook profile accessible to anyone who types the name in any of the search engines, which may be intentional or accidental. Howsoever, this provides an insight to all the profile information i.e. profile picture, gender, networks, username etc. When it comes to Facebook, another risky feature is with respect to the various applications that are available. Out of boredom or necessity, almost everyone has a propensity to use them at least once. These applications do not work in secure mode and hence a person is required to switch onto unsecure connection for access. Thereafter, it requests for permission to access the basic information, photos, videos, wall posts etc. of the user. These advertisers or application makers thereby gain access to the personal information no matter whatsoever the privacy settings are. Also, certain malicious websites cause browsers to take action without permission. For example, clicking on a link on one of these websites might cause the website to be posted to a user Facebook profile. Thus, privacy and security concerns need to be addressed simultaneously.

b. Privacy and security

Social networking sites are good for pulling together groups of people with similar backgrounds or interests. However, there are deep rooted concerns about security and privacy. The security and privacy issues are entirely two different beasts. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. Privacy issues are those involving the unwarranted access to the private information which doesn't necessarily have to involve security breaches. But both types of breaches are often intertwined on social networks, especially since anyone who breaches a site's security network opens the door for easy access to private information belonging to any user. But the potential harm to an individual user really boils down to how much a user engages in a social networking site, as well as the amount of information they're willing to share. The reason why social network security and privacy lapses exist is simply because of the astronomical amounts of information the sites process each and every day that end up making it much easier to exploit a single flaw in the system. Features that invite user participation like messages, invitations, photos, open platform applications, etc. are often the avenues used to gain access to private information, especially in the case of Facebook. A potentially devastating hole is in the framework of Facebook's third-party Application Programming Interface (API) which allows for easy theft of private information which was recognized recently. The third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the application (Felt, 2007).

The problems plaguing social network security and privacy issues, for now, can only be resolved if users take a more careful approach to what they share. In response to the potential threats that users are exposed to, most of the major networks now enable users to set privacy controls for who has the ability to view their information. But, considering the application loophole in Facebook, increased privacy settings don't always guarantee privacy and thereby secured storage of data.

Youth culture, Social Networking and Issues of Privacy

The growing body of research in the area of addiction suggests that Social Networking Sites have led to 'affective disturbances and interruption of social relationships' (Ferris, n.d.) and is a presenting problem that is becoming more common in the society. The World Wide Web is informative, convenient, resourceful, and fun but is leading to the detriment of many.

Digital youth culture refers to young people who are habitual to interact with their peers online via computing technology. This concept was first described in terms of ''digital natives'' and ''digital immigrants'' to distinguish between young people who grew up using computer technology versus older people who did not. These young people who grew up using web technology are so accustomed to it that they may not always know what is appropriate, factual, or legal for them to view or use (Prensky, 2001).

Users in this current age of cyber world and easy access to social networking groups prefer to meet online rather than in person. For many years classic teen ''hangouts'' such as movie theatres, and burger joints have become less popular in favour of the virtual world. Mobile and IT devices, such as cell phones that enable email, instant messaging, and up/downloading of digital files, are also changing youth culture and social dynamics.

In utilizing IT devices, youth can express themselves in creative ways with varying amounts of anonymity and privacy by just depending on the content they post and technological ways in which they do this. Since 2005 online social networking forums have facilitated worldwide communications amongst the youth as never before (Articles, 2011). Having a personal Web page on Facebook or a similar social networking forum is part of what many young people consider ''cool'' if not necessary in order to be accepted by their online and/or in-person friends. For many participants of such forums, having a Web page dedicated to and revealing about their personal life enables outreaching to an ''invisible audience'' of peers who may wish to interact. In short, online social networking provides a technological means to meet new people and make friends online.

A youth who has grown up with computers, other IT devices and the Internet may be developing different standards for behaving "online" as opposed to when they are "offline", because they are interacting more via cyberspace, where social sanctions are not clearly defined or consistently sanctioned as they are in the real world. Being out of line or ''misbehaving'' in an online social networking or gaming environment will not likely bring about the same kind or level of complaint or punishment than that doing this at home, in school, or in a workplace setting.

Abusive and criminal behaviours in social networks have resulted in negative public reactions in the media and concern among parents, educators, and legislators. Concerns about youth creating fake profiles in order to carry out harmful activities online or, conversely, to protect their real identities are also increasing along with social networking popularity.

