Economics & Law

Computer Science Tripos Part 1B

UK Law and the Internet

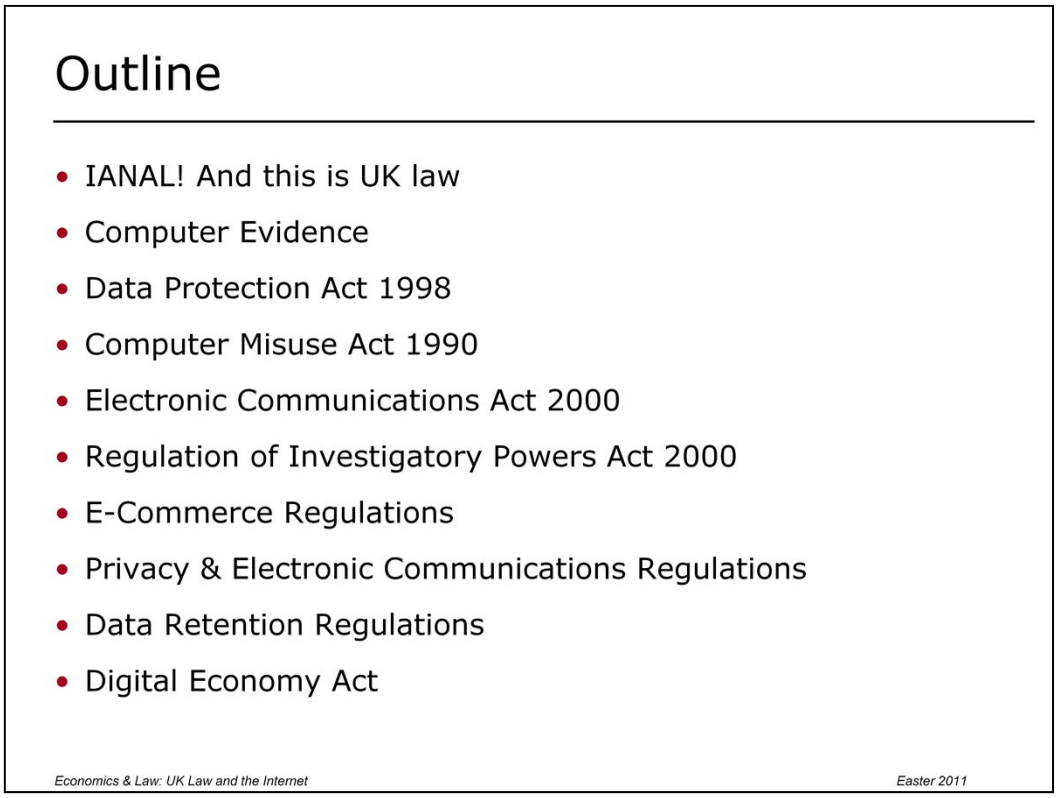
Easter 2011

~~Richard Clayton~~

Jack Lang

These lecture notes were specially prepared for the Cambridge University Computer Science "Economics & Law" course, Easter Term 2011.

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!

Further Reading

- Most of the relevant statutes available online
  - Many court judgments now also appearing online
  - Reading acts of parliament is relatively straightforward
  - Judgments (case law) varies in clarity!
  - However, law is somewhat flexible in practice, and careful textual analysis may disappoint – it's not a programming language
- Wealth of explanatory websites
  - Solicitors seeking to show their expertise
- Anderson – Security Engineering
  - Covers some of this area

Economics & Law: UK Law and the Internet *Easter 2011*

Raw statutes, from 1988 onwards (and statutory instruments from 1987) are published at:

`http://www.opsi.gov.uk/legislation/uk.htm`

Consolidated versions of statutes (albeit with some complex exceptions and limited application of the most recent changes) are published at:

`http://www.statutelaw.gov.uk/`

Computer Evidence

- Civil Evidence Act 1968
  - Ensured that computer records became admissible in civil trials. Records need to be the usual ones that would be created for the business and computer must have been operating properly
- Police & Criminal Evidence Act 1984 (PACE)
  - Initially, s69 required evidence to be brought by an expert that system was operating correctly
  - Now repealed and replaced by a presumption that the computer is operating correctly, but if disputed then relying party must demonstrate correct action

Economics & Law: UK Law and the Internet *Easter 2011*

✶ 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)

