Economics & Law

Computer Science Tripos Part 1B

UK Law and the Internet

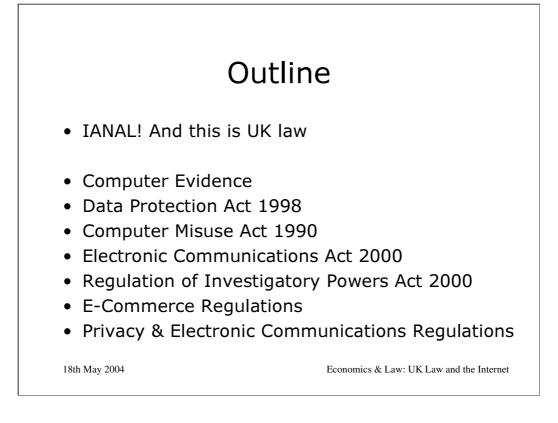
18th May 2004

Richard Clayton

These lecture notes were specially prepared for the Cambridge University Computer Science "Economics & Law" course, Easter Term 2004.

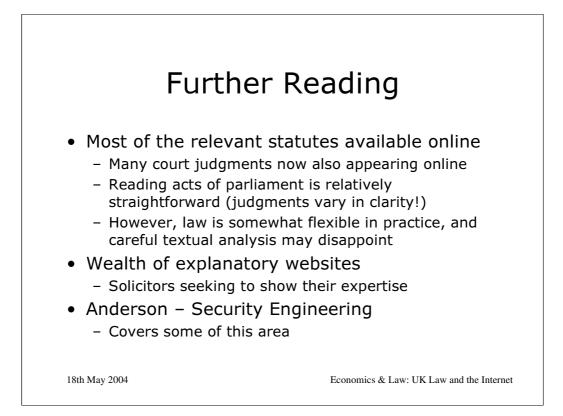
© Richard Clayton 2002, 2004

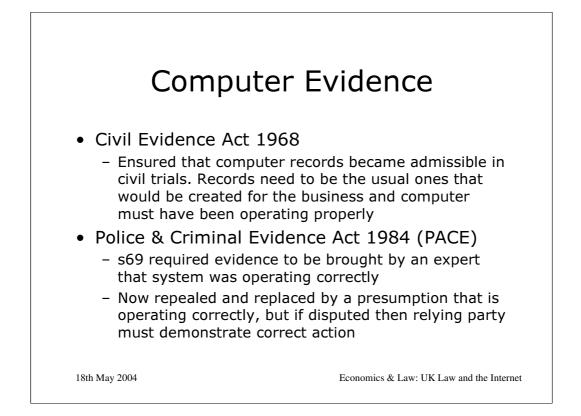
richard.clayton@cl.cam.ac.uk



The slides give the broad outline of the lectures and the notes ensure that the details are properly recorded, lest they be skipped over on the day. However, it is at least arguable that it will be far more interesting to take notice of what I say off-the-cuff rather than relying on this document as an accurate rendition of what the lecture was really about!

Also, please note that "IANAL" (I am not a lawyer). Consult a professional if you wish to receive accurate advice about the law!



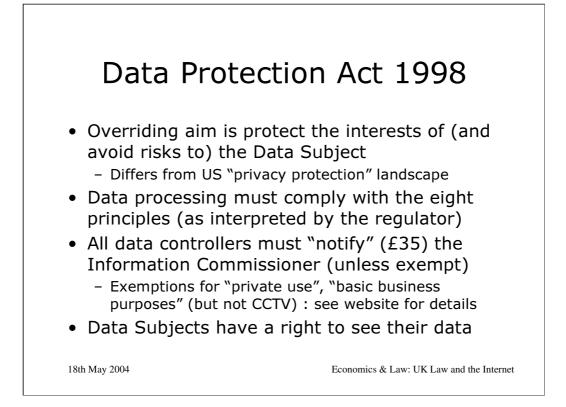


★ The 1968 Civil Evidence Act removed any possibility of computer evidence being labelled as "hearsay". It has since been amended by the Civil Evidence Act 1995, which clarified what a document was – to cover maps, plans, films and even computer databases. In general, authenticity is not an issue in civil trials because of the discovery process. But, if the correctness of the document is disputed then evidence of authenticity will be required.

* PACE 1984 required (expert) evidence that a machine was working properly. This caused practical problems and some strange decisions for a while (as in *DPP v McKeown* where a faulty clock on a breathalyser caused considerable confusion in lower courts; in 1997 the House of Lords eventually decided it was irrelevant to the operation of the device.)

