Chapter 2 summaries

Online crime

- Technology has facilitated the commission of some quite traditional crimes such as theft and fraud.
- New crimes such as hacking have also emerged due to the prevalence of technology.
- Cybercrime does not have a single definition but is an evolving concept as dependent on the technology which facilitates it as the activities it involves.

Responses to cybercrime

- There are a number of ways to respond to online behaviours that are considered unacceptable, whether illegal or not. These include legal, rule based, technical, or user enforced responses.
- The legal route is important particularly for behaviour that has an offline impact.
- Rule-based systems can work well if non-compliance can be detected and suitable penalties or exclusions implemented.
- Technical restrictions can prevent certain behaviour.
- User control can be an important social deterrent.
- No one of these offers a complete solution.
- Taken together they appear to offer an effective response to most online activities.

Soft law and adaptive governance

- International law has shown that a soft law approach using guidelines and norms may be more effective than a hard law or regulatory approach.
- A system of adaptive governance, where policy making is not definitive but experimental and governance is seen as a learning and changing process is suited to online governance.

 Back to top

- In some fields, soft law has been used as a precursor to hard law. This may not be a possible route for the regulation of online behaviour due to the inherent dynamic of change online.

Governance

- The governance of the internet is unlikely to take the form of some Grand Internet Treaty.
- It is more likely that a framework of governance will emerge and may vary depending on the nature of the activity engaged in.
- The digital tracks of all of our online activity are likely to lead to changes in our behaviour.
- The relative merit of enhanced services and the consequent impact on privacy creates a dichotomy in which we trade convenience for privacy.

Social networks

- Social networks have blurred the distinction between private and public communication.
- The combination of social networks and the mobile phone has provided a constant connectedness between a vast number of people who are in continuous communication.
- This pairing of technology has diminished the digital divide but also opened up the possibilities for cybercrime on a larger scale.
- The risks associated with storing so much personal information online and being in constant connection with the internet are matched by many positive and socially constructive benefits.

 Back to top