

Professional Computing Revision Notes

James Brown

April 17, 2017

Contents

1 Introduction 1

2 English Law 1

2.1 What is Law? 1

2.2 Criminal Law versus Civil Law 1

2.3 Torts 1

3 The Computer Misuse Act 1

3.1 Section 1 2

3.2 Section 2 2

3.3 Section 3 2

4 Data Protection Act 2

5 Regulation of Investigatory Powers 3

6 Freedom of Information Act 4

1 Introduction

These are notes I have written in preparation of the 2017 Professional Computing exam. This year the module was run by Iain Styles (I.B.Styles@cs.bham.ac.uk). I shall put an emphasis on topics I think are required for the essay question in the exam - 'Identify and discuss the ethical issues that the combination of big data analytics and video surveillance (including the use of drones) raises, and use your findings to critically analyse Mr Porter's position' - although I will cover all topics in at least some capacity for the multiple choice section. As these notes are public, I must point out that **I am not a lawyer**. None of the information in these notes should be used as legal advice, please see a lawyer for that.

2 English Law

2.1 What is Law?

Law is a complex and difficult entity and can be described as 'a set of laws which can be enforced by a court'. The law is more than just a simple set of rules - there are different systems of courts, different rules concerning how appeals are made and different rules which define how new laws work with old laws. Laws have **jurisdiction** - which is the geographical area which is governed by a single set of laws. For example, the Jurisdiction of English law is England, but the jurisdiction of California state law is solely California, and none of the other states within the USA. Jurisdiction is often not completely obvious in computer use. This means an offence involving a computer may involve laws applicable in other geographical areas than where you are currently sitting.

2.2 Criminal Law versus Civil Law

Criminal law is designed to protect society as a whole from wrongdoers. In all cases, the stance of 'innocent until proven guilty' is taken, and the offender must be proven **guilty beyond reasonable doubt**.

Civil law is for settling disputes between people (we can also count companies as people) and decisions are made based on the 'balance of probabilities'. Usually the objective of a civil law case is to obtain damages (money) or an injunction (court order). Litigation must be brought by one party of the dispute (the plaintiff) against another (the defender). This module mostly concerns itself with civil law.

2.3 Torts

In common law, a tort is a civil wrong. The action may not necessarily be criminal or even illegal but has somehow caused harm. Torts are usually re-addressed through damages which are awarded. Possible causes of torts are negligence, nuisance or defamation (libel and slander). An example of a tort may be copy and pasting some broken code as a software engineer. This may not be against any contract signed, but would be negligence and break the duty of care, and as such can be considered a civil wrong.

3 The Computer Misuse Act

The **Computer Misuse Act** of 1990 covers three offences:

- Unauthorized access to a computer
- Unauthorized access to a computer to commit a serious crime
- Unauthorized modification of the contents of a computer

A person can be found as guilty of a crime violating the Computer Misuse act if either they or the computer in question is located in the UK at the time of the offence.

3.1 Section 1

A person is guilty of an offence if they cause a computer to perform any function with intent to secure access to any program or data held in any computer; the access they intend to secure is unauthorised; and they know at the time when they cause the computer to perform the function that this is the case. An offence committed is punishable by a fine of up to 5000 or 6 months imprisonment.

Key points:

- Knowledge that you didn't have access and intent to secure access
- Just attempt is sufficient to be prosecuted
- There is no requirement for damage to be done

3.2 Section 2

Section 2 covers unauthorized computer access to commit a more serious crime. For example, a blackmailer might hack into an email to gain evidence of an affair. It's not necessary for the crime to be carried out, intent to commit the crime just has to be shown. Punishment can be up to five years imprisonment or an unlimited fine.

3.3 Section 3

A person is also guilty of an offence if they do any act which causes an unauthorized modification of the contents of any computer; and at the time when they do the act they have the requisite intent and the requisite knowledge. Requisite intent covers:

- To impair the operation of any computer
- To prevent or hinder access to any program or data held in any computer
- To impair the operation of any such program or the reliability of any such data

The maximum penalty is five years imprisonment or an unlimited fine. Examples of offences that would oppose section three are spreading a virus, installing ransomware or even redirecting a browser homepage.