★ PACE s69 was repealed by the Youth Justice and Criminal Evidence Act 1999. No special conditions are now necessary for the production of "hearsay evidence" produced by a computer. In the absence of evidence to the contrary, the courts will presume that the system was working properly. If there is evidence to the contrary, then the party seeking to rely on the evidence will need to prove that it was working.

* The Munden miscarriage of justice shows that system design must allow for "hostile" inspection (see: http://catless.ncl.ac.uk/Risks/18.25.html#subj5)



★ The Data Protection Act 1998 is now fully in force. The text of the Act is online at http://www.hmso.gov.uk/acts/acts1998/19980029.htm and there is a wealth of advice on the Information Commissioner's site at:

http://www.informationcommissioner.gov.uk/

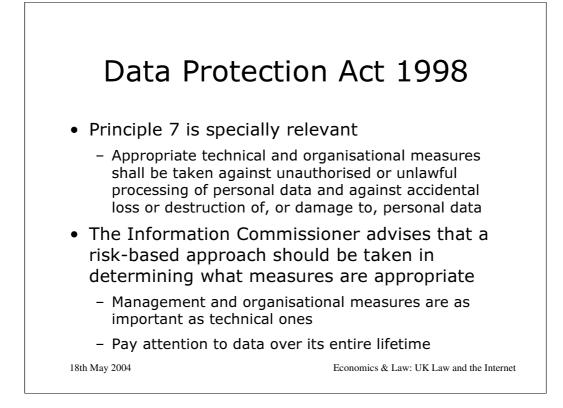
* Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than in the 1984 Act. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'.

★ Exemptions from notification are complex – see the website for details

* Data Subjects may be charged (but not more than £10) for access to data. Many organisations will incur costs that are far higher than this.

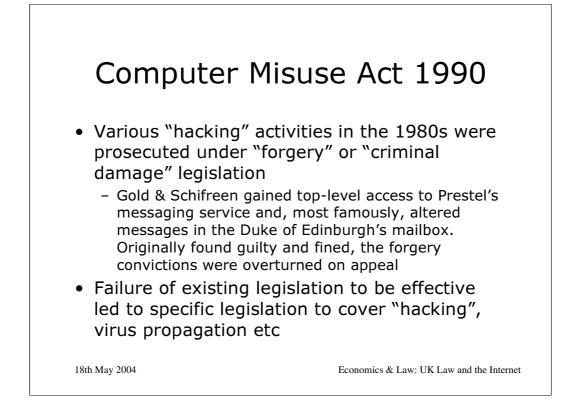


★ The Act has specific requirements with regard to Principle 7:

unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

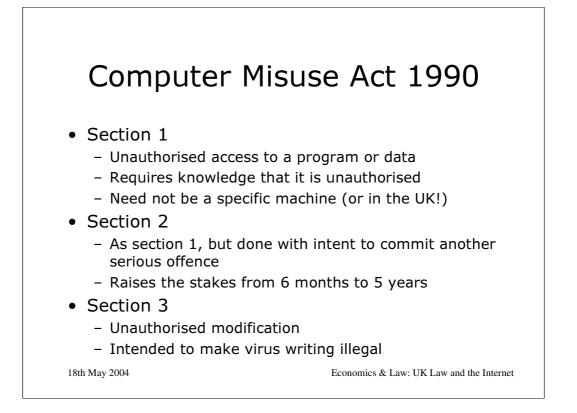
(b) the nature of the data to be protected.

 $s\left(10\right)$ The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.



★ For a racy account of hacking in the 1980s see (especially Chapter 2 of) "Approaching Zero":

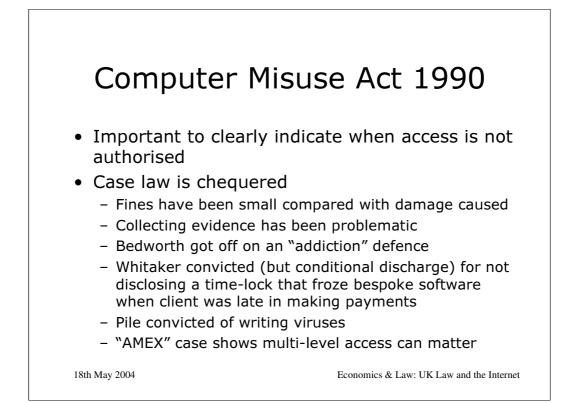
http://www.insecure.org/stf/approaching_zero.txt



\star The Act can be found online at:

http://www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

★ For a contemporary view of the Act see the All-Party Internet Group Inquiry pages: http://www.apig.org.uk/computer_misuse_act_inquiry.htm where you will find that some people are unhappy about the "definition" of computer, some people think that (Distributed) Denial of Service attacks are not covered by the Act (others disagree), and many wish to see the 6 month sentence for s1 offences raised (in the case of the Home Office, to 2 years).



