10. Ethical, legal and environmental impacts of digital technology.

Ethics - the branch of philosophy that is concerned with right and wrong. What is good for an individual and what is good for society as a whole? Developments arising from computer science and the resulting digital technologies produce ethical implications for individuals and society. These implications are not always obvious and sometimes lead to unanticipated problems.

The Digital Divide

The digital divide is a term that refers to the gap between populations that have full access to modern information and communications technology, and those who have restricted access. It is used mainly to describe the split between those with and those without broadband Internet access.

The divide traditionally exists between those in cities and those in rural areas; between the educated and the uneducated; between socioeconomic groups; and, globally, between the more and less industrially developed nations. Even among populations with some access to technology, the digital divide can be evident in the form of lower-performance computers and lower-speed connections.

The next billion people coming online will do so from cheap, mobile phones. While the cost of phone services is falling globally, fixed broadband, typically more reliable and faster than cellular connections, is becoming more expensive in the poorest countries.

Some UN statistics from 2015

- For the least developed countries, the average broadband cost grew by more than 30%, “a sharp increase that will certainly not improve the already very low uptake of fixed-broadband in the world’s poorest countries.”

- 43.4% of the world’s population will use the internet in 2015, but that figure falls to 9.5% for the least developed countries

- women in low and middle income countries are 21% less likely to own a mobile phone, helping perpetuate inequality between men and women.

- 8% of females will have used the internet in 2015 compared with 11.3% of males

The UN has set goals for broadband services to cost no more than 5% of average monthly incomes in developing countries by 2020 and to achieve gender equality among Internet users by 2020.

Do you think achieving these the goals will be enough to close the digital divide? Who should provide the technology and meet the cost?

The World Bank's 'World Development Report 2016: Digital Dividends' summarises (http://www.worldbank.org/en/publication/wdr2016)

"Digital technologies have spread rapidly in much of the world. Digital dividends, that is, the broader development benefits from using these technologies, have lagged behind. In many instances, digital technologies have boosted growth, expanded opportunities, and improved service delivery. Yet their aggregate impact has fallen short and is unevenly distributed. For digital technologies to benefit everyone everywhere requires closing the remaining digital divide, especially in Internet access. But greater digital adoption alone will not be enough."

What other measures will be required to close the digital divide?

Some example discussion topics

Drones.

The idea of remotely controlled unmanned vehicles flying through the air either raises concerns over personal privacy, or leads us to consider citizens who live in fear of drones used for military purposes.

NASA have successfully tested a prototype system that allows unpiloted drones to detect and avoid other aircraft in their midst. The agency's drones are able to sense when something was in their flight path and make adjustments on their own.

In the UK the Civil Aviation Authority is warning that drones being flown as high up as 2,000ft are putting passenger aircraft in danger. Drones can be used to monitor pollution levels and e.g. to track wildlife poachers. Should their use be controlled?

Self-driving cars?

Standard features on many ordinary cars include intelligent cruise control, parallel parking programs, and even automatic overtaking—features that allow you to sit back and let a computer do the driving.

Many car manufacturers are beginning to design cars that take the driving out of your hands altogether. It is claimed that these cars will be safer, cleaner, and more fuel-efficient than their manual counterparts, but can they ever be perfectly safe?

The idea of the computer controlling the car raises some ethical questions. How should the computer be programmed to act in the event of an unavoidable accident? Should it minimize the loss of life, even if it means sacrificing the occupants, or should it protect the occupants at all costs?

Artificial Intelligence.

Google's AlphaGo computer learned to play Go at an expert level by watching people compete and then simulating millions of its own games against itself. It eventually became good enough to defeat even the best software that had been pre-programmed to play Go. In October, Google pitted AlphaGo against Fan Hui, the best player in Europe. They played five games. The computer won all of them. In 2016 AlphaGo defeated multiple world champion Lee Sedol, 4 games to 1.

Neuromorphic chips configured more like brains than traditional chips make computers far more astute about what is going on around them - computers that learn by experience. New generation robotics can react without pre-programming. The possibility of creating thinking machines raises a host of ethical issues relating both to ensuring that such machines do not harm humans and to the moral status of the machines themselves. If something goes wrong who is responsible - should it be the robot's programmer, designer, manufacturer, human overseer or his superiors?

