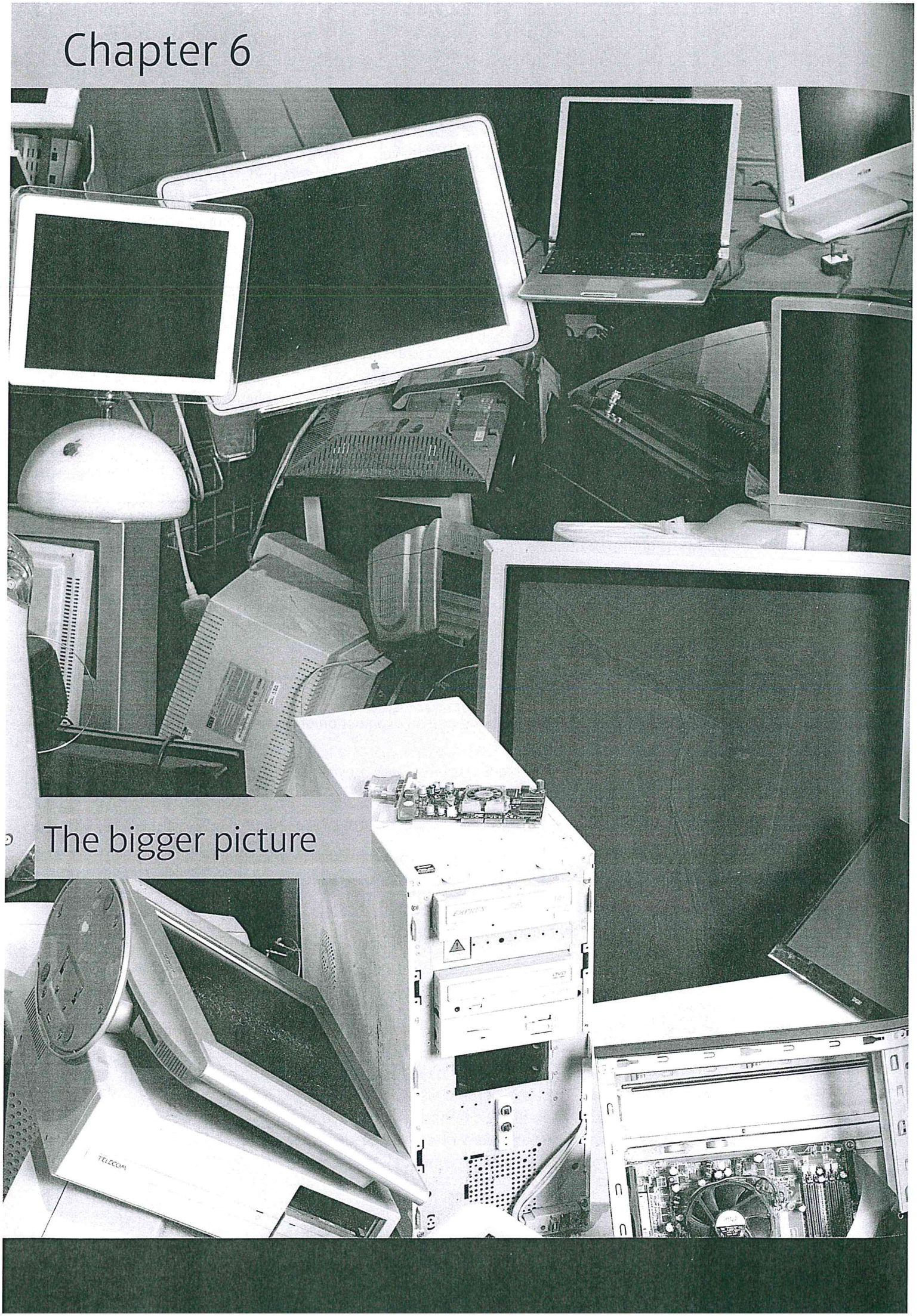
Chapter 6



The bigger picture

6.1 Computing and the environment

Learning objectives

By the end of this section you should be able to:

- explain how the manufacture, use and disposal of computing technology damages the environment.
- describe efforts being made to reduce the environmental damage caused by computing technology.
- give some examples of how computing technology is helping to protect the environment.

It's hard to imagine what life would be like without the internet, social media, search engines and e-commerce. Global demand for smartphones, tablets and other forms of **computing technology**, including embedded processors, web servers, sensors and hard drives, is growing rapidly year on year. At the same time, the pace of new product releases and consumers' desire to own the latest model is shortening the lifespan of these devices. The average life expectancy of a smartphone, for example, is estimated to be less than two years. The more computing technology we buy, the more we throw away.

Not surprisingly, the manufacture, use and disposal of computing technology have a significant impact on the environment, using up dwindling resources of non-renewable materials, creating massive piles of potentially harmful **e-waste**, consuming vast quantities of energy and damaging people's health.

Key terms

Computing technology: an all-encompassing term referring to the hardware, software and infrastructure that underpin current and emerging computer systems.

e-waste: any form of discarded electronic equipment, including computing technology.