4 Data Protection Act

The UK introduced the Data Protection Act in 1984. It was designed to protect individuals against the use of inaccurate or incomplete personal information, the use of information by unauthorised persons and the use of information for reasons other than that it was collected for. In 1998, the Data Protection Act underwent a major revision, which included a number of new definitions:

- **Data:** information that is being processed automatically or is collected with that intention or recorded as part of a 'relevant filing system'.
- **Processing:** obtaining, recording or holding data or carrying out any operation on it.
- **Data Controller:** Who controls why or how the data is processed.
- **Data Processor:** Anybody who processes the data on behalf of the data controller.
- **Personal Data:** Data which relates to a living person who can be identified using this data (possibly with other data the DC might have).
- **Sensitive Data:** Personal data relating to racial, ethnic, religious, political, sexual (etc.) aspects of a person.

The revised data protection act was also comprised of many principles which must be abided by.

The 1st **principle** states that data will be processed fairly and lawfully and in particular will not be processed unless (a) at least one condition in schedule 2 is met and (b) in the case of sensitive data at least one condition in schedule 3. Schedule 2 states that consent is given or there is some legal obligation to process the data (for example, tax returns or law enforcement). Schedule 3 states that *explicit* consent is given.

The 2nd **principle** states that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes. In short, data cannot be collected just in case it ends up being useful.

The 3rd **principle** states that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is collected. This is often broken without thinking and by accident - an example includes asking for marital status when you are signing up to join a library.

The 4th **principle** states that personal data should be accurate and where necessary kept up to date - this can be very hard to achieve in actual practice.

The 5th **principle** states that personal data processed for any purpose or purposes should not be kept for longer than it is necessary for that purpose or those purposes. This poses a further question: how long is enough?

- Financial data must be kept for up to 7 years for auditing purposes.
- Common advice is that emails should be kept for 7 years
- University exam results may be kept indefinitely
- CCTV data is routinely deleted after one month - this practice has implications for freedom of information requests.

All procedures for data deletion must be rigorous and specified - this includes the deletion of backed up data.

The 6th **principle** states that personal data should be processed in accordance with the rights of the data subjects under this act.

The 7th **principle** states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to personal data. In short - security is a legal requirement.

The 8th **principle** states that personal data shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in the relation of processing data. This specifically allows companies to transfer data over national boundaries.

5 Regulation of Investigatory Powers

The Regulation of Investigatory Powers Act (2000) is a framework for lawful interception of computer, telephone and postal messages. It allows ISPs and most employers to monitor communications without consent provided they are doing it to:

- Establish facts
- Ensure company regulations are being complied with
- Ascertain standards which ought to be achieved
- Prevent crime
- Investigate unauthorised use of telecommunications systems
- Ensure effective operation of systems (for example, detecting denial of service attacks)
- Find out whether a communication is business or personal

- Monitor but not record calls to confidential counselling helplines run free of charge by the business.

Any organisation monitoring communications without consent is required to make reasonable efforts to inform users that such interception might take place. RIPA also allows government agencies to ask for interception warrants to monitor communications to or from specific persons or organisations - for example the police, inland revenue or local councils. Councils are now limited to cases involving criminal offences that have at least a potential tariff of six months imprisonment.

6 Freedom of Information Act

The Freedom of Information act is an act to provide clear rights of access of information held by bodies in the public sector - with certain conditions and exceptions.

Index

civil law, 1
computer misuse act, 1
criminal law, 1

data, 2
data controller, 2
data processor, 2
data protection act, 2
defender, 1

internet service provider, 3

jurisdiction, 1

personal data, 2
plaintiff, 1
processing, 2

regulation of investigatory powers act, 3

sensitive data, 2

tort, 1