Economics, Law & Ethics

Computer Science Tripos Part 1B

UK Law and the Internet

Michaelmas 2020

Richard Clayton

These lecture notes were specially prepared for the Cambridge University Computer Science "Economics, Law & Ethics" course, Michaelmas Term 2020.

richard.clayton@cl.cam.ac.uk

Outline

- IANAL! And this is UK law
- Computer Evidence
- General Data Protection Regulation (from Spring 2018)
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Investigatory Powers Act 2016
- Regulation of Investigatory Powers Act 2000
- E-Commerce Regulations
- Privacy & Electronic Communications Regulations

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

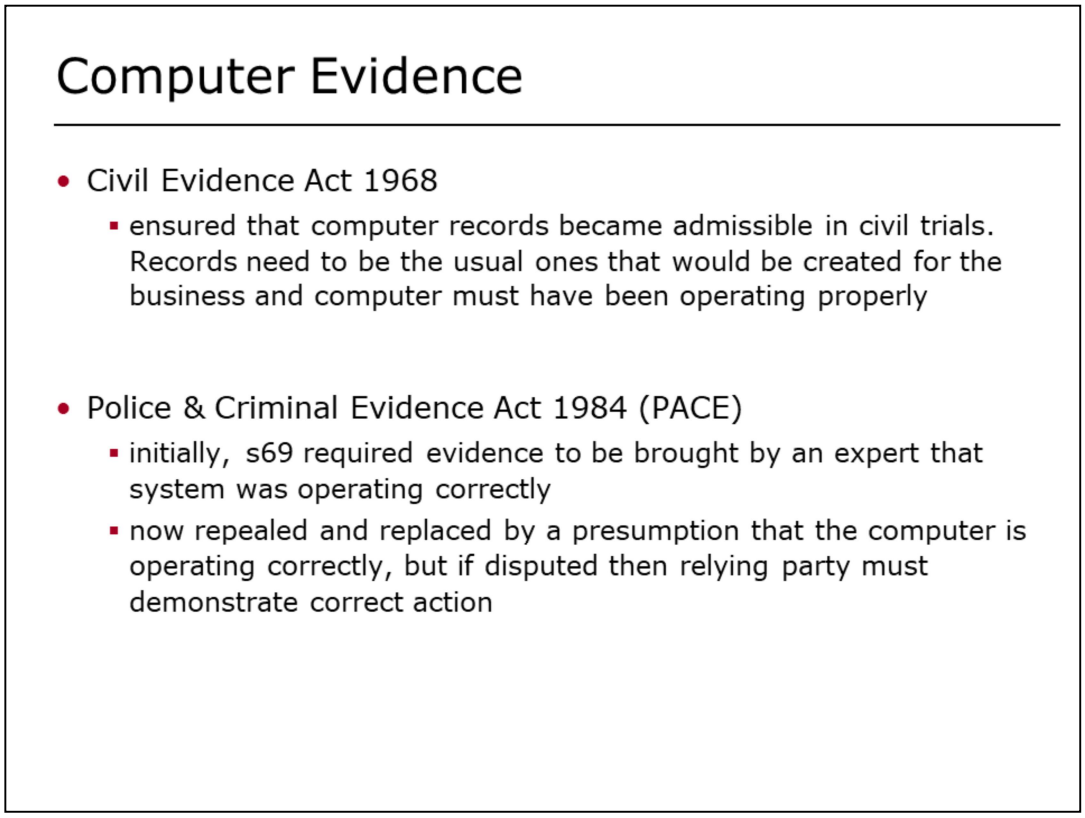
- Most of the relevant statutes available online
  - many court judgments now also appearing online
  - reading acts of parliament is relatively straightforward
  - judgments (case law) varies in clarity!
  - however, law is somewhat flexible in practice, and careful textual analysis may disappoint –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

The text of all relevant UK statutes are published at:

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

On the website you will find most statutes – starting with five that predate Magna Carta – with complete coverage from 1988 onwards. Consolidated versions of statutes (albeit with some complex exceptions and limited application of the most recent changes) are also available, along with an indication as to which sections are currently in force.

The site also holds the text of statutory instruments, with partial coverage from 1948 and a complete set from 1987.