Issues of privacy and cybersecurity

Causes of loss of privacy;

- The monitoring of online activity, including browsing histories and use of social media.

Consider. In 2014, the world discovered that US security agency NSA had been spying on the communications of millions of its own citizens. In 2014 the UK government amended the Computer Misuse Act to provide a new exception for law enforcement and GCHQ to hack without criminal liability. This was done without public consultation or any debates over mass surveillance.

- The interception and reading of email messages.

One ethical problem that relates to the private communications of an individual involves the interception and reading of email messages which is often justified in terms of security.

- Distribution of databases storing personal information.

The individual may not be aware of the extent of the personal information being distributed, or who has access to the database, or whether the information is accurate.

Consider. Genome-based treatment, based on wider and cheaper availability of genome data, will provide new and personalised ways to fight life-threatening diseases, although privacy risks associated with data storage of genome data will invariably arise, particularly as such databases are often shared for security reasons (for example, between international police forces), increasing the possibility of hacking or abuse by authorities.

- Theft of private information by hackers.

In the handling and processing of private and personal information organisations are confronted with several ethical issues:

November 2014 – hackers leak a release of confidential data from Sony Entertainment, including personal information about employees and their families, salaries, internal emails and copies of unreleased films.

- Deciding the scope of personal and private information they can gather.
- The confidential treatment of such information.
- The accuracy of information – who checks that the information is correct.
- The purposes for which various categories of information may be used.
- The rights of a person - question of consent?

February 2016 – there was confrontation between Apple and the FBI over a dead terrorist's iPhone. The FBI wants Apple to write new code that would unlock an iPhone belonging to a dead terrorist. Apple is refusing, arguing that they should not be forced to weaken the iPhone's encryption in the name of national security, as this would compromise the privacy of its customers and the strength of its product security?

Codes of conduct

A code of ethics, or code of conduct, defines acceptable behaviour within an organisation. Higher standards are generally promoted when a code of ethics is accepted and followed by members of an organisation. It is useful as individuals working for the organisation have a benchmark upon which they can judge their own behaviour and that of others.

Informal and formal codes

Most small organisations do not have a formal written code of ethics and instead rely on senior members of staff to lead by example, showing what acceptable behaviour is. Members understand the informal code by observing how senior members conduct themselves, e.g. the type of language used in emails and behaviour towards clients.

Formal codes are written documents that outline expected behaviours within an organisation. Formal codes of ethics are usually enforced by the threat of disciplinary action should the code not be adhered to. Each code of ethics is different and usually reflects an organisation's ethos, values and business style. Some codes are short and set out general guidelines, whereas other codes are large documents that include a variety of aspects relating to an organisation's values, ethics, objectives and responsibilities.

An individual's own personal code

An individual's own personal code often supersedes the bare minimum requirements of an organisations ethics code. An individual's own personal code will vary from person to person as they choose to act upon their own ethical standards in their everyday actions.

Legislation relevant to computing

Many pieces of legislation govern the use of computer systems. Relevant examples of legislation include:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000

Data Protection Act 1998

The Data Protection Act 1998 (DPA) was put in place by the Government in response to growing concerns about the amount of personal data being stored on and processed by computer systems. Organisations that store and process personal data are required to register with the Information Commissioner, who is the person responsible for the DPA. Organisations must register information on the type of data they wish to store and why it is being collected.

Organisations are required to adhere to the eight principles of the DPA. These specify that personal data must be:

- processed against loss, theft or corruption
- accurate and where relevant kept up to date
- adequate, relevant, not excessive
- prevented from being transferred outside EU to countries without adequate provision
- fairly and lawfully processed
- processed within the rights of subjects
- deleted when no longer needed
- used only for the purpose collected

There are a number of exemptions from the DPA. These include:

- the prevention or detection of crime
- the capture or prosecution of offenders
- the assessment or collection of tax or duty
- personal data by an individual for the purposes of their personal, family or household affairs
- national security and the armed forces
- personal data that is processed only for journalistic, literary or artistic purposes
- personal data that is processed only for research, statistical or historical purposes
- personal data relating to an individual's physical or mental health
- personal data that consists of educational records or relates to social work
- personal data relating to human fertilisation and embryology
- adoption records
- statements of a child's special educational needs
- personal data processed for, or in connection with, a corporate finance service
- examination marks and personal data contained in examination scripts

Computer Misuse Act 1990

When the use of computer systems became widespread, the Computer Misuse Act 1990 (CMA) was put in place to help combat issues arising from their misuse.

