Security

Computer Science Tripos Part 2

UK Legislation

13th February 2002

Richard Clayton

These lecture notes were specially prepared for the Cambridge University Computer Science "Security" course, Lent Term 2002.

richard.clayton@cl.cam.ac.uk

Outline

- IANAL! and this is UK law

- Computer Evidence
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- European Electronic Signature Directive
- Regulation of Investigatory Powers Act 2000
- Copy Protection

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
  - reading Acts of Parliament is relatively straightforward
  - many court judgments now appearing online
- Wealth of explanatory websites
  - solicitors seeking to show their expertise
- Anderson - Security Engineering
  - covers some of this area

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)
  - s69 required evidence to be brought by an expert that system was operating correctly.
  - Now repealed and replaced by a presumption that is operating correctly, but if disputed then relying party must demonstrate correct action.

13th February 2002 Security : UK Legislation

✶ 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

- 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.
- 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

13th February 2002 Security : UK Legislation

✶ 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.dataprotection.gov.uk/

✶ 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

✶ For a racy account of hacking in the 1980s see:

http://www.ladysharrow.ndirect.co.uk/library/Books/appzero/approaching_zero%20chapter%202.htm

Computer Misuse Act 1990

- Section 1
  - Unauthorised access to a program or data
  - Requires knowledge that it is unauthorised
  - need not be a specific machine (or in the UK!)
- Section 2
  - As section 1, but done with intent to commit another serious offence
  - raises the stakes from 6 months to 5 years
- Section 3
  - Unauthorised modification
  - intended to make virus writing illegal

13th February 2002 Security : UK Legislation

✶ The Act can be found online at:

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

Computer Misuse Act 1990

- Important to clearly indicate when access is not to be authorised
- Case Law is chequered
  - fines have been small compared with damage caused
  - collecting evidence has been problematic
  - Bedworth got off on an "addiction" defence
  - Whitaker convicted (but conditional discharge) for not disclosing a time-lock that froze bespoke software when client was late in making payments
  - Pile convicted of writing viruses
  - "AMEX" case shows multi-level access can matter

13th February 2002 Security : UK Legislation

✶ 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.
```

✶ For a review of cases brought under the CMA 1990-1995 see:
http://csrc.lse.ac.uk/people/kelmana/CMA_AppendixA.htm

✶ *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 - Licensing regime
  - for "cryptographic support service" providers
  - entirely voluntary
  - 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

13th February 2002 Security : UK Legislation

✶ 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 (anywhere it says writing then email is 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.

European Signature Directive

- Introduces "advanced electronic signature"
- A "qualified certificate" links a person with a private key and is signed with an a.e.s.
  - other EU states must accept a qualified certificate
- Certification service providers issuing qualified certificates must meet stringent criteria
  - The certifier is legally liable (up to some limit) for the accuracy of the information on a qualified certificate and for ensuring it can be revoked
- The UK has not so far enacted this

13th February 2002 Security : UK Legislation

✶ "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures" is at: http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html

✶ 2(2) "advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

✶ Consultation on transposition (rather late) into UK Law is at: http://www.dti.gov.uk/cii/datasecurity/electronicsignatures/signatures.shtml

deadline for comments was 12th Feb !

✶ The proposed UK law will make the issuers of qualified certificates liable for damages regarding the accuracy of the information in their certificates, the sole ownership of the private keys and the timely existence of revocation information. The burden of proof will be on the issuer to prove they were not negligent.

RIP Act 2001

- Part I, Chapter I Interception
  - replaced IOCA 1985
- Part I, Chapter II Communications Data
  - replaced informal scheme under DPA 1984, 1998
- Part II Surveillance & Informers
  - necessary for HRA 1998 compliance
- Part III Encryption
  - end of a long road, starting with "key escrow"
- Part IV Oversight etc
  - sets up Tribunal & Interception Commissioner

13th February 2002 Security : UK Legislation

✶ The Regulation of Investigatory Powers Act 2001 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/oicd/intera.htm#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).

RIP Act 2001 - Interception

- Tapping a telephone (or copying an email) is "interception". It must be authorised by a warrant signed by the Secretary of State
  - SoS means the Home Secretary (or similar). Power can only be delegated very temporarily
  - Product is not admissible in court
- Some sensible exceptions exist
  - delivered data
  - stored data that can be accessed by production order
  - techies running a network
  - "lawful business practice"

13th February 2002 Security : UK Legislation

✶ 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.

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

13th February 2002 Security : UK Legislation

✶ 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 draft Code of Practice on employer/employee issues regarding data protection. It has proved to be somewhat controversial and nothing further has appeared since a consultation period ended in Jan 2001
http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

RIP Act 2001 - Encryption

- Basic requirement is to "put this material into an intelligible form"
  - can be applied to messages or to stored data
  - you can supply the key instead
  - if you claim to have lost or forgotten the key or password, prosecution must prove otherwise
- Keys can be demanded
  - notice must be signed by Chief Constable
  - notice can only be served at top level of company
  - reasoning must be reported to Commissioner
- Specific "tipping off" provisions may apply

13th February 2002 Security : UK Legislation

✶ Part III is not yet in force, and there is not yet 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.

✶ 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.

Copy Protection

- Copyright, Design and Patents Act 1988
  - s296 selling devices or publishing information about how to defeat copy protection is equivalent to a breach of copyright
  - s297 gives protection to pay-TV programmes
- Conditional Access (Unauthorised Decoders)
  - even more protection for pay-TV
- US has the Digital Millennium Copyright Act
  - hot topic!
  - being used to prosecute DeCSS cases
  - Felton is trying to get it declared unconstitutional

13th February 2002 Security : UK Legislation

✶ Copyright, Design and Patents Act 1988 is online at:
http://www.legislation.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

```
s 296(2) The person issuing the copies to the public has the
same rights against a person who, knowing or having reason to
believe that it will be used to make infringing copies—
(a) makes, imports, sells or lets for hire, offers or exposes
    for sale or hire, or advertises for sale or hire, any device
    or means specifically designed or adapted to circumvent the
    form of copy-protection employed, or
(b) publishes information intended to enable or assist persons
    to circumvent that form of copy-protection,
as a copyright owner has in respect of an infringement of
copyright.
```

Basically a civil issue, and there's been very little case law until recently.

✶ Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access:

http://europa.eu.int/eur-lex/en/lif/dat/1998/en_398L0084.html

was transposed into UK Law as Statutory Instrument 2000 No. 1175 The Conditional Access (Unauthorised Decoders) Regulations 2000

http://www.legislation.hmso.gov.uk/si/si2000/20001175.htm

it extended existing criminal offences of importing, advertising, selling or hiring unauthorised decoders to also include possession, installation or maintenance.

Lots of other Legislation !

- Anti-Terrorism, Crime & Security Act 2001
  - Part 11 creates obligations for data retention on "communication service providers"
- Lots of E-Commerce stuff
  - Sale of Goods
  - Distance Selling Regulations
  - Contract Law
  - Unfair Terms
  - Unsolicited Faxes
  - etc etc etc
- Cybercrime Convention, 2001

13th February 2002 Security : UK Legislation

✶ 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 (eg 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

once ratified may require a Computer Misuse Act v2.0

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
- Understanding the basics of what the law means does not require you to study to become a lawyer!

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)