Professional Computing
Revision Notes

James Brown

April 12, 2017

Contents

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 a 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 is 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

5 Freedom of Information Act

Index