Data Protection Act 1998

- Overriding aim is to protect the interests of (and avoid risks to) the Data Subject
  - Differs from US "privacy protection" landscape
- Data processing must comply with the eight principles (as interpreted by the regulator)
- All data controllers must "notify" (£35) the Information Commissioner (unless exempt)
  - Exemptions exist for "private use", "basic business purposes" (but not CCTV) : see website for details
- Data Subjects have a right to see their data
  - Systems need to be designed for this right to be exercisable

Economics & Law: UK Law and the Internet *Easter 2011*

✶ 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.ico.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

Data Protection Act 1998

- Principle 7 is specially relevant
  - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- The Information Commissioner advises that a risk-based approach should be taken in determining what measures are appropriate
  - Management and organisational measures are as important as technical ones
  - Pay attention to data over its entire lifetime

Economics & Law: UK Law and the Internet *Easter 2011*

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

Schedule I, Part II:

s(9) Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to-

(a) the harm that might result from such 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(10) The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

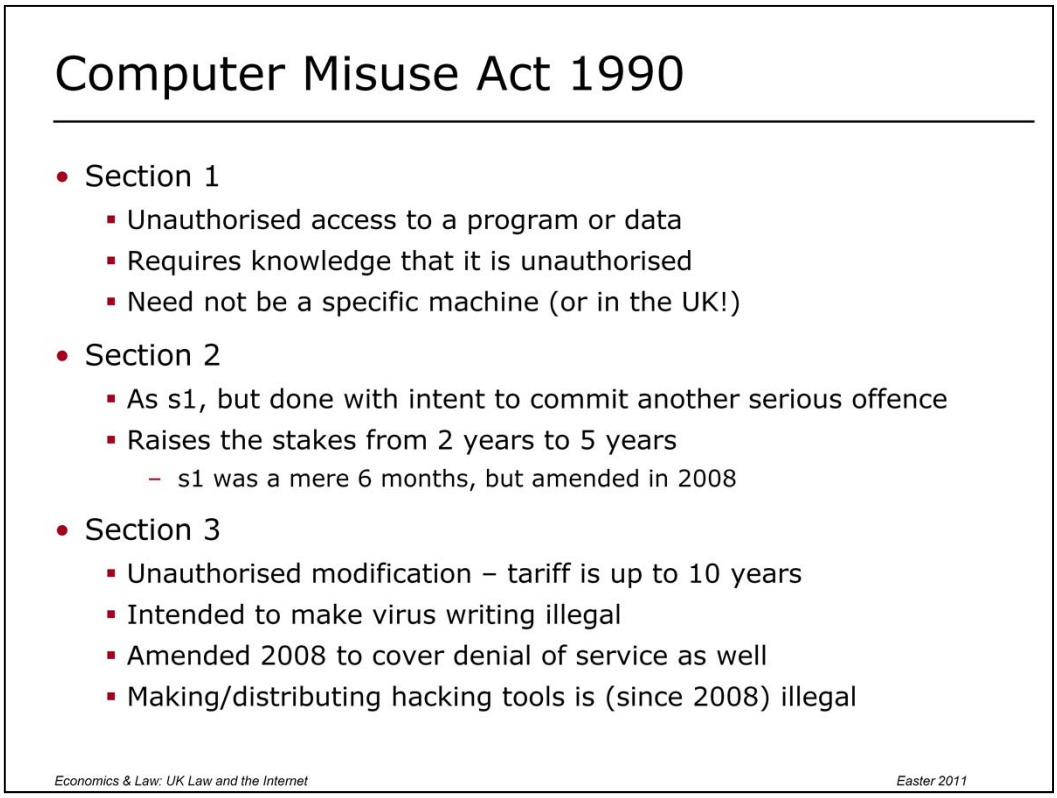
Computer Misuse Act 1990

- Various "hacking" activities in the 1980s were prosecuted under "forgery" or "criminal damage" legislation
  - Gold & Schifreen gained top-level access to Prestel's messaging service and, most famously, altered messages in the Duke of Edinburgh's mailbox. Originally found guilty and fined, the forgery convictions were overturned on appeal
- Failure of existing legislation to be effective led to specific legislation to cover "hacking", virus propagation etc

Economics & Law: UK Law and the Internet *Easter 2011*

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

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



✶ The Act can be found online at:

`http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm`

✶ The tariff changes in recent amendments were widely welcomed. Though do note (see *R. v. Lennon*) that not everyone gets the maximum sentence!