Top tip

Try to stay up to date with computer science news, so that you know about emerging technologies and are aware of current issues. The BBC's Click website is a good starting point. It's also worth checking out the technology section of the BBC website and subscribing to the cs4fn magazine.

Manufacture

Manufacturing a smartphone, a PC or any other piece of computing technology is a complex process, starting with the extraction of raw materials and ending with the finished item being shipped to the customer, with lots of stages in between. This makes it difficult to determine accurately the overall environmental impact, although there's no doubt that it's considerable.

Raw material extraction

A number of non-renewable natural resources are used in the manufacture of computer products. They include sand (to make glass for screens), oil (used to make plastics) and various metals used in wiring and circuit boards. Some of the metals used, such as silver, gold, copper and palladium, are precious and in short supply. Others, such as arsenic, cadmium and chromium, are hazardous and pose a serious health risk. Radioactive metals used in computer products, such as uranium and thorium, can contaminate air, soil and groundwater, and are toxic to human health.

In some regions of the world, mining of raw materials is poorly regulated. Excavation causes extensive damage to the local environment, scarring the landscape with unsightly holes and waste heaps, contaminating water

Extend your knowledge

China is the world's largest producer of rare earth metals – a group of 17 chemical elements that, due to their unique magnetic, luminescent and electrochemical properties, help improve the performance of computing technology and make it more energy efficient.

supplies and endangering wildlife habitats. Poorly equipped miners working in dangerous conditions run the risk of being seriously injured and are also susceptible to long-term respiratory illnesses, such as silicosis, bronchitis or lung cancer.

Production

Once extracted, the raw materials are shipped to factories – often thousands of miles away – to be manufactured into components, such as circuit boards, chips, screens, disk drives and cases.

In turn, the components are dispatched onwards for assembly into finished products.

The manufacture of computing technology is energy intensive. Large amounts of non-renewable fossil fuels, such as coal and oil, are used during the process. Burning fossil fuels produces carbon dioxide (CO_2) and contributes to global warming.

Extend your knowledge

The United Nations University has estimated that the manufacture of a computer and monitor weighing 24 kilograms requires ten times the amount of fossil fuels (240 kilograms), approximately the same weight of chemicals and around 1,500 litres of water.

Semiconductors are present in every piece of computing technology. Manufacturing semiconductors is highly water intensive. For example, a factory producing 40,000 semiconductors a month uses around 20 million litres of water a day – on a par with the consumption of a city with a population of 60,000. This can result in water shortages in areas where semiconductor factories are located, and untreated wastewater discharge can cause environmental pollution.

This table lists six of the most hazardous materials used in the manufacture of computing technology.

Material	Examples of use
Cadmium	A metal used in the manufacture of rechargeable batteries, printer inks and toners.
Lead	A metal used in the manufacture of circuit boards and cable sheathing.
Mercury	A metal used in the manufacture of LCD screens.
Hexavalent chromium	A chemical compound used to make casings.
Polychlorinated biphenyls (PCBs)	Toxic compounds added to plastics, circuit boards, and connectors to make them more fire retardant.
Polybrominated diphenyl ethers	

Research indicates that exposure to these materials is harmful to human health, causing both physical and neurological damage. Furthermore, chemical emissions and wastewater from manufacturing plants put people living in the vicinity at risk.

There is growing recognition of the need to address this problem.

The EU Restriction of Hazardous Substances (RoHS) Directive was transposed into UK law in 2013. It restricts the use of all six of the materials listed in the table above, forcing manufacturers of computing technology to replace them with safer materials.

At the same time, governments are imposing tough recycling targets designed to ensure that more reusable material is recovered from redundant computing technology, and reused so that fewer raw materials are needed and reserves of scarce resources are protected.

Growing public awareness is putting pressure on manufacturers to improve working conditions in their plants and impose stricter requirements on their component suppliers.

Usage

The amount of energy consumed in the manufacturing process pales into insignificance when compared with the energy required to keep mobile phones, computers, networks, telecommunication links, etc. up and running day after day. Even though each individual device doesn't require a huge amount of electricity, close to two billion connected PCs and laptops and more than six billion mobile devices collectively do.

In recent years considerable efforts have been made to improve the energy efficiency of computing devices. However, the amount of energy they actually consume depends on how they are used and what they are used for. The task that a computer is performing and the software being used are key determinants of the actual energy usage. High-end applications, complex calculations, 3-D modelling and video games are particularly power hungry.

Cloud computing (see section 4.2, page 151) and data centres in particular are major energy guzzlers. Vast amounts of electricity are needed to power and cool all the computer equipment that is needed, putting them ahead of the aviation industry in terms of the energy they consume. The worst culprits are the small, inefficient data centres hosted by private organisations and government departments, which tend to be far less efficient than the large facilities operated by cloud providers such as Google® and Apple.

Energy efficiency measures and the use of renewable energy can significantly reduce the **carbon footprint** of data centres. Facebook, for example, has built a huge data centre in northern Sweden, just 100 km south of the Arctic Circle. Its location was selected because of its access to renewable hydroelectricity and the cold climate that helps to keep the servers cool.

Activity 2 ?

