1.5.1 Computing Related Legislation

Revision sheet

Until the Computer Misuse Act was introduced in 1990 there were no legal provisions in the UK law which governed computer systems. As computers have become more widespread, new laws have been introduced. There are different laws for different areas of computing.

1 Data Protection

GDPR is a regulation in EU law that governs data protection and privacy for citizens of EU and EAA. it is combined into the UK law along with the Data Protection Act 2018. Data protection is enforced by the Information Commissioner through the Information Commissioners Office (ICO).

1.1 Principles of Data Protection

The principles of data protection are a set of rules that govern systems that collect, store and process personal data. They must make sure that the information is: used fairly, lawfully and transparently; for specified explicit purposes; limited to only what is needed; accurate (and kept up to date); handled in a way that ensures the security of the data. There is stronger legal protection for some much more personal information (eg, race; religious belief; genetics and more). There are different safeguarding protocols used for personal data for criminal convictions and offences.

1.2 Personal Rights

Under the DPA, you have the right to find out what information organisations store about you. These rights also include: to be informed about how your data is being stored and used; obtain a copy of your data when requested; have incorrect data updated; have data erased; restrict or stop the processing of data; stop data being processed in certain circumstances. There are also personal rights when an organisation is using personal data for example as part of an automated decision making process, or profiling you.

1.3 Access To Data

One of the key rights in the DPA is the access to data - you should be able to access a copy of the data which the company stores about you by making a written request. This is often to the organisation's DPO (data protection officer) or to the company secretary. The data should be provided within one month but if there is a delay, the requester should be informed of the delay (and what the delay is) within one month of requesting the data. There are some circumstances in which the organisation can withhold data (eg, active crime or police investigation, national security or military; assessment or collection of taxes), the organisation doesn't have to say why they're withholding data. Requests for data are usually free however there might be a small charge if there is a lot of data requested or if it will take a lot of time and effort to process the data.

1.4 When Something Goes Wrong

In the event that data is misused or not held securely, the first person to contact is that organisation. If they don't respond satisfactorily, then the Information Commissioner's Office should be contacted. There have been a number of high profile court cases of companies being fined for contravening the law. These are generally as a result of external hacking. Data protection legislation requires that organisations notify the ICO of any security breaches that compromise personal data.

1.5 Digital Footprints

Companies store lots of information about everyone. This information which exists on the internet about a particular person is called their digital footprint. Whilst this information might now be stored on a secure server there is always a chance that it is not secure in the future and the information might be made publicly available.

2 Regulation of Investigatory Powers Act

The Regulation of Investigatory Powers Act (RIPA) 2000 was needed because of the growth in internet communications. It defines what police and government agencies can and can't do, as well as the responsibilities of companies such as ISPs, telecom companies and social media platforms. It has been edited a number of times since it was introduced. The most recent amendment brings the online world more in line with the offline world.

2.1 Provisions of the Act

Under the act, the police and specified public bodies can: demand that ISPs provide access to their customers' digital data without informing the customer; carry out mass surveillance of digital communications; demand that ISPs fit equipment that allow for digital surveillance; demand that someone hand over the keys to encrypted information; intercept and monitor communications; keep the existence of interception warrants and any data collected under them (even from within courts).

3 Computer Misuse Act

The Computer Misuse Act (CMA) 1990 makes it illegal for anyone to access and make changes to a computer system with malicious intent. Amendments have made the act stronger in an attempt to keep up with cyber criminals. Different offences have different punishments, ranging from a two-year prison sentence and a £5000 fine to a 14 year prison sentence. Even if an attempt to break into a computer system was not successful, it is still illegal. If hacking is accompanied by other offences (eg, fraud) the penalty goes up. Virus writing is also illegal, even if you don't distribute it yourself. DDoS is specifically covered by the act.

4 Copyright, Designs and Patents Act

This law gives an individual or organisation the right to control a piece of original work. The act applies equally to digital content (eg, movies and music) as it does to content in more traditional forms (eg, movies on a DVD or a piece of sheet music). In 1992, the act was extended to cover computer programs. A patent allows an original idea (within certain fields) to be protected. Most work is protected for 70 years after the death of the creator, although some categories have shorter protection periods. Computer Networks (and the internet) have made it very easy to share files, this can be a good thing for creators who wish to share their work but it also makes it easier to plagiarise and/or illegally distribute the work. It is a common misconception that because something is freely available on the internet, it can be copied; this is not the case. There are different forms of distribution available, some which require certain citations to the creators, some which don't require citations and some which allow modification and redistribution. The illegal distribution of digital content can be prevented (or made more difficult) by some types of hardware and software control. This is very important because lots of people are moving away from owning physical media and moving towards just streaming content.

4.1 Digital Rights Management

Digital Rights Management (DRM) is used to prevent unauthorised distribution of material. DRM is a set of access control tools which can limit how long the material is accessed for, the number of devices it can be used on, or prevent the copying of data all together.

4.1.1 Piracy

Piracy is the illegal copying of software or data without regard to copyright. The internet has made the distribution of pirated materials much easier to achieve and much harder for law enforcement to detect and stop.

4.2 Software Licences

Software authors can choose to licence their software, this could be a paid-for licence or a free licence (allows the program to be distributed for free while retaining the copyright).

4.2.1 Cracked Software

There are illegal methods available for distributing "cracked" versions of software. This is where the software may have been copied illegally or contain extra code which avoids requirements placed by the software's author (eg, to avoid needing a licence key).

4.2.2 Always Connected Protection

Software developers have begun to use the always connected nature of the internet to verify the legitimacy of an installation of an installation of a piece of software. There has been controversy around this, with some console users unable to use their console until the decision to use always connected verification was overturned.

5 Challenges Facing Legislators

There are a number of challenges which legislators face.

5.1 Global Networks

Laws vary from country to country. This poses a challenge to legislators as content that is deemed illegal in one country may not be illegal in the country where the website is hosted.

5.2 Tracking Down Criminals

Law enforcement agencies can use information collected by internet service providers and mobile phone companies to track down criminals. Access to digital devices' storage can provide evidence to enable prosecutions.

5.3 Access to Encryption Keys

There is often contention between a person's right to privacy and the need to keep people safe online. An example of this encryption allows transactions ot be secure and allows communications to be private; it also allows paedophile rings to operate and terrorists to communicate in secret. Some countries have legislation where companies have to hand over encryption keys on the order of a magistrate; in some countries data must be decrypted or keys supplied on ministerial order and in some countries there is no legislation surrounding this therefore companies don't have to do anything.

5.4 The Dark Web

This is a part of the internet that must be accessed through specialist software and hosts a wide range of mainly illegal content.