Part V: Social networking and Internet governance

In this issue of netgov Speak, in the lead up to Third Internet Governance Forum, to be held in Hyderbad, India, we bring you a hot topic for debate on governing Social Networking sites. With the proposal of EU to bring forth a new legislation to regular these sites, it opens up the issues that confront lawmakers and law enforcement agencies on one hand to those who campaign for the value of digital freedom on the other.

Is there a need to monitor the content on social networking sites?

On 27 May 2008, the European Network and Information Security Agency (ENISA) issued a position paper for drawing up a new legislation that would regulate social networking sites. ENISA, which was created in 2004 to oversee online security measures in the 27 EU countries, in which it pointed out that social networking sites such as Facebook and MySpace need more regulation to protect their users against security risks. "Social networking sites are very useful social tools but we must make recommendations for how to better protect people from the risks these sites create," said Andreas Pirotti, executive director of ENISA and author of the report. In Pirotti's opinion, network security is under a permanent threat from spammers or criminals. "Internet security is extremely important, considering how much business takes place online now." Some of the threats related to social networking identified by ENISA are related to face recognition, digital dossiers, reputation damage, social engineering attacks on enterprises, phishing attacks, ID theft and others. The report of the organisation includes 19 recommendations to social networks on ways to improve security practices. Among other things, ENISA calls for a regulatory review of social networking frameworks, an increased transparency of data handling practices, more education for users on security, and the discouragement or even banning of social networking in schools.

A study conducted by enterprise IT management company CA and the National Cyber Security Alliance in 2006 found out that the majority of users of social networking sites were not very aware of the security issues involved. 83 percent of them admitted having downloaded unknown files from unknown users and 74 percent said that they were easily providing the personal data online.

Also, a Symantec report issued in 2007 showed that social networking sites offer easy pickings for phishers. The security practices of the respective sites make it easier to invade and to spread attacks to more people.

The booming social networking space and web 2.0 technologies

With more than 130 hugely popular community networking sites, and booming rapidly, social networking on the Internet has taken a new dimension in defining the ethos and culture of the use of Internet. The social

networking spaces have evolved in an organic way and have used several interactive tools including feeds, polls, commenting, sharing, and modular tracking services like birthday tracker, rss feeds, digg it, etc, which allows knowledge to flow freely. This evolution has created a new ethos of knowledge sharing and digital rights for the masses. People no more need to be technically savvy to publish, code or upload content on the Internet. Such a free flow of information from various quarters is not without its set of problems, and potential challenges that face regulators, lawmakers and enforcement agencies, who worry about its potential for misuse.

According to Venkatesh Hariharan, Co-founder of Open Source Foundation of India, "Social Networking Sites are very useful to form communities with like-minded people. For example we have been actively engaged in a community which is against software patents, and a candlelight vigil, using Facebook, and other networking media. This is especially valuable when people are distributed across the country, and globally, online communities makes it possible to mobilise the support at

very short notice, which otherwise is not possible! Even though these communities are asynchronous, they are faster, and more responsive that email discussion lists."

Social networking sites have a huge youth following!

In a survey conducted among the youth in India on the value of social networking sites and their value to the users, the respondents strongly felt that the social networking sites like Orkut, Facebook, Myspace and LinkedIn must not be regulated and it should permit free flow of information. The respondents, however, felt that they should have more control and checks of who could and could not view their profiles and to have a system by which they could regulate who coud access their information.

Kriti Madhukar, a first year college student of Delhi University, is an "Orkutter" who is adept at multi-panel chatting, sharing photos, planning events, sharing music, and discussions, and having fun catching up! She has also experimented with Facebook, Hi5, and says, "social networking space is an important aspect of today's urban youth. We cannot imagine that only less than a decade ago, the Internet was not so robust or even accessible in many parts of the world. It is very important to create more such opportunities for also the rural folks in India, who speak innumerable languages, and once they have access to public Internet, they should immediately be able to join the social networking space."

Social networking sites have also created an empowering avenue for early learners, people who are otherwise not social to explore the world for friendship, learning, sharing, peer support, etc. These social networks have evolved as a result of more openness in accessing and publishing on the net. It has also led to a world of challenges while experiencing the power of freedom of expression. The current debate to examine the privacy and security issues and whether they must be regulated faces many contrasting perspectives. The European Union, as cited above, would like to address several issues and has provided a concrete picture of how to handle the concerns, in the rapidly expanding universe of social networking space.

Sociology of online social networks

Some of the social impacts of networking sites are worth reflecting on. LinkedIn, for example, is a professional, business network, which is used extensively across the world, and in India too, for job scoping and senior executive searches. It is also used to create a network of professional interest and to build alliances. The kind of services that the network provides makes it of different value than that of generic social networking sites that allow gathering in cyberspace based on social aspects, like friendship, interactions, informal dialogues, and peer-to-peer sharing of data, images, audio and video footages, that are now getting more and more prevalent.

One of the key issues that worries parents, teachers and policy makers is whether these online social networking sites are "child safe". The responsibility lies at all levels. Parents have to play a direct role in keeping a watch on their children's behaviour online,

the networking sites should have their norms and standards of what content can be shared, and governments have to be more rigourous in the laws on admissible content, though it is one of the most chalenging assignments. Owners/promoters of the online social networking sites have the responsibility to create mechanisms to vote out unfavourable site, and to block users who post irresponsible materials.

Yet, there remains some key concerns relating to privacy, quality of content, IPR issues, both from the point of view of security and ownership of content. There could be two opposing schools of thought: one, which advocates for no-holds-barred and open sharing, and another that ensures that the community space is "safe, secure, and condusive". The debate thus is very interesting.

Identity issues in social networking sites

Identity thefts is a major issue that worries most users, even in countries where privacy issues are not that seriously taken. There have been instances when intruders have stolen identities and personal information, impersonated and sent out posts that cause serious concerns. The recent Mumbai wifi hacking case, which misused the identity and IP of the person to send out terror mails, is an example of the risks that we are subjected to when nefarious persons steal identities and further their vicious and malafide intents.

The issue is more serious with bankers getting interested to address the privacy issues as well as ecommerce applications wherein the identity thefts are happening in greater numbers. Cybersecurity is still a nascent area of law and administration, and the police departments across the world are gearing up to be responsive and be aware of the nuances of laws of the land, and how they are applicable. A lot of work on awareness creation among the police officers is also essential, as per the views of a Human Rights and Freedom of Expression Activist, who has been associated with advocacy work around the rights of expression.

The debate continues… with more questions than answers!

Readers are invited to share their views/experiences/ new issues to raise, to be part of the debate, on the social and security impacts of online social networking sites. Have your say! Please write to:

response@i4donline.net
info@i4donline.net