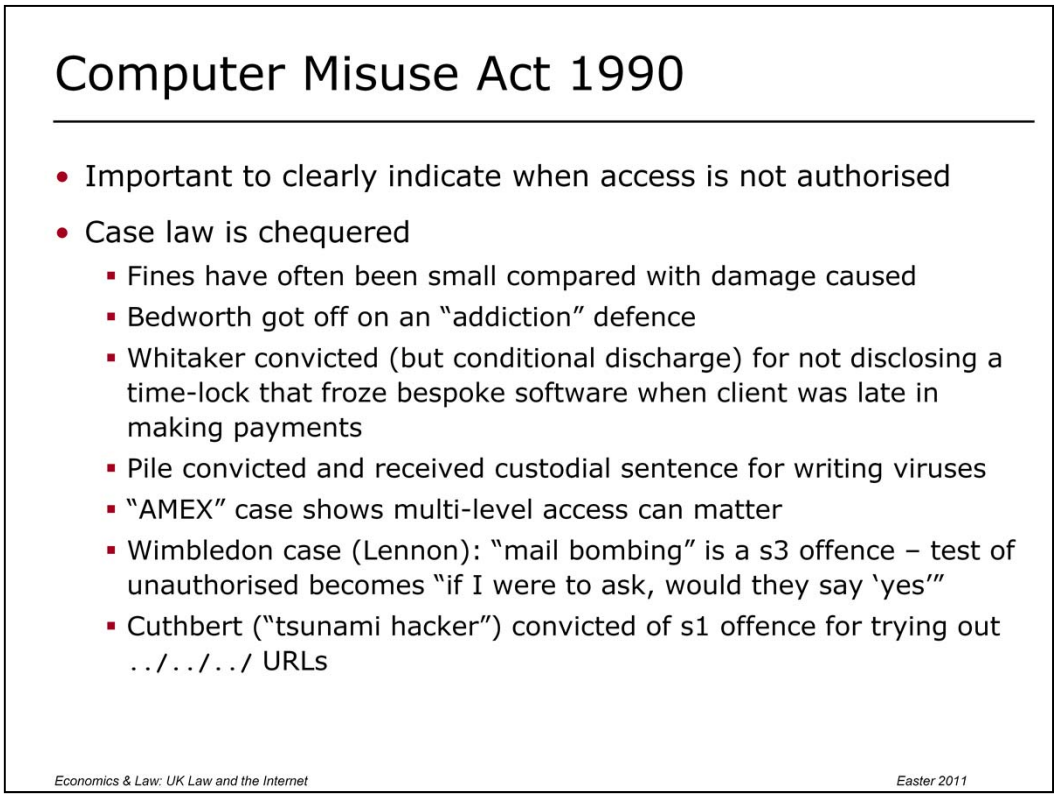
✶ The wording to cover "denial of service" looks plausible, but there will be significant interest in seeing if it works when the first test case occurs.

✶ The Council of Europe Convention on Cybercrime has been signed by the UK and will soon be ratified (now we have the amendments in place):

`http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm`

✶ The Convention requires the UK to make 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 should only make it illegal if you're doing it for bad reasons ("without right") and not for good, "such as for the authorised testing or protection of a computer system". Parliament settled on the need for "intent" for creating the tools (or just offering to create them) and likewise for "obtaining" (so the good guys have a defence because they have no intent to commit offences). However for distribution the wording is "likely to be used". The Director of Public Prosecutions has issued guidance on this:

`http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990`



✶ A typical warning, that could assist in 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.
```

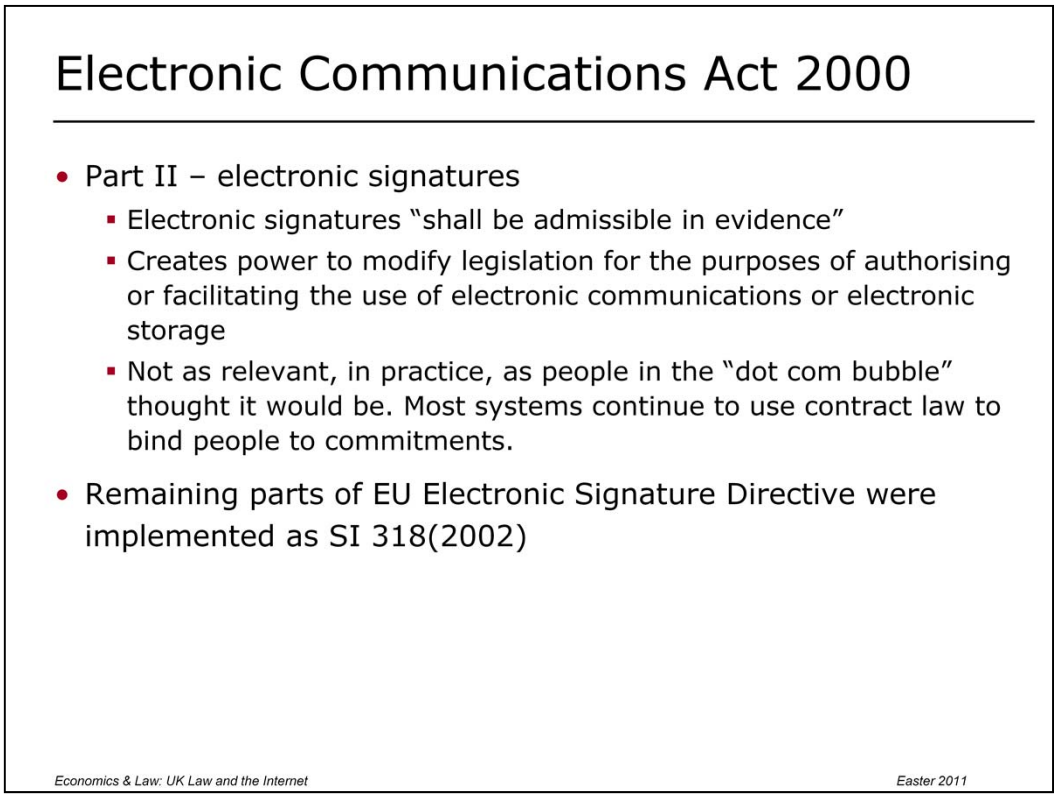
✶ *R. v. Bedworth 1991* It was alleged that Bedworth and two others modified code at the Financial Times share index, and disrupted research work at a European Cancer foundation. Two pleaded guilty. Bedworth argued that he had developed an addiction to computer use, and as a result was unable to form 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 (and an operator did the typing for them).

✶ *R. v. Lennon 2005* Lennon caused five million emails to be sent to an server, which was unable to cope with the load – a so-called "mail bomb". He was charged under s3(1). The defence argued that it was implicitly permitted to send email, and that there was no specific number at which permission ceased. The District Judge agreed, but the on appeal the court said "If he had asked if he might send the half million *(sic)* emails he did send, he would have got a quite different answer" and sent the case back for retrial. Lennon pleaded guilty and got a two month (electronically tagged) curfew.

✶ For a discussion of the *Lennon* and *Cuthbert* cases (and to see the perils of not being frank with the police at interview) see `http://pmsommer.com/CLCMA1205.pdf`



✶ The Electronic Communications Act 2000 is online at:

`http://www.hmso.gov.uk/acts/acts2000/20000007.htm`

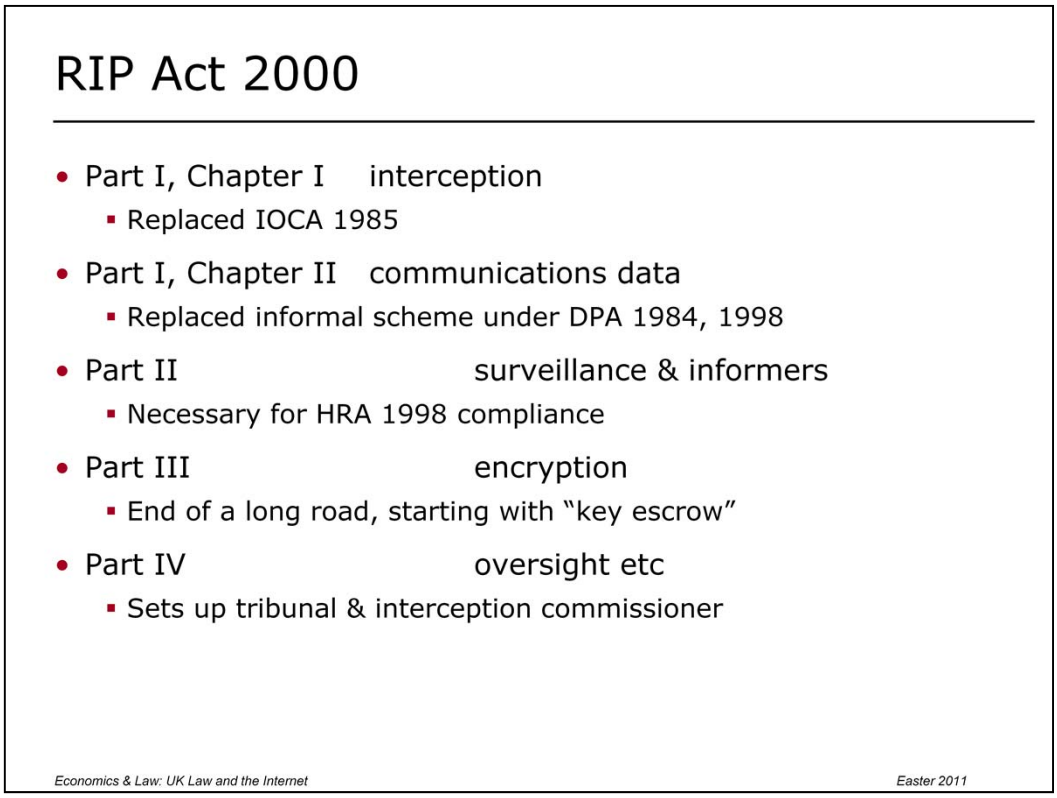
✶ The voluntary licensing scheme in Part I was the last vestige of the "key escrow" proposals of the mid 1990s when the NSA (and others) tried to grab the world's keys to mitigate the effects of the use of encryption upon their snooping activities. This part of the Act fell under a "sunset clause" on May 25th 2005. Note that 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 slowly coming to fruition (perhaps complete by 2015).

✶ Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures: `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN: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`

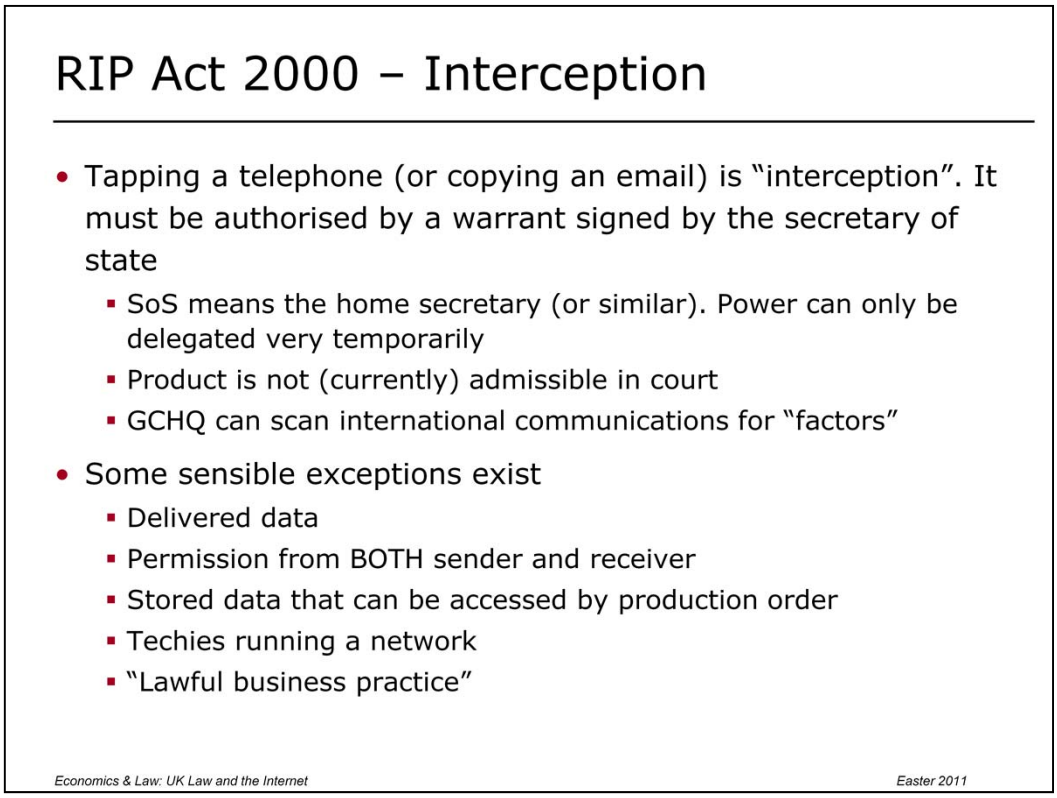
✶ A history of interception in the UK (from 1663 onwards) can be found at:
`http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/oicd/ioca.pdf`

✶ 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 by the ISP industry can be seen at:
`http://duncan.gn.apc.org/DPAFORM.htm`

✶ Surveillance, bugging and the use of informers needed to be formally regulated so that these activities did not 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).



✶ `s2(2) ...a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he-`
`(a) so modifies or interferes with the system, or its operation,`
`(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.