Data centres consume large amounts of energy.

1. Research what this energy is used for.
2. Identify four measures that can be taken to make data centres more environmentally friendly.

Did you know?

A lot of energy is wasted while a computer or printer sits idle. Using the 'sleep mode' when a device is not in use can reduce consumption by more than 50 per cent.

Activity 1 ?

Research why using a laptop rather than a desktop is more energy efficient.

Key term

Carbon footprint: the amount of carbon dioxide an individual or organisation produces as a result of the energy they consume.

Disposal

The disposal of redundant computing technology represents another serious threat to the environment. The quantity of e-waste is growing at a tremendous pace. According to the UN's StEP Initiative, e-waste will soon weigh as much as eleven of the great Egyptian pyramids.

Although great efforts are now being made to recycle more e-waste, large amounts are still shipped overseas to developing countries where they are dumped in landfill sites. This can have serious consequences for the environment and public health. The problem is compounded by the fact that the developing nations themselves are generating more and more waste of their own.

E-waste that is not recycled properly can be a serious health and environmental issue. As you know, computer products contain a whole host of dangerous materials. Once a computer is dumped in a landfill site, the likelihood is that some, if not all, of these toxic substances will leak out into the ground, contaminating water supplies, infiltrating the food chain and polluting the air.

For every one million mobile phones, 24 kg of gold, 250 kg of silver and nine tonnes of copper can be recovered. The presence of these valuable metals in old computing technology is a powerful incentive for local people living near the landfill sites, many of whom are desperately poor, to try to recover them. However, dismantling old computer equipment without protective clothing and specialist training is extremely dangerous. People who do so risk exposure to hazardous materials such as mercury and lead and are in danger of inhaling toxic fumes.

Did you know?

Electronic waste is expected to top 60 million tonnes globally by 2017 – an increase of a third in five years.

Activity 3 ?

'One person's cast-off is another person's treasured possession.' Research, then briefly describe two initiatives that aim to prolong the life of pre-owned computing technology.

The Waste Electrical and Electronic Equipment (WEEE) Regulations (2013) set targets for the collection, recycling and recovery of computing technology and other electronic items. They apply to businesses but not to individuals.

The aim of responsible recycling is to recover valuable metals and reusable components such as plastic, glass and metal, and to dispose of dangerous substances safely.

Major manufacturers of computing technology now have recycling programmes. In developing countries there are some promising initiatives to create state-of-the-art recycling plants that can turn e-waste into an e-opportunity.

Activity 4 ?

1 Give three possible environmental impacts of using computing technology.

2 Suggest one possible action that could be taken to reduce each of them.

Preserving the environment

The picture is not entirely bleak. Computing technology is at the heart of efforts to combat climate change, provide disaster warnings, protect endangered species and habitats, and reduce energy consumption.

Climate change

NASA is analysing satellite data and measuring sea surface temperatures to learn more about how and why sea levels are rising.

Networks of wireless sensor probes are used to gather information about glaciers. The probes are placed under the surface of the ice and measure temperature, pressure, stress, weather and sub-glacial movement. A base station collects the data from them. The system is helping scientists to understand more about the speed at which glaciers are melting.

Researchers at the University of Oxford are using spare home computer time to establish if global warming is to blame for heavy flooding in the UK in recent years.

Early warning

Tsunami early warning systems use sensor networks to detect approaching tsunamis and a communications infrastructure to issue timely warnings so that coastal areas at risk can be evacuated.

Conservation

Information from GPS and satellites is being used to track Malaysian elephants. The results are analysed by computer to help improve conservation strategies and assess the effectiveness of the Malaysian Government's elephant conservation programme.

Miniature transponders fitted to bees allow scientists to study the effects of disease and pesticides.

Mobile phones are being used to listen out for illegal logging activities in the rainforest and provide rangers with real-time alerts.

Energy

Engineers at Manchester Metropolitan University are working on a project to make buildings more energy efficient. Sensors in each room monitor light levels, temperature, how many people are present and electricity consumption. Real-time analysis of the room data enables automatic adjustment of electricity usage.

Did you know?

Green computing indicates the efficient use of resources in computing. It makes companies and individuals responsible for producing and using technology with a minimal carbon footprint. The main emphasis is on energy efficiency, use of safer materials during the manufacturing process and promoting environmentally friendly systems.

A lioness with a tracking device. GPS collars help to monitor and conserve wildlife.

The bigger picture

The latest generation of giant solar energy farms uses sensors to track the movement of the sun and computer-controlled motors to adjust the position of the solar panels to optimise power generation. Developments in battery storage allows surplus electricity to be stored.

Exam tip

Make sure you give real positive and negative examples of how computing technology affects the environment.

