Chapter 5
Legal Treatment of Cyber Crimes Against Women in USA

CHAPTER OVERVIEW

US, is one country, which started the evolution of the Internet and also the first to be affected and the first to retaliate to the ugly side of the Internet, the cyber crimes. US saw a sea of growth in the cyber crimes against women and created new laws to mitigate such crime and prevent future victimization. In this chapter, we discuss about various laws developed by the US to prevent cyber victimization of women as well as conventional laws that were applied to protect women in cyber space. Regulation of crimes in cyber space such as cyber bullying, cyber stalking are examined in detail. The issue of privacy in cyber space vis-à-vis the laws related to that are identified and analyzed.

5.1 INTRODUCTION

The United States of America evidenced rapid growth of the internet and the subsequent eruption of cyber crimes. Also in the US a surge in the cyber crimes against women was seen in the new millennium. As per the WHOA statistics of 2000,[1] among 353 respondents, 87% victims of cyber crime were females and 68% of the harassers are male and only 27% harassers were females. As per this statistics, the victimization begun mostly through emails (39.5%), message boards (17.5%) and also chat rooms (15.5%), other than Instant Messaging (IM) or websites. The 2009-2010 statistics of WHOA shows that among 349 respondents, women victims still remained a majority who formed 73% of the victim ratio. Only 27% men were reported to be harassed. The statistics showed that 44.5% harassers were male and

DOI: 10.4018/978-1-60960-830-9.ch005

36% of the harassers were females. The major crime hubs still remained email communications (34%); followed by Instant Messaging (IM), chat rooms etc.[2]

The policies and terms of the various US hosted internet service providers[3] highlight the fact that freedom of speech and expression, as has been guaranteed in the First Amendment, is given highest priority when regulating "offending" contents in the sites (Citron, 2009b). Various literature reviews would show that the birth of various cyber crime regulating laws in the US, were marked by huge debates over probable clashes of constitutional rights and confusions. Laws were created one after another, publicly debated over their practical usability and constitutionality; some stood the acid test of judicial accountability by the Supreme Court, some didn't. However, none was created with a sole purpose to safeguard women's interests in the internet. In the following segment we will analyze the applicability of existing penal laws for the cause of prevention of online victimization of women.

5.2 REGULATIONS FOR MODIFICATION OF CONTENTS AND RELATED ACTIVITIES

Hacking when described in legal terms in the US, may mean unauthorized access to computer as a machine, the computer network, the data stored therein and modification of such data. Hacking in general is regulated by the Computer Fraud and Abuse Act, which is again encompassed by Title 18, USC 1030. A brief examination of the provisions therein will show that this particular legislation is made for national security and protecting financial frauds. As such, this Act safeguards "protected computers" more and not private individual's private data excluding those stored for government purposes.[4] Hence, hacking email ids, personal websites, modifying and misusing them etc, are considered more as invasion to privacy of common cyber users where unauthorized access to computer data and modification of the same are used as tools. As such, personal information of women stored in personal computers, websites, social networking profiles, email data, blog profiles etc are highly sorted after targets by miscreants, online harassers and those who set up personal enmity with the female victim(s) due to her ideologies or romantic breakups or even professional as well as personal ego-clashes. The hacking of the email id of the former Alaska Governor Sarah Palin, the then US Vice-Presidential nominee, could be taken as prime paradigm of victimization of women based on the above mentioned issues. Her Yahoo account was breached and private emails were posted online by a college student (O'Connell, 2008).

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.[5] In other