* A typical warning, that could assist in bringing CMA prosecutions,

would be: This machine is the property of xxx Ltd. Only authorised users are entitled to connect to and/or log in to this computing system. If you are unsure whether you are authorised, then you are not and should disconnect immediately.

* *R. v. Bedworth 1991* It was alleged that Bedworth & two others modified code at the Financial Times share index, and disrupted research work at a European Cancer foundation. Two pleaded guilty. Bedworth argued that he had developed an addiction to computer use, and as a result was unable to form the intent which has to be proven under the statute. The jury acquitted.

★ *R. v. Pile 1995* Christopher Pile (aka the 'Black Baron') got 18 months under CMA s3. Pile pleaded guilty to five charges of gaining unauthorised access to computers, five of making unauthorised modifications and one of inciting others to spread the viruses he had written. Pile has created "two vicious and very dangerous computer viruses named 'Pathogen' and 'Queeg'".

* *R. v. Bow Street Magistrates Court and Allison: Ex Parte Government of the United States 1999* Allison was to be extradited to the USA for accessing American Express information about credit cards (used to steal \$1million from ATMs). The House of Lords held that although Allison was authorised to access some information, he did not have authorisation to access the relevant information. This effectively overturned the decision in *R.v.Bignell 1997* where access to data on the Police National Computer (about who was parked outside an ex-wife's house) was held not to be unlawful, because the police officers involved were authorised to access the system.

Electronic Communications Act 2000

- Part I voluntary licensing regime
 - For "cryptographic support service" providers
 - Sunset clause if not activated before May 2005
- Part II electronic signatures
 - Electronic signatures "shall be admissible in evidence"
 - Creates power to modify legislation for the purposes of authorising or facilitating the use of electronic communications or electronic storage
- s14 prohibits key escrow
- Remaining parts of EU Electronic Signature Directive were implemented as SI 318(2002)

18th May 2004

Economics & Law: UK Law and the Internet

The Electronic Communications Act 2000 is online at: http://www.hmso.gov.uk/acts/acts2000/20000007.htm

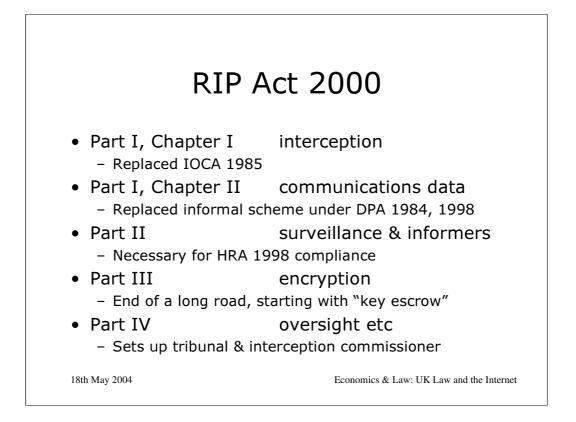
★ The voluntary licensing scheme is the last vestige of the "key escrow" proposals of the mid 1990s when the NSA (and others) tried to grab the world's keys to mitigate the effects of the use of encryption upon their snooping activities. The DTI hopes that the industry initiative called tScheme (http://www.tscheme.org/) will succeed and there will be no need for the DTI to create an approvals body. s14 is present to ensure that everyone understands that the old policies are dead.

★ Electronic signatures were probably effective (certainly in England & Wales) before this Act was passed. However, there's now no doubt that courts can look at them and weigh them as evidence.

★ The Government decided against a global approach to amending legislation (i.e. anywhere it says "writing" then email would be OK) but is instead tackling topics one at a time. Perhaps the most visible change so far is the option to take delivery of company annual reports by email. There are also significant changes at HM Land Registry, where electronic conveyancing of land is on the horizon (perhaps with a pilot in 2005).

★ Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/ 1_013/1_01320000119en00120020.pdf Transposed, very literally, into UK Law (rather late) as Statutory Instrument 2002 No 318

http://www.hmso.gov.uk/si/si2002/20020318.htm



- The Regulation of Investigatory Powers Act 2000 can be found online at: http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
- ★ A history of interception in the UK (from 1663 onwards) can be found at: http://www.homeoffice.gov.uk/docs/intera.html#Chapter%202