✶ In *R v Stanford & Liddell 2005* an email server was configured so that emails to the CEO of Redbus were copied to where the defendants could read them. The judge ruled that "right to control" does not mean has right of access or operation (passwords) but needed the right to authorise or forbid the interception. The defendants then changed their plea to guilty and received fines and suspended sentences.

Lawful Business Practice

- Regulations prescribe how not to commit an offence under the RIP act. They **do not** specify how to avoid problems with the data protection act or other relevant legislation
  - Only applies to "business" (or govt departments)
  - Must be by, or authorised by, system controller
  - For recording facts, quality control etc
  - Or detecting business communications
  - Or for keeping the system running
- **Must** make all reasonable efforts to tell all users of system that interception may occur

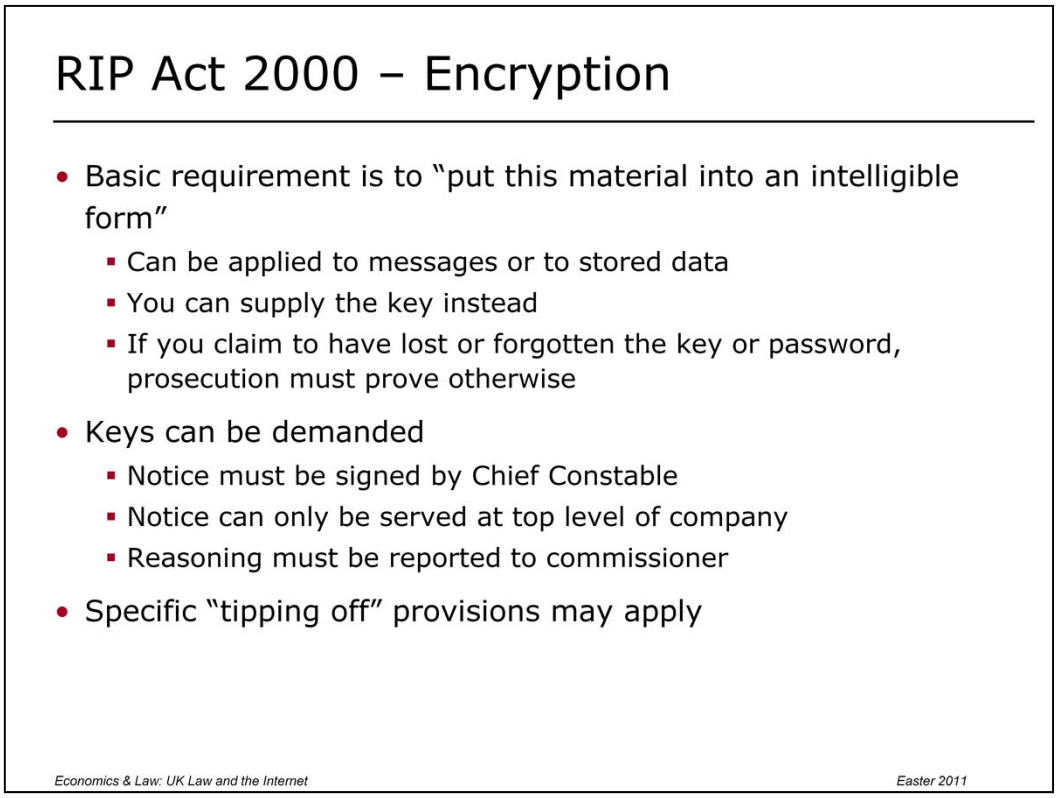
Economics & Law: UK Law and the Internet *Easter 2011*

✶ Statutory Instrument 2000 No. 2699 : The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

`http://www.opsi.gov.uk/si/si2000/20002699.htm`

✶ The Information Commissioner has a Code of Practice on employer/employee issues regarding data protection and monitoring. It also covers "lawful business practice". See Part 3:

`http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html`



