Cyber Crimes Against Women: US Legal Regulations And International Perspectives

The United States of America has shown unprecedented internet growth and the resulting cybercrime explosion. A spike in cybercrimes against women in the new millennium was also seen in the US. The policies and conditions of the numerous US hosted internet service providers highlight the fact that freedom of speech and expression, as has been guaranteed in the First Amendment, is given highest priority when policing “offending” contents in the sites. Laws were created one after another, their practical usability and constitutionality widely debated; some stood the Supreme Court's acid test of judicial accountability, some didn't. Nevertheless, none was created for the sole purpose of protecting the rights of women on the Internet.

Hacking can mean unauthorized access to the computer as a server, the computer network, the data stored therein and alteration of such data when defined in legal terms in the US. In general, Hacking is governed by the Computer Fraud and Abuse Act, which is again protected by Title 18, USC 1030. A quick analysis of the provisions will demonstrate that this particular law is intended to protect national security and financial fraud. As such, this Act safeguards “protected computers” more and not private individual’s private data excluding those stored for government purposes.

Consequently, hacking email ids, personal websites, altering and misusing them, etc., is regarded more as an infringement of the privacy of regular cyber users, where unauthorized access to computer data and alteration of the same are used as instruments. As such, personal information of women stored in personal computers, blogs, social networking accounts, email records, blog profiles etc. is highly sorted after targets by miscreants, cyber harassers and those who set up personal enmity with the female victim(s) due to their politics or relationship breakups or even professional as well as personal ego-clashes. The hacking of the former Alaska Governor Sarah Palin's email I d, the then US Vice-Presidential nominee, could be taken as the prime example of women's victimization based on the issues listed above. Her Yahoo account was hacked, and a college student posted private emails online.

In such cases Section 2701 of Chapter 121, USC 18 (Part 1) may be applied as a preventive legislation which makes it an offence when a person

(a) intentionally accesses without authorization, a facility through which an electronic communication service is provided, or in other words attacks the computer and computer networks as a whole and disrupts the right to use the electronic communications; or

(b) intentionally exceeds an authorization to access that facility, or in other words hacks and cracks in other’s data without the owner’s permission; However, it is interesting to note how the language of the second paragraph of this provision suggests punishment depending upon the motive of the accused. As such, when the ‘offence’ is done with a motive to gain for “commercial purposes, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or any State”, which may very well justify cases of hacking and morphing female

victim’s pictures and information for online commercial adult entertainment industry, or even defamation of the female victim and humiliating her in front of large internet audience etc. The law provides monetary fine and imprisonment sentence ranging from 5 to 10 years. In other cases when such activities are not done for the purposes as stated above, and done for rather teasing the victim, harassing etc, the law provides punishment with fine and imprisonment which may range to 1 to 5 years depending upon whether the offence is a first offence or has been committed after a conviction. Thus, it could be seen that both civil as well as criminal remedies are available for offences of this nature. However, it will depend upon the prosecution largely to establish the case as fit for civil or criminal remedy. These legislations may play as safety valves along with the principles of First Amendment limitations when hacking is done for furtherance of defamation including tampering the document and publishing the hacked content for portraying the victim in an indecent manner and labelling the victim in obscene fashion.

Provisions against stalking

Since the beginning of 90's, the United States Congress had been experimenting with various laws to prevent cyber stalking and associated abuse. Cyber bullying received its first formal legal sanction in the US by Michigan Criminal Code, in 1993. This clause incorporated the word 'harassment' from a new angle to cover actions relating to stalking. Harassment was thus defined as “conduct directed toward a victim that includes repeated or continuing unconsented Contact that would cause a reasonable individual to suffer emotional distress, and that actually causes the victim to suffer emotional distress”. Unconsented contact meant sending unsolicited and unwanted mail or electronic communications to the victim. It is notable that offline stalking has long been recognized in the US, and the California Penal Code was the first law to identify harassment as a criminal offense through telecommunications (excluding the internet). This was the first anti-stalking legislation of the US, and it charged a person guilty of stalking when the accused “willfully and maliciously and repeatedly follow nor harass another person and make credible threats with the intent to place that person in reasonable fear for his or her safety or that of an immediate family member”. The Alaska Code in section 13-2921 penalizes harassment when the harassor interacts or triggers contact with another person through verbal, electronic, mechanical, telegraphic, telephone or written means in a manner that causes harassment.