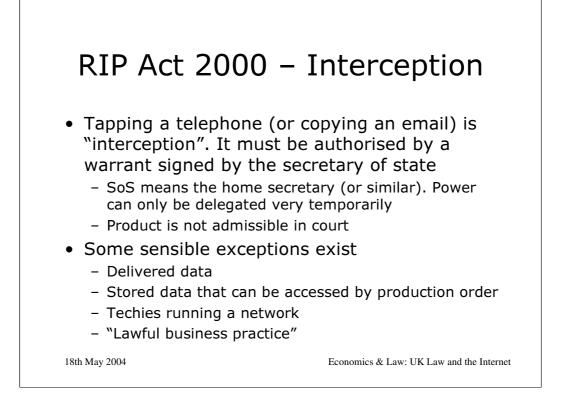
The judgement of the European Court of Human Rights in *Malone* made legislation necessary and the Interception of Communications Act 1985 (IOCA) was the result. The 1997 *Halford* decision (relating to interception on private networks) showed that the law needed revision.

★ Access to communications data was previously done using the exemptions provided by s28 of DPA 1984 (s29 in DPA 1998). The form used in the ISP industry can be seen at:

http://www.linx.net/misc/dpa28-3form.html

★ Surveillance, bugging and the use of informers needed to be formally regulated so that these activities did under infringe Article 8 of the European Convention on Human Rights ("right to privacy").

★ The Government proposed numerous policies through the late 1990s which were intended to address the problems caused by the use of encryption by criminals. Eventually compulsory "key escrow" was dropped and we have ended up with the requirement to "put into an intelligible form" along with some GAK (Government Access to Keys).



```
(b) so monitors transmissions made by means of the system, or
```

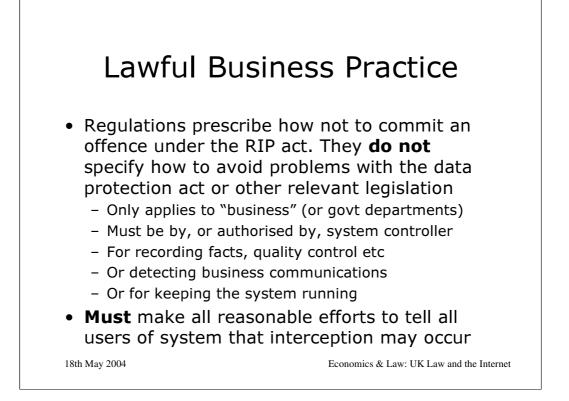
(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

* Note that once the data has reached its destination then it's no longer interception. However, storage so that the recipient can collect it or have access to it doesn't count as the destination. So it's interception to look at maildrops or undelivered SMS messages.

* Interception is lawful if both the sender and recipient has given permission s3(1) or s3(2) if the recipient has and the police have a Part II warrant (this is the "tap the kidnapper's call" scenario).

* Techies working for the communications service provider can lawfully intercept [s3(3)] if what they're doing is required for the provision or operation of the service. This means that filtering for viruses is lawful, as is sniffing network traffic for diagnostic purposes.



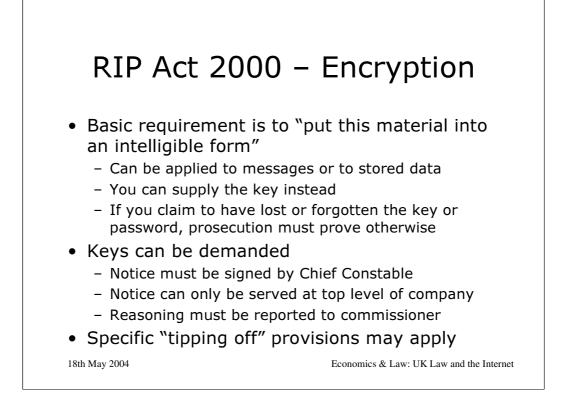
 Statutory Instrument 2000 No. 2699 : The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm

★ The Information Commissioner has a Code of Practice on employer/employee issues regarding data protection and monitoring. As usual, the URLs are quite dreadful:

http://www.informationcommissioner.gov.uk/cms/DocumentUploads/The%2 0Employment%20Practices%20Data%20Protection%20Code%20Part%203% 20Monitoring%20at%20work.pdf

Other Codes of Practice are linked from:

http://www.informationcommissioner.gov.uk/eventual.aspx?id=437



★ Part III is not yet in force, and there is not even a draft for the Code of Practice which will (possibly) answer a whole lot of practical questions about how this part of the Act will operate. At present, the Home Office have no plans to implement this part of the Act, but this could change at any time.

★ Details about the notice that is served are given in s49. You will get a reasonable time to comply and access to your keys. You can provide the key instead of the data – which might be a sensible thing to do where a message is being sought and the "session key" can be provided. If you only have a partial key then you must hand that over, or if you don't have the key but know where it can be located then you must report where it can be found.