The number of digital forums available now includes instant messengers, chat rooms, community message boards or forums, and blog style social networking sites. One has the option to include or exclude people of their choice in these forums. Privacy controls are an essential part of filtering who can and cannot visit a personal Web page or contact one via a messenger service. By adjusting privacy settings one is able to minimize the number of people who can view their personal web page or swathe information that one has revealed online. However, these controls are only effective to the extent of the user's knowledge or the one's which he chooses to enable, along with the type and amount of information that is shared with others online. Given potential flaws in computer coding, discovery of exploits have also been found in the privacy settings of software, such as those used by social networking firms like Orkut and Facebook (CIPPIC, 2008). When this happens, personal information posted by millions of youth participants can become known despite their efforts to keep certain information from becoming public (Articles, 2011).

Technological controls for signifying real profiles are typically quite limited when it comes to verifying age or an email address for admission by a social networking website host, both of which are easily defeated by the creation of alternate email accounts and/or simply lying about one's age.

The digital world has impacted how youth behave and interact today. It has created new methods for forming social groups and establishing interconnections between their members. Social interactions, beginning with physical contact, are no longer a necessary defining point of friendship. In the digital world, people merely search for a common interest on a social network and request to be added as a friend. The dynamics of social interactions between and among youth continues to change as online computing becomes more complex and arguably less manageable. For better and worse they are engulfing themselves in online activities that may involve little or no adult supervision. As the Internet and IT continues to evolve and be used in new ways, social interactions and digital youth culture will follow suit (Articles, 2007).

Data Protection by Corporations

With these new tools of social network, companies are in a great flurry to come up with new social media policies and set off new elegant ways for their customers to communicate with each other. But, with the rapid growth in this sort of social networking, one factor has suddenly become a silent threat and that is social networking fraud. These sites create exponential networks and allow tapping into other people's network and their friends' networks. This is extremely powerful and even powerful for those who want to tap into one's network with less than honourable intentions (Snow, 2010).

The most common method for obtaining personal information is social engineering (Naavi, 2009). Once personal information is provided to an unscrupulous company or person, it is difficult to regain control of the information. The sensitive information is bought and sold in the market without any ethical issues considered.

Recently, the BBC also did an extended article on cyber dangers (Ward, 2008). They say: "It is remarkable that people use social networking websites to publish details about their lives, loves, jobs and hobbies to the entire world that they would not dream of sharing with a stranger in a bar." And yet, the BBC ends their article with mixed advice. "There were a lot of benefits to using social networking sites, said Mr. King and the downsides should not put people off using them. "It's about trying to manage risk rather than avoid risk," he said."

There could be confidential information posted about a company on blogs, discussion forums and Social Networking Sites. The main risk here is the loss of corporate intellectual property, but gaining access to insiders may also be a component in a broad range of other crimes, such as hacking corporate networks to cause damage, blackmailing of employees to reveal sensitive customer information and even to access physical assets. Therefore, in our opinion it is important that stringent security measures be taken in an organization to protect it from the unhealthy social networking website activities. Even if access is granted to such websites then it should be done on computers which are not connected to the main system that stores the important corporate data.

Lohrmann (2008) provides justification for restricting employee Internet access to social networking sites in an organization for the following reasons:

- virus or spyware prevention
- employee productivity drain
- bandwidth concerns
- liability issues

Hence it is an undisputed fact that welcoming social networking sites in a corporate environment is equivalent to inviting danger. But if Corporations feel its pros outweigh its cons then they would be advised to manage this risk with utmost care.

The newly inserted Section of the Information Technology (Amendment) Act, 2008 Section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which; they would be liable to compensate those affected by any negligence attributable to this failure.

It is only the narrowly defined 'body corporate' engaged in 'commercial or professional activities' that are the targets of this section. "Body corporate" has been defined as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. Thus, government agencies and non-profit organizations are entirely excluded from the ambit of this section. This does not necessarily mean that these entitles are exempt from taking reasonable care to safeguard information that they collect, maintain or control – only that remedy against the government must be sought under general common law, rather than under the Information Technology Act.

Security Measures adopted by Social Networking Websites

Many people view social networking sites as a kind of online cocktail party where one gets to establish contacts and raise a personal or corporate profile. But the cocktail party metaphor isn't entirely accurate. In fact, users would be better served if they thought of social network services in the context of a loud glass house; a place with endless visibility.