✶ Part III finally came into force in October 2007. It has been retrospectively applied to data that was seized before it came into force.

✶ Details about the notice that is served are given in s49. You 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 the OFT website:

`http://www.oft.gov.uk/business-advice/treating-customers-fairly/distance-selling/`

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 at the above URL. These regulations apply if you sell goods by email or website (or run an ISP!).

✶ The 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://webarchive.nationalarchives.gov.uk/20070807090336/http://www.dti.gov.uk/consumers/consumer-support/resolving-disputes/Jurisdiction/rome/index.html`

The Brussels Regulation (and Brussels Convention and Lugano Convention !) address which court it will be heard in. Similar rules as above:

`http://webarchive.nationalarchives.gov.uk/20070807090328/http://www.dti.gov.uk/consumers/consumer-support/resolving-disputes/Jurisdiction/brussels/index.html`

✶ EU "Directive on Privacy and Electronic Communications"

`http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF`

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

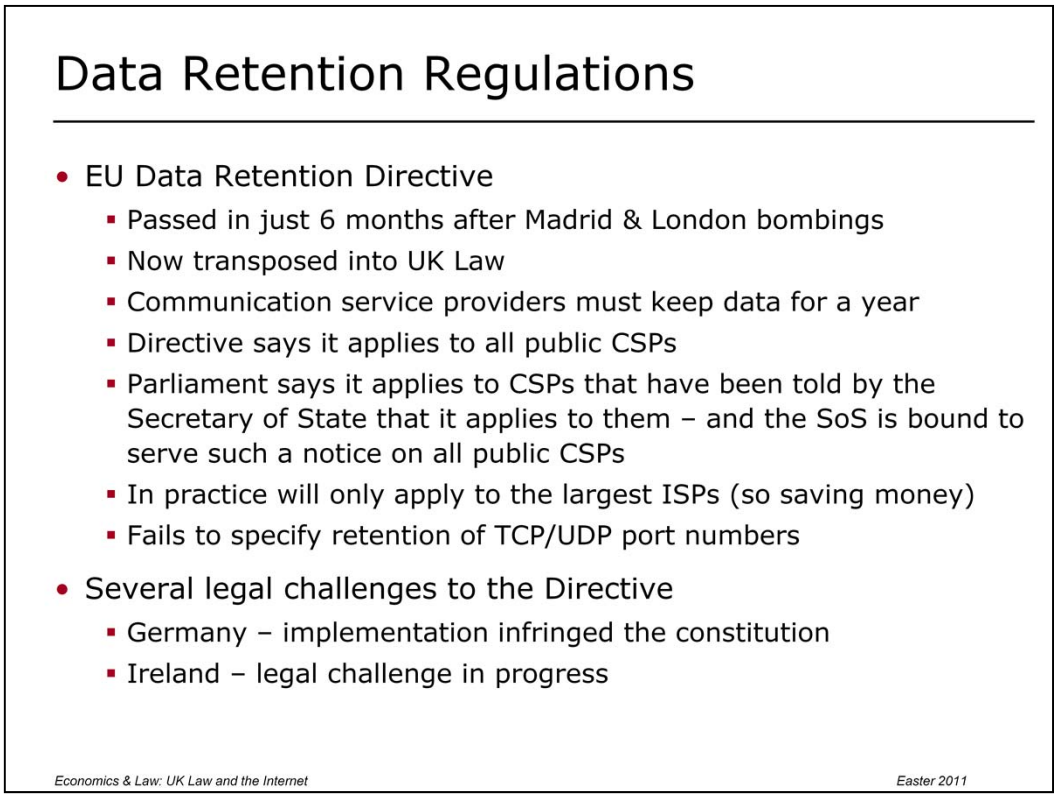
`http://www.opsi.gov.uk/si/si2003/20032426.htm`

✶ 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:

`https://www.linx.net/good/bcpindex.html`

✶ Cookie rules are 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
```