★ In "special circumstances" you can be required to hand over a key. The notice has to be signed by a Chief Constable (or customs/military/security services equivalent) and the circumstances must be reported to the Chief Surveillance Commissioner (or in some cases the Intelligence Services Commissioner). If such a notice is served on someone for a key that "belongs to the company" then it has to be served at board level.

These safeguards were added as the RIP Bill went through Parliament because there was considerable concern expressed by industry that the UK would not be a safe place to keep encryption keys. It has yet to be seen whether industry will move systems abroad to meet a perceived GAK threat.



* The Consumer Protection (Distance Selling) Regulations. Statutory Instrument 2000 No 2334.

http://www.hmso.gov.uk/si/si2000/20002334.htm There are useful explanatory notes on DTI website:

http://www.dti.gov.uk/ccp/topics1/guide/distsell.htm Applies to Internet, Phone, Mail Order, Fax even television selling. Enforced by Trading Standards. Ensures that consumer knows who they are dealing with and what the terms are. Straightforward to comply with, but you do need to design compliance into your systems.

★ The Electronic Commerce (EC Directive) Regulations Statutory Instrument 2002 No 2013

http://www.legislation.hmso.gov.uk/si/si2002/20022013.htm Again there's useful guidance from the DTI: http://www.dti.gov.uk/ industries/ecommunications/electronic_commerce_SME_guide.pdf and http://www.dti.gov.uk/industry_files/pdf/businessguidance.pdf These apply if you sell goods by email or website (or run an ISP!).

★ Rome Convention (1980) addresses which country's law applies. B2B contract will say, consumer's law will apply unless your website addresses a particular country (eg: multiple languages, prices in Euro etc).

http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction_rome.htm The Brussels Regulation (and Brussels Convention and Lugano Convention !) address which court it will be heard in. Similar rules as above:

http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction_brussels.htm

Privacy & Electronic Communications

- Implementing EU Directive 2002/58/EC
- Replaces existing Directive (& UK Regulations)
- Rules on phone directories, location info etc
- Bans unsolicited marketing email to natural persons – but not to legal persons)
 - but see your ISP's "acceptable use policy"
- Controls on the use of "cookies"
 - transparency: so should avoid, or provide a choice
 - or if essential, then tell people what you're doing

18th May 2004

Economics & Law: UK Law and the Internet

 EU "Directive on Privacy and Electronic Communications" http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/ l_20120020731en00370047.pdf

★ UK implementation in "The Privacy and Electronic Communications (EC Directive) Regulations 2003"

http://www.hmso.gov.uk/si/si2003/20032426.htm

★ Unsolicited marketing communications subject to "soft opt-in" rules; viz: OK if person has given their permission (not really unsolicited then!) and also OK if person has purchased (or negotiated for the purchase) of something with the SAME company AND the email (or SMS) is promoting a "similar" product or service. ISP contracts apply a more rigorous interpretation of what is acceptable behaviour:

> http://www.linx.net/noncore/bcp/ube-bcp.html http://www.linx.net/noncore/bcp/mailinglist-bcp.html

★ Cookie rules hidden away in s6: of which this is an extract: a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless ... the subscriber or user of that terminal equipment - (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and (b) is given the opportunity to refuse the storage of or access to that information... etc etc



The Anti-terrorism, Crime and Security Act 2001 is online at: http://www.legislation.hmso.gov.uk/acts/acts2001/20010024.htm

It contains a little of everything (e.g. s47(1)(a) makes it an offence to knowingly cause a nuclear weapon explosion). Part 11 provides the framework for a Code of Practice for the retention of logging data. If your system provides communication services then you may well be expected to comply. However, the CoP will be voluntary unless the Secretary of State decides that it is not working.

- ★ Convention on Cybercrime
 - http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

to be ratified by the UK it will require a Computer Misuse Act v2.0 (or other legislation) making illegal "the production, sale, procurement for use, import, distribution or otherwise making available of" "hacking tools" or "passwords". However since these things are "dual use" the law will only make it illegal if you're doing it for bad reasons and not for good, "such as for the authorised testing or protection of a computer system".



- Computer evidence is admissible in court
- Electronic signatures are admissible in court
- Hacking is illegal!
- Interception is illegal
 - Though there are sensible exceptions, provided you jump through the appropriate hoops
- E-Commerce is simple within one country
- Understanding the basics of what the law means and requires does not require you to study to become a lawyer!

18th May 2004

Economics & Law: UK Law and the Internet

Ignorance of the law excuses no man; not that all men know the law; but because 'tis an excuse every man will plead, and no man can tell how to confute him.

John Selden (1584-1654)