This can be illustrated by few cases decided by the Indian Judiciary where it accepted activities done on Facebook as evidence. The case of *Mattel Inc. and Others vs Jayant Agarwalla and Others* (CS(O S) 344/2008) decided by the Delhi High Court on 17 September 2008 is a good example where copies of Facebook pages were used to decide a case on Trademark Infringement. In another case of *Carla Gannon and Another vs Shabaz Farukh Allarakhia and another* (Criminal Writ Petition No.509 of 2009) decided on 10 July 2009, Facebook activities were taken as evidence to decide the matter of custody of a minor child. Hence it leaves no room to doubt the importance of activities undertaken mindlessly on a Social Networking Site. The Indian Judiciary also gives due recognition to the same.

The Delhi High Court in an ongoing battle against Social networking websites and other similar web forums has ruled that unhealthy content on such websites is required to be removed, failure of which would lead to a total ban of the same. The Indian government also sanctioned the court's stance after reviewing all the evidence and being satisfied that they can be proceeded against as per section 153-A, 153-B and 295-A of the

Indian Penal Code (Singh, 2012). As with every fast-growing technology, security and privacy have not been the first priority in the development of such sites. As a result, along with the above benefits, significant privacy and security risks have also emerged (Gross & Sweeney, 2007). Although this case involves the question of integrity of our nation however it is a welcoming order in respect of pressurizing such multi nationals to consider privacy and security issues and built mechanism to control information on their respective websites.

Security issues have gained so much momentum now, that big names like Facebook and LinkedIn are forced to introduce a number of features on their websites to protect privacy of their users. A user can adjust how much information about posts, photos, online status and other factors are accessible to other people. Users can reduce what appears in their profile and what information about their online activities is public, such as their use of specific Facebook applications. Users can also block specific Facebook users from seeing more than a limited profile, or from finding users via search.

Facebook also limits the ability of search-site Web crawlers to harvest user information, saying in its privacy policy, "*Facebook limits access to site information by third party search engine 'crawlers' (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond the name, profile picture, and limited aggregated data about the profile (e.g. number of wall postings)*" (Policy, n.d.).

A new option has also been introduced by Facebook where a user who logs in from a different computer is asked for authorization. This login is notified to the registered email of the Facebook user. So if the account is hacked or an unknown user logs in, the information of such an access is instantaneously sent on the registered email.

LinkedIn is the most business like social networking website, and its users seem generally aware of the need to behave professionally. The site provides a wide range of tools for customizing others' views of users, such as the ability to change whether people the user is connected to can see just those having in common, or the entire connections list.

Legal Issues

1. Indian Information Technology Act

Jurisdiction under Information Technology Act, 2008 extends to persons outside India and persons who are not citizens of India provided at least one computer situated in India has been used in the commission of the offence. So far such crimes have been covered by the Indian Penal Code under Section 3 (Punishment of offences committed beyond India but which by law may be tried within India) and Section 4 (Extension of the provisions of the Code to extraterritorial offences) (Hosein, 2006). Clearly, cybercrime brings along with it numerous issues concerning jurisdiction. The India legislators were possibly aware of the potential challenges that the tricky subject of jurisdiction would pose. That is the reason why they have adopted two distinct provisions relating to jurisdiction, in Section 1(2) and Section 75 of the Information Technology Act.

Other relevant provisions of the Information Technology (Amendment) Act, 2008 which cover new offences are as follows (Aarora, 2010):

Section 66: This Section is attracted when the imposter fraudulently and dishonestly with ulterior motive uses the fake profiles to spread spam or viruses or commit data theft. The act is punishable with imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both.

Section 66A: This section is attracted when the imposter posts offensive or menacing information on the fake profile concerning the person in whose name the profile is created. Further, the fake profile also misleads the recipient about the origin of the message posted. The offence is punishable with an imprisonment for a term which may extend to three years and fine.

Section 66C: When the imposter uses the unique identification feature of the real person like his/her photograph and other personal details to create a fake profile, the offence under Section 66C Information Technology Act is attracted which is punishable with imprisonment for a term which may extend to three years and be liable to a fine which may extend to one lakh rupee.

Section 66D: When the imposter personates the real person by means of a fake profile and cheats then the provision of Section 66D Information Technology Act is attracted which is punishable in the same manner as preceding Section 66C.