Exam-style question

Discuss the impact of computing technology on the environment.
(6 marks)

Summary

- Some of the materials used in the manufacture of computer components are non-renewable and in short supply. Others are dangerous and pose a risk to human health.
- The Restriction of Hazardous Substances (RoHS) Directive restricts the use of hazardous materials in computing technology, forcing producers to find more environmentally friendly alternatives.
- Computing technology consumes huge amounts of energy. Data centres are one of the worst culprits.
- Energy efficiency measures and use of renewable energy can significantly reduce the carbon footprint of computing technology.
- There is a possible health risk, especially for children, from exposure to the electromagnetic fields generated by wireless devices, such as smartwatches and smart clothing.
- Unregulated disposal of e-waste in landfill sites poses a significant threat to the environment.
- The Waste Electrical and Electronic Equipment (WEEE) regulations set targets for responsible recycling of e-waste.
- Computing technology is helping to preserve the environment in a number of ways, including monitoring and modelling climate change, conservation and smart energy.

Checkpoint

Strengthen

S1 Identify two hazardous substances used in the manufacture of computing technology.

S2 Which UK law restricts the use of hazardous substances in the manufacture of computing technology?

S3 Why is dumping e-waste in landfill sites harmful to the environment?

S4 List two ways of reducing the environmental damage caused by data centres.

S5 List two ways in which computing technology is helping to preserve the environment.

Challenge

C1 Summarise the health risks associated with the manufacture and disposal of computing technology.

C2 Describe three ways in which computing technology can help to reduce energy consumption.

How confident do you feel about your answers to these questions?
If you're not sure you answered them well, reread this section and have another go at the activities.

6.2 Privacy

Learning outcomes

By the end of this section you should be able to:

- explain why computing technology poses a threat to privacy.
- weigh up the benefits and drawbacks of giving away personal information.
- describe the legislation that protects against computer misuse.

Now that you know about the damaging environmental impact that computing technology has, does it make you have second thoughts about swapping your smartphone for the latest model? Might you decide that your concern for the environment outweighs your desire for a new phone? If so, you are making an ethical decision. **Ethics** relate to what is right and wrong and govern a person's behaviour.

An action might be legal, but not necessarily ethical. For example, it's perfectly legal to leave your old desktop computer gathering dust in the attic, but if you know that someone in a developing country would benefit enormously from having it, the right thing to do might be to dust it down and pass it on to them.

Computing technology confers a wide range of social and economic benefits, but it also creates a host of challenging ethical issues. **Privacy** and security are two of them.

While most people would agree that computing technology has helped to create a much more open society, some would argue that it comes at too high a cost. The amount of personally identifiable information that is gathered, stored and analysed represents a massive invasion of privacy.

Key terms

Ethics: a set of moral principles that govern a person's behaviour.

Privacy: the right to be left alone and free from unwanted scrutiny and intrusion.

Personal data: information that is personal and unique to an individual.

Personal data

Every time you post an update on social media, sign up for an online account, use a web-based email service or a search engine you are adding, knowingly or unknowingly, to an enormous hoard of **personal data** that is held about you – where you live, what you look like, who your friends are, your likes and dislikes, your bank account details, products you're interested in buying, the route you take to school each morning.

This personal data is stored on servers that belong to online services, such as Facebook and Google®, not to you.

Every organisation you come into contact with, not just the online companies, is likely to collect information about you. Your school, for example, stores your attendance record, your end-of-year exam results, which books you've borrowed from the library, the after-school activities you take part in and much more besides. Does this worry you?

Did you know?

Facebook has the biggest database of faces in the world, with over 350 million photos posted and tagged to the website every day.

Some people are very concerned about the amount of personal information that is collected, often without their consent and over which they believe they have little or no control. They are worried about who has access to it, what they are using it for, how secure it is and how accurate it is.

Weak security could result in personal information falling into the wrong hands, making people vulnerable to phishing attacks, scams, **identity theft** and fraud.

Sometimes the information is inaccurate, but getting it changed or removed is extremely difficult, if not impossible. It's not unheard of for inaccurate information about a person to follow them throughout their entire life, affecting how they are seen and treated by others.

Key term

Identity theft: the stealing of another person's personal details, such as their bank account number, sort code or passport number, for the purpose of making purchases and running up debts in their name.

Did you know?

The UK Data Protection Act (1998) controls how organisations and the government can use personal data. It specifies the following principles.

- Data must be processed fairly and lawfully.
- Data must be obtained and used only for the specific and lawful purposes for which it was collected.
- Data must be adequate, relevant and not excessive.
- Data must be accurate and up to date.
- Data must be kept for no longer than necessary.
- Data must be kept secure.
- Data must **not** be transferred to regions not bound by similar principles of the Act.

Activity 5 ?

1 What information can you find out about yourself by typing your name into a search engine? Is it accurate? What sort of impression of you does it portray?

2 Research the Safe Harbor Decision privacy principle. Why has the EU declared it invalid?

One reason why so many people voluntarily give away information about themselves is that it enables an organisation to understand their needs better and provide them with a more personalised service. For example, setting up an account with an online supplier makes it faster and more convenient to purchase from them.

But do these benefits outweigh the drawbacks?

You might not mind that an online retailer knows who your favourite band is if it means you get to hear quickly when their next album is released, but is it right to target a financially vulnerable person with adverts for products they will want but can't afford?

Did you know?

Cookies are small data files that keep a record of your web browsing history. They record which websites you visit and how often, which products or services you buy or show an interest in. Cookies enable online stores to learn a lot about you.

