

Chapter 8

Cyber Crime Against Women and Regulations in Australia

CHAPTER OVERVIEW

This chapter deals with the legal regulations that protect Australian women in cyber space. Various issues that are discussed in this chapter are: Cyber harassments including hacking and hacking related offences against women and regulatory provisions, stalking women and the concerned laws, harassments, threatening, blackmailing, defamation and related laws. Legal approach to problems of 'forced pornography', obscenity and the liability of the ISPs as per the Australian laws are also discussed. The chapter ends with a discussion. In this chapter a strong emphasis is made on the need for new laws that will protect Australian women in cyber space.

8.1 INTRODUCTION

Cyber crime against women in Australia deserves a better analytical treatment from law and justice machinery as well as cyber criminologists, socio-legal researchers and activists. Ironically, most surveys show economic loss as the highest rated cyber crime happening in Australia, closely followed by virus infections, hacking, child pornography and cyber bullying among children (Rust, 2008; Arias, 2007, Roberts, 2008). Even though stalking has been enlisted as a crime,¹ besides other general cyber crimes listed above, we could find no good survey results of stalking by intimate partners to women or cyber victimizations of women including cyber bullying, privacy-penetration, cyber gender sensitive defamation, forced pornography etc. More emphasis is given to child grooming, crimes against children and

DOI: 10.4018/978-1-60960-830-9.ch008

youth belonging to the age group of 16-19 and identity theft (in relation to monetary crimes especially) in Australia (Roberts, 2008). In Australia, century old laws have been amended and adjusted to prevent cyber crimes and cyber borne crimes against the society as a whole. Even though victimization of women have taken a technical turn since long, little thought has been given to draft gender sensitive penal laws to save women from being abused and tormented. However, the good news is, several such 'adjusted' laws do help women victims while in 'cyber –distress'. In the following sections, we will discuss some of these federal and provincial laws, which are being used to prevent and protect cyber victimization of women in Australia and the government, and non-government initiatives, which are being taken to prevent cyber harassments of women.

8.2 CYBER HARASSMENTS

As per our typology discussed in the chapter 2, hacking may constitute a separate gender sensitive cyber crime even if it is not necessarily related to financial crimes. Hacking may lead to various other cyber crimes such as destroying personal information and blocking others to contact the victim, leaving her completely isolated in a cyber - imprisonment state; accessing the individual's personal and professional information and creating cloned web profiles to impersonate the victim; misusing the information of the female victim(s) including her pictures for illegal financial gains, especially by making her website / public profile look like hard core adult entertainer's profile; intentionally destroying her professional identity and make her a 'laughing stock', etc. As such, these sorts of harassments, which involve hacking, hacking and cloning, hacking and morphing, hacking and impersonation etc, are well controlled by the Federal Criminal Code Act, 1995, as has been amended by Cyber Crime Act, 2001.² The Cyber Crime Act, 2001, prohibits unauthorized access, modification or impairment of computer data, which is done with intent to commit a serious offence under section 477.1,³ 2, 3, and 4.⁴ However, these provisions are used maximum for preventing crimes against governments and corporations (Smith, Grobosky & Urbas, 2004). We found no literature to show that these provisions have also been used to prevent hacking and hacking related problems targeted towards women.

According to the Australian laws, hacking and hacking related problems are construed more as an offence towards the computer as a machine, towards the network and towards the government and financial data. In short, hacking is termed as "computer offence" done through 'carriage service.'⁵ These provisions especially when read with provisions regarding invasions to privacy under the Privacy Act, 1988, may well be used as preventive legislation to prohibit harassing women when hacking and hacking related activities are done to publicly humiliate the victim by publishing her personal information, religious, feministic and sexual opinions and beliefs. Even though the main objective of the Privacy Act, 1988, is to secure financial, health and government identity related information, "sensitive records" as has been interpreted by Section 6 of the Act, could be extended to cover information or opinion about any individual's racial or ethnic origin, political opinion and belief, membership to unions and associations, religious opinions and favoritisms, sexual practices and preferences, criminal records, health records and also genetic records. It is presumed that women and men as well, may be victimized when the harasser hacks and cracks such information and uses it to fulfill revengeful or other harmful activities.

However, it must be noted that Privacy Act, 1988, does not provide protection to information which are generally available to public, including information "however published".⁶ In such cases the provisions enacted in divisions 477 and 478 of the Criminal Code Act, 1995, must be used to protect women

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cyber-crime-against-women-regulations/55536

Related Content

A Model for Hybrid Evidence Investigation

Konstantinos Vlachopoulos, Emmanouil Magkos and Vassileios Chrissikopoulos (2012). *International Journal of Digital Crime and Forensics* (pp. 47-62).

www.irma-international.org/article/model-hybrid-evidence-investigation/74805/

A Blind Image Watermarking Scheme Utilizing BTC Bitplanes

Chun-Ning Yang and Zhe-Ming Lu (2011). *International Journal of Digital Crime and Forensics* (pp. 42-53).

www.irma-international.org/article/blind-image-watermarking-scheme-utilizing/62077/

Fingerprint Liveness Detection Based on Fake Finger Characteristics

Gian Luca Marcialis, Pietro Coli and Fabio Roli (2012). *International Journal of Digital Crime and Forensics* (pp. 1-19).

www.irma-international.org/article/fingerprint-liveness-detection-based-fake/72321/

Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks

Dennis K. Nilsson and Ulf E. Larson (2011). *New Technologies for Digital Crime and Forensics: Devices, Applications, and Software* (pp. 115-128).

www.irma-international.org/chapter/conducting-forensic-investigations-cyber-attacks/52848/

Visibility Control and Quality Assessment of Watermarking and Data Hiding Algorithms

Patrick Le Callet, Florent Autrusseau and Patrizio Campisi (2009). *Multimedia Forensics and Security* (pp. 163-192).

www.irma-international.org/chapter/visibility-control-quality-assessment-watermarking/26993/