Section 79 has been modified to the extent that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if; (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; (b) the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties.

Section 85 marks the liability of a Company if it commits an offence. Every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company would be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention. Further, where a contravention has been committed, and it is provided that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary, or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be protected against and punished accordingly.

2. Draft Reasonable Security Practices Rules 2011

The Ministry of Information and Technology, Department of Information Technology (2011), published draft rules under Section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporate must observe in relation to the information they hold.

Rule 3 of the Draft rules defines what constitutes sensitive personal information which includes password, user details, medical records etc. However this would not include information already in the public domain or information available under the Right to Information Act.

Body Corporate are forbidden by Rule 5 of the Draft rules from collecting sensitive personal information unless - (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and (b) the collection of the information is necessary for that purpose. They and "any person" holding sensitive personal information are forbidden from "keeping that information for longer than is required for the purposes for which the information may lawfully be used". This is perhaps a bit vague, since the potential 'lawful uses' are numerous and could be inexhaustible. It is unclear whether "lawful usage" is coterminous with "the uses which are disclosed to the individual at the time of collection". In addition, this rule is framed rather weakly since it does not impose a positive obligation (although this is implied) to destroy information that is no longer required or in use. In addition to the restrictions on collecting sensitive personal information, body corporate must obtain prior consent from the "provider of information" regarding "purpose, means and modes of use of the information".

Rule 7 of the Draft Rules stipulates that a body corporate shall be deemed to have complied with reasonable security practices if it has implemented security practices and standards which require:

a) A comprehensive documented information security programme;

b) Information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

In case of an information security breach, such body corporate will be "required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies".

The Rule stipulates that by adopting the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements", a body corporate will be deemed to have complied with reasonable security practices and procedures.

The Rule also permits "Industry associations or industry clusters" who are following standards other than IS/ISO/IEC 27001 but which nevertheless correspond to the requirements of Sub-Rule 7(1), to obtain approval for these codes from the government. Once this approval has been sought and obtained, the observance of these standards by a body corporate would deem them to have complied with the reasonable security practice requirements of Section 43A.

3. The Failed Legislations

Though the Indian Government introduced a separate bill called "Personal Data Protection Act 2006" to meet the growing need, the Bill is still pending in the Parliament and is likely to lapse. Now Information Technology (Amendment) Act, 2008 has tried to address the demand of the IT industry by specifically introducing two sections, namely Section 43A and Section 72A which specify that they are measures towards "Data Protection". This may make the Personal Data Protection Act 2006 redundant and superfluous (Bajaj, 2009).

However critics opine that the Indian Government should consider enacting a separate data protection law along the lines of Directive 95/46/EC so that the country is in the forefront of legal developments around the world.

There have been attempts all around the world to restrict access of social networking sites to minors but nothing so far has been passed as a law. The Deleting Online Predators Act (DOPA), was introduced in the U.S. House of Representatives in May 2006 by Michael Fitzpatrick (Republican Pennsylvania Representative (R-PA)), passed by a vote of 410 to 15 on July 26 2006. The Act aimed to block access of minors to social networking sites as well as chat rooms (Roush, 2006).

But the bill ended up stagnating in the Senate until the session ended and the Democrats took over, much to the relief of many critics. Unfortunately, that wasn't the last time that such a bill was proposed and a new bill, ambiguously named S.49 for the time being, was introduced to the Senate by Senator Ted "Internet Tubes" Stevens (R-AK) that was similar to DOPA. However none of these bills ever saw the light of day.

Therefore it is an accepted fact that legislation don't really help to curb unhealthy activities as it tend to make it all very stringent.

Conclusion and Suggestions

Social network sites are potentially useful business tools, but only if one approaches them with an adequate amount of caution and common sense. Staying safe on a social networking service is about recognizing some factors and working knowledgeably within a set of simple guidelines. The best solution to protect oneself would be by self-regulation. All major social network services have specific privacy guidelines that are published on their Web sites. Users should take the time to read and understand these documents, since they include the types of information that these sites will reveal or sell to other parties (including spammers). If one is not satisfied with the terms, one should not use the service. Sophos, an internet security and control firm suggested that Facebook should implement additional security measures such as a pop-up confirmation dialogue every time users "Like" something, rather than only when a page already known to be suspicious is involved (Weekly, 2011).