The Privacy and Electronic Communications Regulations (2011) gives consumers the right to opt out of having data about their browsing habits collected in this way.

Unlike a cookie, spyware is a computer program stored on your hard drive (usually without you realising it's there) that collects information about you and transmits it to a third party. It represents another serious threat to privacy.

Big data

Data analysts are able to learn more and more about us and gain insights into our behaviour by analysing huge volumes of personal data gathered from various sources.

Analysis of so-called 'big data' can benefit society. For example, by helping to identify adverse side effects of drugs that might otherwise go unnoticed, optimising energy use in cities and providing insights into the spread of disease.

But is the price we pay too high? Where do we draw the line? Big data comprises large amounts of information, each piece of which on its own could be seen as being harmless, for example your phone number, what music you download, your hobbies, etc. However, when collated together these individual bits of information produce a very accurate, detailed profile of an individual, revealing far more about them than they might have willingly disclosed. This might lead to the individual becoming a victim of identity theft or an intruder illegally accessing personal information through social engineering. (See 'Personal data' on page 213.)

Surveillance

Have you any idea how often you've been watched on CCTV today? Could a drone have been hovering overhead taking aerial photographs of you on your walk to school? If you've driven anywhere by car, travelled by public transport or been in a shop, the chances are you've been recorded by some form of **surveillance technology**.

Most people are willing to allow the security forces to use surveillance technology to track people's movements and tap their phones if it enables them to uncover terrorist plots. But what if it were used by companies to monitor your shopping habits or by criminals noting the time you leave the house each morning? It's not unheard of for employers to use hidden cameras to check up on their staff. Is this acceptable?

Some people believe that use of surveillance technology goes too far. In 2013 Edward Snowden, a so-called '**whistle-blower**', raised awareness of the extent to which governments worldwide are now monitoring and spying on their citizens.

Activity 6 ?

Find two examples of how society is benefiting from big data analysis.

Key terms

Surveillance technology: CCTV, drones, number plate recognition, bugging and tracking devices used to monitor and record people's activities, often without their knowledge.

Whistle-blower: someone who draws attention to the activities of an organisation or person believed to be acting illegally or unethically.

Activity 7 ?

The right to privacy must be balanced against the needs of society. Describe two situations in which you believe an invasion of privacy is justified. Explain your reasoning.

Key term

Location-based services: services that enable people to access and share real-time location information online.

Activity 8 ?

Describe three ways in which location-based services can benefit a user and three risks associated with their use.

Did you know?

UK police track vehicle movements in real time using automatic number plate recognition and CCTV. Records can be kept for two years to be analysed for intelligence.

CCTV combined with facial recognition software enables the police to identify and track specific individuals.

Location-based services

With the help of **location-based services** and Wi-Fi, people can share their current location, arrange to meet up with friends nearby, check in to a venue, find their way to a particular location and much more. A drawback is that location-based services also allow other people to track your movements, find out where you live and what you are doing. This can be dangerous and represents a huge invasion of privacy.

Privacy-enhancing tools

Privacy-enhancing tools, while not 100 per cent effective, do give some protection against privacy invasion. This table lists some of the most popular of these tools.

Tool	Purpose
Encryption	Prevents unauthorised people from reading your data.
Cookie cleaners, anti-spyware and ad blockers	Software that detects and removes cookies, spyware and adware installed on your computer.
Identity management services	A trusted third party holds evidence of your identity and issues you with an identifier that enables you to conduct transactions with other parties without revealing any personal information about yourself.
Password managers	Stores all your website login information in an encrypted password database with a master password, which is the only one you have to remember.

Cyber-security

As you learnt in Chapter 5 (see page 192), hacking represents a serious security threat.

The Computer Misuse Act (1990) makes hacking a crime. It identifies three types of illegal activity.

- Unauthorised access to computer material, either a program or data.
- Unauthorised access with intent to commit further offences (e.g. accessing personal data about a person so as to steal their identity).
- Intentional and unauthorised destruction of software or data (e.g. by installing malware).

A 2015 amendment to the Act grants immunity from prosecution to the security services, enabling them to hack data on laptops and mobile phones, and in databases belonging to suspected criminals.

Activity 9

Research the 'Carphone Warehouse Data Breach' of 2015. How many customer records were thought to have been stolen? What are the implications of this breach for both the customers and the company?

Did you know?

Sony was the victim of a major cyber attack in 2014. The company claims that hackers working for the North Korean Government were to blame. Private emails were disclosed to the public, and a number of unreleased films were made available on sharing websites.

Summary

- Computing technology enables organisations to gather, store and analyse vast quantities of personal information about the people they come into contact with.
- Individuals give away all sorts of personal information about themselves online.
- Collecting and analysing information about the people they come into contact with enables organisations to provide a more personalised service.
- Big data analysis benefits society at the expense of many individuals' privacy.
- Surveillance technology helps keep us secure, but encroaches on our privacy. It is difficult to determine what level of surveillance is acceptable.
- The Computer Misuse Act (1990) makes hacking illegal.

Checkpoint

Strengthen

S1 Describe two ways in which an individual's personal data could end up stored in databases owned by a third party.