✶ EU Directive "on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks"

`http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF`

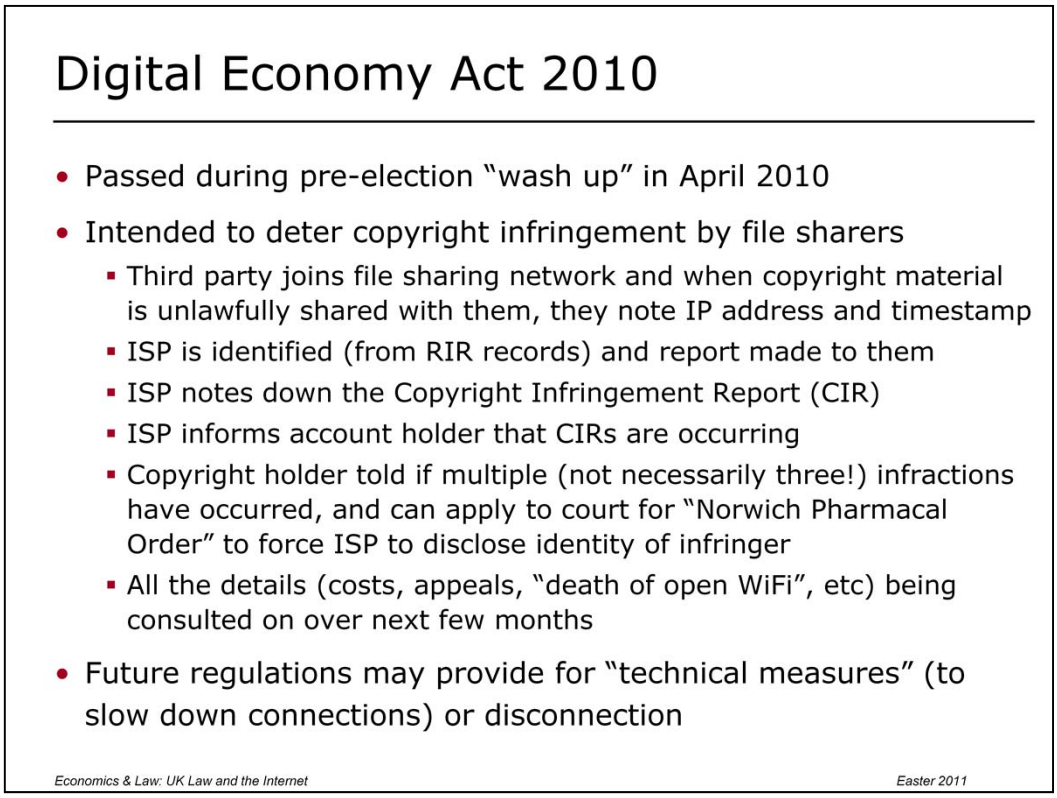
✶ The EU Directive was transposed for telcos in Oct 2007, and for ISPs as well in April 2009, by means of Statutory Instrument 2009 No. 859: The Data Retention (EC Directive) Regulations 2009

`http://www.opsi.gov.uk/si/si2009/uksi_20090859_en_1`

See s10(1) for the "it only applies to you if we tell you so" rule.

✶ The Directive (and the Regulations) are very didactic, and fail to require the retention of TCP/UDP port numbers. Widespread use of NAT by mobile providers drives big hole through the effectiveness of the regime.

`http://www.lightbluetouchpaper.org/2010/01/12/extending-the-requirements-for-traceability/`



✶ The Digital Economy Act 2010 can be found at:

`http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1`

✶ What it will actually mean in practice will depend on the content of the various codes of practice and on secondary legislation. There will be a number of (mainly) OFCOM consultations on these.

✶ Note that the "graduated response" that the Act envisages – with warnings followed by sterner measures is often called "three strikes". This name comes from early discussions of how it would work (inform, warn, disconnect). It currently seems unlikely that the number 3 will appear in the UK mechanisms.

✶ s17 of the DEA is a "Power to make provision about injunctions preventing access to locations on the internet". Expect some interesting discussions about likely effectiveness and proportionality when the secondary legislation to implement this is consulted upon.

Lots of other Legislation !

- Lots more E-Commerce stuff
  - Sale of Goods
  - Contract law
  - Unfair Terms
  - Unsolicited faxes
  - Etc etc etc
- Lots of rules for adult content
  - Indecent images of children – possession (+ making etc) is illegal
  - Extreme pornography – possession (+ making etc) is illegal
  - Obscene Publications Act – webmaster of foreign site was convicted
- Lots of other specialist issues
  - Selling age-restricted goods (& TV watersheds)
  - Fund-raising for political parties

Review

- 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
- Unlawful file sharing may affect your connectivity (& wallet)
- 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!

Economics & Law: UK Law and the Internet *Easter 2011*

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)