Users should encourage awareness-raising and educational campaigns on the sensible usage of Social Networking Sites. These sites themselves should, where possible, use contextual information to educate people. The Social Networking Sites present several scenarios which were not foreseen when current legislation (such as The Information Technology Act) was created. The regulatory framework governing Social Networking Site should be reviewed; especially review into social networking sites filtering (Hogben, 2007). For addressing Social Networking Site spam similar techniques to those used for e-mail such as anti-spam reputation systems should be developed to eliminate spam comments and traffic. For addressing Social Networking Site Phishing, the best practices promoted by The Anti-Phishing Working Group (APWG) which is the global pan-industrial and law enforcement association focusing on elimination of fraud and identity theft should be adopted (Hogben, 2007).

More research should be carried out in the areas of mobile Social Networking Site, convergence with virtual worlds, misuse by criminal groups and 3D representation and online presence (Hogben, 2007). The investigating, prosecuting and judicial officers also should improve their knowledge and skill to understand the unique subject better which would help in enforcement. Children need to be taught about the harms of the cyber world and ways to counter it. It would deeply help to build up a generation who has been already conditioned to deal with such everyday internet problems. Like quality auditors, Information Security Auditors need to be present in an organization. Presence of Internal auditors shows the awareness of the importance of cyber security measures in the organization. The need for external auditors is to emphasize the constant necessity for updating knowledge, systems and procedures within the organization in keeping with the emerging situations (Srikumar, 2010).

Social networking websites should seek to achieve security through profile tracking and cross-reference, IP tracking, and simple observation. Currently, social networking websites are not taking these steps to protect their users, and they have little, if any, incentive to do so. In the Indian context the ICP should be made liable and not the ISP because the ICPs are in a better position than ISPs to monitor relationships among online identities and Internet Protocol (IP) addresses. Social networking websites should cross-reference information posted by the user in order to check a profile's validity, or to raise red flags. For instance, age verification could be assisted by cross-referencing information provided by the user. Additionally, Facebook and other major social networks with consistently large traffic often use data gathered from users to increase usage and thereby increase revenue. These same websites could easily discover trends, associations, and correlations between content and reports of abuse to prevent future harm. Furthermore, encouragement needs to be given to spread a "Security Culture" in the community which emphasizes on guidance, solutions and mandatory compliance. Such compliance can be brought about by education, accountability, practices and certification.

Apart from the measures indicated above, it is necessary for Corporates and Individuals to be provided with a suitable "Cyber Crime Insurance Programme" (Vijayashankar, 2008) which enable non-experts to off-load their security concerns to the Insurance industry. Currently our system uses IPv4, and provides over four billion unique IP addresses. ICANN (Internet Corporation for Assigned Names and Numbers) is running out of IP addresses to distribute, and is therefore planning to introduce a new system called IPv6, which provides substantially more IP addresses (Espiner, 2008). Although computers are currently being built that incorporate IPv6 compatibility, very few use it. The use of this new system would mean better monitoring capabilities and Internet security may change drastically. There is a silver lining to the regulation and monitoring network who will be better equipped to handle criminals and curtail crime over the internet.

Indian laws governing electronic commerce and data security are not that complex; all that is needed is effective enforcement of the same and to ensure that laws are more stringent and easy to act upon. Social Networking Websites herald the end of passive media and if this development is cautiously used then it would lead to the blooming of inter-connected and informed work force.

References

Aarora, N. (2009, February 02). "Every man's house is his castle": Right to privacy and Information Technology (Amendment) Bill, 2006. Retrieved September 13, 2010, from http://www.neerajaarora.com/every-mans-house-is-his-castle"-right-to-privacy-and-information-technology-amendment-bill-2006/

Aarora, N. (2010, September 8). Cyber imposter created fake profile of President of India. Retrieved May 30, 2011, from http://www.neerajaarora.com/cyber-imposter-created-fake-profile-of-president-of-india/

Articles, English (2011, May 11). Digital Youth Culture and Social Networking. Retrieved June 02, 2011, from http://www.englisharticles.info/2011/05/11/digital-youth-culture-and-social-networking/

Attacks, S. N. P. (2009). Social Networking Phishing Attacks. Retrieved September 14, 2010, from http://www.spamlaws.com/fake-social-networking-sites.html