S2 What might happen if personal information falls into the wrong hands?

S3 List two privacy-enhancing tools and describe what they do.

S4 List the activities that the Computer Misuse Act (1990) makes illegal.

Challenge

C1 Why do some people decide that the benefits of revealing personal information about themselves outweigh the drawbacks?

C2 Describe a situation where the right to privacy is less important than the needs of society.

How confident do you feel about your answers to these questions? If you're not sure you answered them well, reread this section and have another go at the activities.

6.3 Digital inclusion

Learning outcomes

By the end of this section you should be able to:

- explain how people benefit from being 'technology-empowered' and the disadvantages of being 'technology-excluded'.
- describe measures that are being taken to promote digital inclusion.

Computing technology is a great enabler, giving many people access to news, information, products and services at any time wherever they are. But those people who neither have the opportunity nor knowledge to use this technology are excluded from the advantages it provides. Is this fair?

Digital inclusion is about providing everyone with affordable access to computing technology and the skills to use it.

The gap between those who are 'technology-empowered' and those who are 'technology-excluded' is known as the **digital divide**.

There is a digital divide between industrialised and developing countries and also between people who live in the same country.

Key terms

Digital inclusion: ensuring that everyone has affordable access to computing technology and the necessary skills to take advantage of it.

Digital divide: the gap between people who are technology-empowered and those who are technology-excluded.

Impact

There are many reasons why technology exclusion is not a good idea.

Information and services	The internet is becoming the default option for accessing information, public services and entertainment.
Employment	Having poor digital literacy skills makes it harder to find a job and limits employment opportunities, relegating individuals to poorly paid work with little prospect of progression.
Democracy	The internet gives people a voice and lets them express their views to a worldwide audience. This is particularly important where citizens have limited freedom of expression.
Economic growth	Businesses that are able to exploit computing technology to the full have a competitive advantage over those that can't.
Saving money	Paying bills and shopping online often saves consumers money and gives them better protection.
Social isolation	Having access to the internet helps people to keep in touch with friends and relatives.

Towards digital inclusion

Data from the Office for National Statistics suggest that the UK is making good progress towards achieving digital inclusion for its citizens. Figures for 2015 for England, Scotland and Wales show that:

- the internet was accessed every day by 78 per cent of adults (39.3 million), compared with 35 per cent (16.2 million) in 2006;

- 96 per cent of adults aged 16 to 24 accessed the internet 'on the go', compared with only 29 per cent of those aged 65 years and over;
- 61 per cent of adults used social networking and, of those, 79 per cent did so every day or almost every day;
- 76 per cent of adults bought goods or services online;
- 86 per cent of households (22.5 million) had internet access, up from 57 per cent in 2006.

Other industrialised nations in North America, Europe and Northern Asia are also doing well.

The same can't be said for other parts of the world. According to the United Nations' *State of Broadband* report (2015), billions of people living in the developing world are still without broadband internet, including 90 per cent of those living in the poorest nations.

Age, disability, disinterest, poverty and cultural norms all play a part in digital exclusion, but lack of connectivity is one of the major causes.

The good news is that, according to the World Bank, 77 per cent of the world's population already live within range of a mobile phone network. In areas with a limited or non-existent landline infrastructure, mobile phone technology can fill the gap. Even though the number of phones per 100 people in poor countries is much lower than in the developed world, they are having a huge impact.

Did you know?

Facebook plans to use drones and satellites to bring the internet to Africa. They have also developed an app, called Free Basics, which provides free basic access to services.

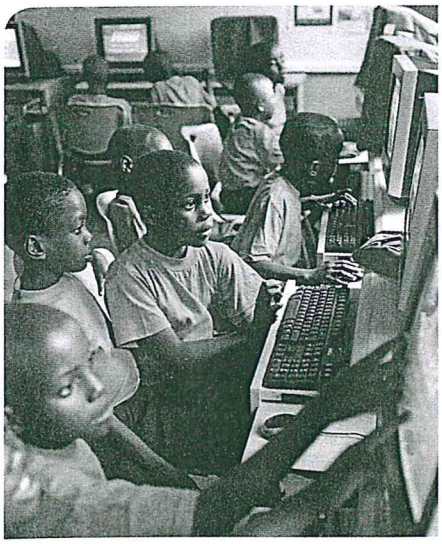
Activity 10 ?

Use the internet to find some actual examples of how mobile phones are being used in Africa or elsewhere to promote digital inclusion. Write a brief report summarising your findings.

Efforts to bridge the digital divide require more than simply giving people internet access. The UK's digital inclusion strategy sets out the actions that the government and its partners are taking to reduce digital exclusion.

Activity 11 ?

Identify five actions a government can take to reduce digital exclusion.



Ambitious digital literacy programs are under way in India, Kenya, Colombia and elsewhere to ensure that people have the know-how and skills they need to exploit digital technology to the full

The bigger picture

Summary

- Digital inclusion means that everyone has affordable access to computing technology as well as the skills to use it.
- A number of factors contribute to the digital divide – lack of or poor connectivity is one of the main ones.
- Someone who is 'technology-excluded' misses out on all the opportunities computing technology offers.

