**Ethical, social and privacy issues in information systems**

**Introduction to ethics**

Ethics are moral principles that define a individuals choices and behavior.

* The distribution of money, authority, rights and obligations is under threat because information systems have the power to create social change, which all factors above can provide.
* ICTs can be utilized to commit crimes, threaten values as well as achieve social progression.

**Ethical** issues can occur in the areas of:

* **Internet and commerce** – construction, integration distribution of information.
* **Personal privacy** – having to protect intellectual property.

**Social** issues occur in the areas of:

* Posting pictures, making status updates on Facebook, telephone calls all reveal information about you, this has privacy implications.

**Political** issues occur in the areas of:

* Government monitoring social networking sites, telephone calls, text messages for the purpose of crime prevention may lead to political unrest and citizens not trusting the political party in power.

**Five moral dimensions of the information age**

1. **Information rights and obligations** – what information rights possessed by individuals and organizations can be protected?
2. **Property rights and obligations** – how is it possible to be protect intellectual property (IP) in a digital society in which tracing and accounting for ownership is difficult?
3. **Accountability and control** – who is held responsible for harm done to individuals, collective information and property rights?
4. **Systems quality** – What specific level of data and systems quality should we demand to protect individuals rights and safety?
5. **Quality of life** – what values should be preserved in the knowledge society? Which institutions, cultural values and practices should be protected?

**Ethics principles**

**Golden rule** – Treat others the way you liked to be treated.

**Immanuel Kant’s categorical imperative –** if an action is not right for everyone to take, it is not right for anyone e.g. if everyone did this would the business survive.

**Risk aversion principle** – take action producing the lowest possible damage or potential risk.

**Utilitarian principle** – take action achieving the greatest possible output or result.

**The slippery slope –** if the action cannot be taken repeatedly, it is not right to take at all i.e. a single action may bring a small acceptable change now, but if repeated it would bring unacceptable change in the long run.

**Information systems and privacy**

**Privacy** is the right for individuals to be free from surveillance and not be observed by other parties.

**Cookies** – data stored as a small text file within the computer’s browser, which identifies and authenticates the user as well as tracking their visits to the website.

**Spyware** – software secretly running on the user’s computer with the intend of doing minimal surveillance without the consent of the user.

**Opt-out model** – allows the business to collect personal information about the consumer, until the user requests to discontinue the collection of their data.

**Opt-in model** – business will only collect personal data with the approval of the user.

**Non-Obvious Relationship Awareness (NORA)**

**NORA** technology retrieves information from different sources to discover unclear and nonobvious relationships e.g. a job applicant for a bar is discovered to share a telephone number with a known criminal, this can issue an alert to the hiring manager.

**Property rights: Intellectual Property (IP)**

**IP –** the work of individuals or organizations that required special knowledge and understanding.

**Trade secrets –** a formula, pattern or compilation of data – provided it is not based on information on the public domain.

**Copyright** – a grant protecting the unauthorized use, duplication or distributing of the intellectual property of the original author throughout his/her lifetime and an additional 70 years after their death.

**Patent** – the official right granted to an inventor to use, duplicate or distribute his/her invention for a period of 20 years.

**Information systems and liability laws**

**Examples:**

* If a person is injured by a machine controlled by software, who is liable?
* Should a social networking platform like Twitter be held liable for postings that are anti?
* When credit card information are compromised and individuals and businesses are harmed who is liable?

**Social costs of introducing ICT**

* **Cyber Crime** – may fail victim to identity theft, ransomware attacks, etc.
* **Reduced response time to competition** – technology evolves quickly and firms will take a while to adjust to changes.
* **Computer abuse** – computers utilized to their maximum capability might not be illegal but may raise ethical concerns e.g. junk mail, spam.
* **Unemployment** – technological changes to the production line might leave unskilled workers redundant.