Bajaj, K. (2009) Data Protection and Cyber Crimes under the Amended Information Technology Act. Retrieved September 7, 2010, from http://www.nasscom.in/...../IT_Act_Amendments_Details.pdf

Brasser, R. (2010). The Social Networking Paradigm Shift and Internet Fraud. Retrieved June 1, 2011, from http://thetargetedgroup.wordpress.com/.../the-social-networking-paradigm-shift-and-internet-fraud/

E-Crime, W. I. (2010). What is E-Crime? Retrieved September 6, 2010, from http://www.ecrimewales.com/server.php?show=nav.8856

Espiner, T. (2008, May 12). ICANN: IPv4 will run out by 2011. Retrieved January 5, 2012 from http://www.zdnet.com.au/icann-ipv4-will-run-out-by-2011-339288828.htm

EU Directive. Retrieved June 29, 2011 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Felt, A. (2007). Defacing Facebook: A Security Case Study. Retrieved June 16, 2011, from http://www.cs.virginia.edu/..../facebook-xss-censored.pdf

Ferris, J. R. (n.d.) Internet Addiction Disorder: Causes, Symptoms and Consequences. Retrieved September 8, 2010, from http://www.files.chem.vt.edu/chem-dept/dessy/honors/papers/ferris.html

G.O.I.-Department of Information Technology. Draft Rules- Reasonable Security Practices & Procedures and Sensitive Personal Information. Retrieved January 8, 2012 from http://www.mit.gov.in/sites/upload_files/dit/files/senstivepersonainfo07_02_11.pdf

Gross, R., & Sweeney, L. (2007). Towards real-world face de-identification, IEEE Conference on Biometrics: Theory, Applications and Systems. Retrieved June 19, 2011, from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4401915

Hogben, G. (2007) Security Issues and Recommendations for Online Social Networks. Retrieved June 22, 2011, from http://ec.europa.eu/information_society/activities/social_networking/docs/enisa_report.pdf

Hosein, I. (2006) International co-operation as a promise and a threat. In: B. J. Koops,& S. W. Brenner (eds.), *Cybercrime and jurisdiction: a global survey* (pp. 217-218). The Hague : TMC Asser, West Nyack, NY.

Lohrmann, D. (2008, January 16). Social Networking Security Risks. Retrieved May 23, 2011 from http://blogs.csoonline.com/social_networking_security_risks

Naavi (2009, November 04). Are You ITA 2008 Compliant? Retrieved September 4, 2010, from http://www.naavi.org/cl_editorial_09/edit_nov_04_09_compliance.htm

Policy, Facebook's Privacy (n.d.). Facebook's Privacy Policy. Retrieved June 16, 2011, from https://www.facebook.com/policy.php

Prensky, M. (2001). Digital Natives, Digital Immigrants. Retrieved June 26, 2011, from http://www.marcprensky.com/writing/prensky%20-%20digital%20natives,%20digital%20immigrants%20-%20part1.pdf

Singh, S. (2012, January 14) Government Nod to Prosecute Google, Facebook, Yahoo. Retrieved January 4, 2012 from http://timesofindia.indiatimes.com/tech/news/internet/Government-nod-to-prosecute-Google-Facebook-Yahoo/articleshow/11482173.cms

Roush, W. (2006, August 07). The Moral Panic over Social-Networking Sites. Retrieved June 20, 2011, from http://www.technologyreview.com/printer_friendly_article.aspx?id=17266

Rules & Policies, eBay (n.d.). Rules and Policies. Retrieved December 28, 2011, from http://pages.ebay.com/help/policies/overview.html

Snow, G. M. (2010, July 28). Statement before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. Retrieved June 16, 2011, from http://newsroom-magazine.com/2010/governance/law-enforcement/fbi-report-social-networking-poses-immense-personal-risks/

Vijayashankar, N. (2008, November 29). Threats to Cyber Security. Retrieved September 5, 2010, from http://www.naavi.org/cl_editorial_08/edit_nov_29_cyber_threat.htm

Ward, M. (2008, January 3). Cyber thieves target social sites. Retrieved June 10, 2011 from http://news.bbc.co.uk/2/hi/technology/7156541.stm

Weekly, Computer (2011, May 13). Facebook security measures do not go far enough, say security experts. Retrieved May 27, 2011 from http://www.computerweekly.com/news/1280095874/Facebook-security-measures-do-not-go-far-enough-say-security-experts