Checkpoint

Strengthen

S1 What is meant by the terms 'technology-empowered' and 'technology-excluded'?

S2 List three drawbacks of being 'technology-excluded'.

S3 List four factors that contribute to the digital divide.

S4 Describe two ways of providing access to the internet in areas with a poor landline infrastructure.

Challenge

C1 Access to the internet is a key factor in reducing the digital divide. Describe two further measures that governments can take to promote digital inclusion.

How confident do you feel about your answers to these questions? If you're not sure you answered them well, reread this section and have another go at the activities.

6.4 Professionalism

Learning outcomes

By the end of this section you should be able to:

- explain what professionalism means in the context of computer science.

Computer scientists write software to make computers do new things or accomplish tasks more efficiently, create mobile apps, design and build embedded systems, devise security policies, invent new products and much more besides.

Some work for big multinational computing companies, such as Microsoft® and Apple, others for small start-ups; some are self-employed, some are employed in the IT departments of organisations such as hospitals, universities and companies.

Wherever they work they are expected to behave ethically and demonstrate **professionalism**.

The British Computer Society (BCS) is the Chartered Institute for IT. The BCS Code of Conduct sets out the professional standards its members are expected to uphold. Among many other matters, it specifies that computer scientists must:

- respect the privacy, security and wellbeing of others and the environment;
- avoid injuring others, their property, reputation, or employment;
- develop their professional knowledge, skills and competence on a continuing basis;
- be familiar and comply with relevant legislation;
- **not** disclose confidential information;
- **not** misrepresent or withhold information on the performance of products, systems or services.

Exam-style question

Airtest produces exhaust emissions testing software. A programmer discovers that there is a bug in the software that produces inaccurate results under particular circumstances.

State what course of action the programmer should take and explain why. **(3 marks)**

Exam tip

This is a scenario-based question, so make sure you relate your answer to the scenario – don't mention what you personally would do, but what the Airtest programmer should do. Don't forget to refer back to the code of conduct.

Key term

Professionalism: the skill and competence expected of a person in a professional setting.

Did you know?

Most computer scientists pay an annual membership fee to belong to a professional association. This gives them access to specialist technical conferences, training and publications. It also provides them with an opportunity to interact and share knowledge and expertise with each other. Having membership of a professional association on their Curriculum Vitae (CV) sometimes carries weight when a computer scientist is applying for a new job.

The three main professional bodies for computer scientists in the UK are:

- The British Computer Society (BCS)
- The Institute of Electrical and Electronics Engineers (IEEE)
- The Association for Computing Machinery (ACM).

Activity 12 ?

A computer scientist is developing an embedded system to control car brakes.

Discuss in a group how she should respond if:

1. she spots a bug, but knows that fixing it will delay completion of the project;
2. she's aware that there is a remote possibility that someone could hack into the code and stop the brakes from working;
3. a competitor offers to pay her for details of the code;
4. her employer makes claims for the system that are not entirely true.

Discuss any other ethical dilemma she might encounter as a professional.

Summary

- Computer scientists must abide by the law.
- They should behave ethically by adhering to a professional code of conduct.
- It is important that programmers demonstrate professionalism as the work they do could put the lives of other people at risk.

Checkpoint

Strengthen

S1 What does the BCS Code of Conduct say a computer scientist should do?

Challenge

C1 What does 'professionalism' mean for a computer scientist?

How confident do you feel about your answers to these questions? If you're not sure you answered them well, reread this section and have another go at the activities.

6.5 The legal impact

Learning objectives

By the end of this section you should be able to:

- describe how copyright and patents can protect intellectual property.
- explain the purpose of a software licence.
- differentiate between open-source and proprietary software and outline the benefits and drawbacks of each.

Intellectual property

Intellectual property (IP) – not to be confused with an IP address – is a unique creative product of a human mind. A piece of software, a computer game, a design for a new processor, a digital image, a piece of music and a literary work are all examples of IP. Each of them was created by somebody, is unique and has a commercial value.

Copyright and patents

The Copyright, Designs and Patents Act (1988) makes it illegal to copy, modify or distribute intellectual property without permission.

That said, there are a multitude of peer-to-peer networks, torrent sharing websites and forums on the internet that allow people to download copyrighted software without paying for it. Not only is this illegal, it is also unethical, since it means that the programmer who wrote the code doesn't get the money that is due to them.

Copyright only protects the expression of an idea, not the idea itself. So if you were to develop an original piece of software, its source code would be protected, but there's nothing to stop someone else from copying the idea and writing a program that essentially performs the same task. You would have to prove that the similarities between the two programs are more than just coincidence and can only be explained by copying.

The © symbol indicates that a piece of software, a movie or some other type of artefact is protected by copyright.

Did you know?

In 1994, Apple agreed to license parts of its GUI (see section 4.4, page 162) to Microsoft® for use in the first version of Microsoft® Windows®. When Microsoft® released Windows® 2.0, it used the overlapping windows feature of the Macintosh OS, which was not included in the original licence agreement. Consequently, Apple sued Microsoft® for copyright infringement.