the California Civil Code also discusses the issue of stalking under section 1708 which holds a stalker responsible for harassing / threatening / abusive messages via electronic communications along with other means of conveying the harassment message. Various US states have established similar laws as those mentioned above to discourage and protect abuse by means of information technology. None of these acts apply to the word 'cyber bullying' and we find it to be a conspicuous mistake. The statute 'harassments' clauses have been revised in several of these laws to change the legal requirements for cyber-stalking prevention. Cyber stalking, however, does not automatically have to be associated with cyber harassment; but it needs to be taken as another type of cyber harassment. The points may be backed by the views expressed in the United States Department of Justice's 1999 Report on cyber stalking prepared by the Attorney General. The report states as follows:

Although there is no universally accepted definition of cyber stalking, the term… refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behaviour that an individual engages in

repeatedly, such as following a person, appearing at a person’s home or place of business, making harassing phone calls,leaving written messages or objects, or vandalizing a person’s property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim’s immediate family; and still others require only that the alleged stalker’s course of conduct constitute an implied threat. While some conduct involving annoying or menacing behaviour might fall short of illegal stalking, such behaviour may be a prelude to stalking and violence and should be treated seriously (Para 5).

It is not always essential that such harassing behavior should mean cyber stalking. The present statutes that were discussed above therefore denote a very wide arena in the name of cyber stalking.The ambiguity resulting from the use of harassmentrelated languages in the U.S. provincial legislatures aimed at preventing cyber bullying was effectively put to rest by the implementation of the 'Violence against Women and the Department of Justice Reauthorization Act, 2005.' This Act was the first legislation to penalize cyber stalking and found the vulnerable victims to be women.

Provisions against cyber bullying, hate speech and cyber defamation of women

A perusal of the abovementioned stalking and harassment laws will reveal that U.S. provincial and federal legislatures reject harassing, irritating, and threatening Internet and telephone communications. Prevalent cyber cultures such as ridiculing women with harsh taunting languages together with First Amendment guarantees elasticity helped develop cyber bullying for women and cyber hate speech targeting women as a rapidly increasing cyber offense towards women. Kathy Sierra's case is a fascinating example of how women bloggers are abused because of their gender in the US cyberspace. The hardest reality is that such cyber hate and harassment against women in the U.S. is rife not only for blogs, but also for women on social networking sites, chat rooms and other cyber hangouts like YouTube, personal websites etc.

The reason for the rise of cyber-hate speech and bullying targeting women is often felt to be the loose definitions of the protections of First Amendment. Additionally, with the advent of time, the extension of First Amendment rights has influenced nearly all public communications tools, such as motion pictures, radio and television shows, print media, and even the digital communications network, including mobile phones, SMS and internet.

We recognize that it may not be possible in the US to control non-sexual offensive speech against women that does not produce particular threat but that provides ample scope for publicly demeaning women. Women's rights in cyber space are often ignored when it questions the rights guaranteed by the traditional' internet languages' under the First Amendment, which often contain women's slang remarks. It remains much like a question of cyber space ethics, and not a topic to be governed by law. Because of the' Miller test'-verdict, it often seems that young generations of internet users, including teenagers and young adults, have relaxed the watermark for slang languages that target women to be 'obscene' to a large extent. In this regard, the absence of any particular gender-sensitive prohibitive provisions also allows women victims to seek justice by applying Civil Rights provisions under Title 18, USC, Chapter 13 of Section 1, along with other relevant provisions on defamation and abuse of communications that we have mentioned above.