Seminar session 6: Principles of Digital Forensics and Cyber Law – Case Reports

End of Module Assignment: Expert Report

- This is final module assessment
- This accounts for 40% of you final module mark. Word count is 2,500 words.
- Your task is to produce an expert report on all possible aspects of cyber-identity theft that apply to the country in question.
- You will have to carry out extensive independent research.
- The report should have appropriate headings, containing the following aspects, with the applicable grading criteria highlighted for your information:
  - ➔ Knowledge and Understanding weighted at 30%
  - ➔ Use of relevant sources weighted at 10%
  - ➔ Criticality weighted at 30%
  - ➔ Use of relevant sources weighted at 10%
  - ➔ Presentation and Structure weighted at 10%
  - ➔ Academic Integrity weighted at 10%

What is Cyberbullying:

- Threating someone during online communication using electronic devices
- No legal definition of cyberbullying
- No specific anti-cyberbullying legislation
- Can be dealt with other criminal and civil laws
- Can have potential serious consequences for the victim
- Cyberbullying could appear as a minor incident but could have serious and long-term consequences

Types of Cyberbullying:

- 1 – Mobile-phones and other mobile devices
  - ➔ Mobile devices or other electronic device could be used to send abusive or threaten messages
  - ➔ Messages could be text, video, photo or a phone calls
  - ➔ It includes anonymous text messages sent using Bluetooth
  - ➔ It can be a disturbing phone video footage or physical attacks on people or ‘happy slapping’

- 2 – Email
  - ➔ It includes abusive or threatening emails sent to a targeted person

➔ It can be sent to a group of person to encourage or incite other to take part in the sending of abusive emails or phone messages to single person

- 3 – Instant Messenger & Chatrooms
  ➔ This medium is also used to send abusive messages to encourage others to send abusive or threatening messages to individual.

- 4 – Social Networking sites
  ➔ This is the most common medium used in cyberbullying
  ➔ It includes crating profiles or contributing to pages on social networking sites, such as Facebook or Twitter to abuse individual
  ➔ Posting images or emails of others on the social networking sites without their permission
  ➔ Assuming the identity of others by holding their account details
  ➔ Posting messages on their behalf
  ➔ Abusing or harass others also called 'Trolls'

- 5 – Interactive gaming
  ➔ Use of games to abuse or threaten others
  ➔ This includes locking people out of games, spreading rumours about others
  ➔ Adding email addresses and profiles of others to gaming mailing lists
  ➔ Hacking into other accounts

- 6 – Sending Viruses
  ➔ The use of viruses sent to others to corrupt or delete information on their personal computers

What to do if becoming a victim of Cyberbullying?

- Decision depends upon the location where it happens
- If its during school hours and not serious, could be dealt with in school
- School teachers have strategies in place which could be used to deal with the problem effectively
- All schools are required to have an anti-bullying policy either under the School Standards and Framework Act 1998 or
- Under the Education (independent School Standards) regulations 2003
- In other serious circumstances, police should be contracted immediately

Cyberbullying and the law

- Cyberbullying and bullying are not specifically criminal offences
- There are criminal and civil laws that can be used
- These include:
  - ➔ Protection from Harassment Act 1997
  - ➔ The Malicious Communication Act 1988
  - ➔ The Communications Act 2003
  - ➔ The Public Order Act 1986
  - ➔ The Education and inspections Act 2006 (EIA 2006 – for staff and Teachers to confiscate items from pupils, such as mobile phones)