A **patent** offers more protection than copyright. It protects the idea or design of an invention, rather than just a particular form of it. In order to get a patent you have to be able to demonstrate that what you have invented is distinct from anything else that already exists. A patent holder has the exclusive right for 20 years to make, use and sell their invention.

Key terms

Intellectual property (IP): a creation of the human mind that is unique and has a commercial value.

Patent: an exclusive right granted to an inventor to make, use and sell an invention for a fixed period of time.

Did you know?

The creators of the illegal software sharing website, The Pirate Bay, received a prison sentence and were fined over US$4,000,000 for hosting hyperlinks to illegally obtained software and media.

Top tip

Make sure you know which laws affect the use of computing technology, including the Data Protection Act (1998), the Computer Misuse Act (1990), the Copyright, Design and Patents Act (1988) and the Regulation of Investigatory Powers Act (2000).

Keep an eye out for any amendments to these laws or for relevant new government legislation.

Did you know?

For years, various smartphone manufacturers including Apple and Samsung have been battling in the courts over patent infringements. Apple alleged that Samsung had stolen the 'look and feel' of its iPhone and used it in the Galaxy smartphone.

There is a real concern that the inventiveness that patents are designed to encourage will suffer as a consequence of these so-called 'patent wars', with manufacturers spending their money on lawsuits rather than on new inventions. This would be very bad news for consumers.

Activity 13

1 Get into groups of three. Each person in the group should describe how they would feel if an app they have created was made available for free on the internet, without their permission.

2 Create a podcast for software developers, explaining how software can be protected as intellectual copyright.

Key terms

Creative Commons: an organisation that allows people to set copyright terms for their intellectual property. One use of a Creative Commons licence is to allow people to copy material as long as it is not used commercially.

Open-source software: software that is free to edit and redistribute.

Exam-style question

Assess the extent to which the patent system is a barrier to technological innovation. **(4 marks)**

Exam tip

The command word here is 'assess', which means you should consider both sides of the argument and come to a conclusion.

Licensing

Every piece of software, even if it is free, has a licence. Even though the user purchases a piece of software, the licence states that they don't actually own it. The licence allows the buyer to use the software subject to the licence terms, but the manufacturer retains ownership. Before you can install the software you have to agree to the terms of its licence. These specify:

- how many copies of the software you are allowed to use;
- whether you can install the software on more than one computer;
- what type of organisation can use the software – some licences are for charities, students or home users only;
- how long the software can be used for – perpetual software licences last forever, but some licence agreements expire unless you renew them.

You are usually not allowed to resell the software. Paid-for software is often supplied with a unique licence key, which certifies that the software is genuine and prevents illegal copying.

If a computer scientist wants to permit other people to use their code without charge, they can use an open-source licence to specify what restrictions (if any) there are.

A **Creative Commons** licence provides a way for the creator of a piece of music, a photograph or other form of intellectual property - including software - to allow other people to use it providing they abide by the conditions specified in the licence.

Open-source and proprietary software

Open-source software is freely available on the internet. Anyone is permitted to edit the code and pass it on to others, providing they don't charge a fee.

The advantages and disadvantages of open-source software are shown in this table.

Advantages	Disadvantages
• It is free to use. • It can be modified. • It can be used to demonstrate programming concepts.	• It might not be particularly 'user friendly' and might look unprofessional. • There might be little or no technical support available. • Criminals may be able to identify and exploit vulnerabilities in the code.

Proprietary software is the opposite of open source – it is closed source. This means its source code is protected and users are not allowed to modify it.

On the plus side, proprietary software is extensively tested prior to release, any bugs that do come to light thereafter are quickly fixed and there is plenty of user support. The drawback is that if the software doesn't exactly do what you want it to, you're not allowed to change it.

Summary

- A programmer loses out financially if their software is downloaded illegally.
- The Copyright, Designs and Patents Act (1988) makes it illegal to copy, modify or distribute intellectual property without permission.
- Copyright protects the expression of an idea, not the idea itself.
- A patent offers more protection than copyright. It protects the idea of an invention rather than just a particular form of it.
- A software licence specifies how a piece of software can be used.
- Open-source software is freely available and can be edited and shared.
- The source code of proprietary software is protected and users are not allowed to modify it.

Did you know?

The Python programming language is open source and is maintained by the Python Software Foundation. Members of the programming community often contribute to the source code to build on the language.

Key term

Proprietary software: software that belongs to an individual or a company. Its licence specifies that users are not allowed to modify the source code and places restrictions on its use.

Did you know?

Microsoft® Windows® 10, iTunes, Adobe Photoshop and Mac OSX are all examples of proprietary software.

Activity 14 ?

Create a table that summarises the differences between open-source and proprietary software.

Checkpoint

Strengthen

S1 Describe the purpose of a software licence.

S2 What are the main differences between open-source and proprietary software?

Challenge

C1 Explain how a patent would protect you as an inventor of a product.

C2 Identify relevant legislation that computer scientists should be familiar with.

How confident do you feel about your answers to these questions? If you're not sure you answered them well, reread this section to enhance your knowledge.