The CMA makes it an offence to:

- access data without permission, e.g. looking at someone else's files
- access computer systems without permission, e.g. hacking
- alter data stored on a computer system without permission, e.g. writing a virus that deliberately deletes data.

Freedom of Information Act 20000

The main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to have this information.

Most countries operate some form of freedom of information law. In the UK it is the Freedom of information act 2000. The Act provides public access to information held by public authorities in two ways;

1. public authorities are obliged to publish certain information about their activities;
2. members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.

There are some exemptions, including information held for criminal investigations or relating to correspondence with the royal family and where disclosure may cause a specific type of harm, such as , endangering health and safety, prejudicing law enforcement, or prejudicing someone's commercial interests.

Environmental impacts

The technologies we use every day consume a lot of resources and power and can present health hazards such as obesity and RSI arising from technology addiction.

Building the hardware can cause harm to the environment, including air, water, heat and noise pollution arising from manufacturing processes and the use of non-renewable resources, including precious metals such as gold used in circuitry.

Carbon emissions are released into atmosphere when electricity created from burning fossil fuels is used. Creating electricity takes a lot of resources, and it can be expensive to use it. It is sensible to reduce how much you use, by taking measures, such as:

- Turning off computers and peripherals when not in use.
- Adjusting the settings of your power options to help minimise power consumption.
- Choosing more energy efficient and environmentally friendly options;

    - Laptop computers use 75% less power than desktop machines.
    - Monitors account for up to half of the energy used by a computer, and the larger the monitor, the more power it uses.

- Ink jet printers use about 90% less energy than laser jets.
- Any product that earns the Energy Star label uses 30 to 75% less electricity than a standard product.

Landfill

Old computers get thrown out when they become out dated. They contain all sorts of hazardous materials that need to be disposed of using special methods; otherwise the waste would become landfill.

Most electronics contain non-biodegradable materials, and heavy metals and toxic materials like cadmium, lead and mercury. Over time, these toxic materials can leak into the ground, where they can contaminate water, plants and the animals that live around the area. Many countries have banned technology products from landfills.

Increased populations

The negative impacts of technology on society include increased pollution and the depletion of scarce resources. A further negative impact arises from improving health research helping people to live longer, resulting in increases in population.

This is good news for people in developed countries, but causes problems in developing countries that may not be in a position to access the health care benefits brought about by technology. In these countries mortality rates remain high, food is scare and health care is poor.

To repair or re-cycling?

Before throwing away old computers, or mobile devices, consider repair or re-cycling. There are many charities that will try to refurbish and repair old computer equipment and then donate the equipment to worthwhile causes, either at home, or abroad.

Repair pro-longs the life of the equipment, delaying the need to manufacture a replacement. Re-cycling is also an environmentally friendly solution that allows components, such as precious metals, to be retrieved and re-used.

Before donating a machine for repair or re-cycling it is important to remove all of your files and data from it. The recycle bin only partially removes the information - you need to run a special program that erases your hard drive.

Paper and packaging waste

You can reduce waste paper by thinking twice about printing documents, email messages, pictures, and things you find on the Web. Buy paper that is made from recycled products and recycle the paper that you do use. Software companies are reducing their waste by offering their products as an online download instead of selling it in a box.

Positive impacts of technology on the Environment

Advances in computer technology have produced many positive impacts on society, including;

- In the development of new materials and processes that are sustainable and do not harm the environment.
- Enabling the study of our environment to better understand how it works and the impact of our actions on it
- Smarter technologies that respond to how we use them and adjust themselves to reduce their environmental impact
- Helping experts from all fields share their research, experience and ideas to come up with better solutions.
- Communications that reduce the environmental impact people would normally cause from traveling
- Improved education, including distance learning and visual learning using integrated technologies.