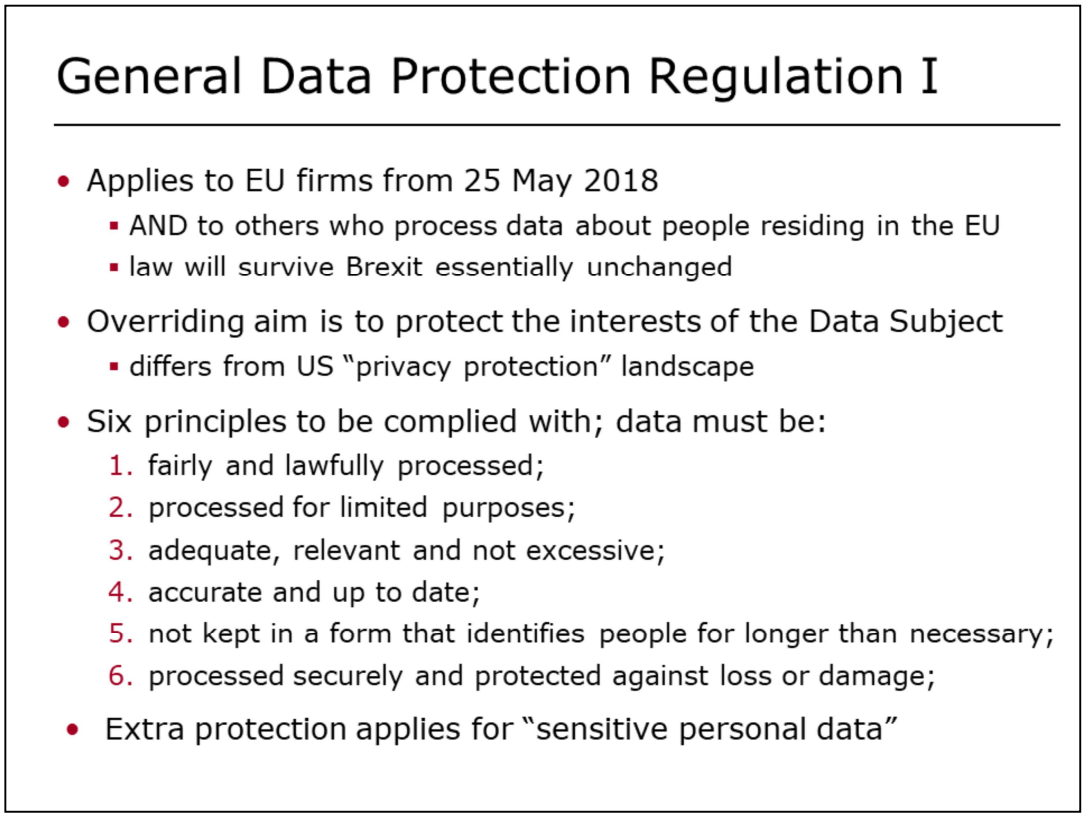


✶ The 1968 Civil Evidence Act removed any possibility of computer evidence being labelled as "hearsay". It has since been amended by the Civil Evidence Act 1995, which clarified what a document was – to cover maps, plans, films and even computer databases. In general, authenticity is not an issue in 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://www.five-ten-sg.com/risks/risks-18.25.txt)



✶ GDPR is a "Regulation" so it immediately applied across the whole of the European Union on 2018-05-25

✶ English text of GDPR

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT

✶ Lots of fine advice on the Information Commissioner's page

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

✶ The GDPR applies to 'controllers' **and** 'processors'. The controller says how and why personal data is processed and the processor acts on the controller's behalf. A processor has specific legal obligations (eg maintaining records of the processing). A controller is obliged to ensure that contracts with processors conform to GDPR.

✶ See Article 5 for the full text of the six principles and note that 5(2) says: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

✶ A risk-based approach is required in determining what measures are appropriate for principle 6:

Management and organisational measures are as important as technical ones

Pay attention to data over its entire lifetime

General Data Protection Regulation II

- Requirement to keep internal records of your databases
  - who you are, the type of data and who provided it
  - retention schedules
  - security arrangements (technical & organisational)
  - details of transfers (especially when involves third countries)
- Essential to identify why processing is allowed
  - consent: for each purpose must be freely given, specific, informed & unambiguous; can no longer use pre-ticked boxes or infer it
  - contract
  - legal compliance
  - then there's "vital interest of a human (life or death)", "public interest", "legitimate interest (complex!)", "member state specific reasons", "crime & justice", and "new purposes".
- Must get permission from parents if a child under 16 (UK: 13)

✶ You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply with GDPR. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - Data minimisation;
  - Pseudonymisation;
  - Transparency;
  - Allowing individuals to monitor processing; and
  - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

✶ Age limit for "children" differs across member states:

https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/children

General Data Protection Regulation III

- GDPR provides the following rights for individuals:
  - The right to be informed
    - need to have a privacy notice that explains your processing
  - The right of access
    - systems need to be designed for this right to be exercisable
  - The right to rectification
    - errors need to be corrected (and passed on if data was passed on)
  - The right to erasure
    - "right to be forgotten": when no compelling reason to keep the data
  - The right to restrict processing
    - you can keep data, but not otherwise process it (unless you have to)
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling

The privacy notice will need to specify:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer
- Purpose of the processing and the lawful basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

General Data Protection Regulation IV

- New systems must have data protection designed in
  - AND you may have to do an impact assessment
- Data breaches must be reported to regulator within 72 hours
  - PLUS a requirement to notify data subjects (if data is high risk)
- Fines can now be much bigger
- Firms processing data at scale (& public authorities) **must** appoint a Data Protection Officer
  - can be a contractor
  - must be capable of advising on GDPR obligations
  - must monitor compliance with GDPR
  - must report to the board and not be fired for doing their job!
- DPO optional for other firms, but they must have sufficient staff & skills to discharge their duties under the GDPR

✶ Fines can be up to 20m Euro or 4% of global turnover (whichever is greater)

✶ British Airways were fined £183 million (1.5% of turnover) in 2019 for failing to keep their website secure and Marriott were fined (one day later) £99 million (3%.) for a breach of customer data security. Both companies continue to pursue appeals and (after 15 months) nothing has yet been paid

Computer Misuse Act 1990 I

- 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 (especially Chapter 2 of) "Approaching Zero":

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

Computer Misuse Act 1990 II

- 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 s1, but done with intent to commit another serious offence
  - Raises the stakes from 2 years to 5 years
    - s1 was a mere 6 months, but amended in 2008
- Section 3
  - Unauthorised modification – tariff is up to 10 years
  - Intended to make virus writing illegal
  - Amended 2008 to cover denial of service as well
  - Making/distributing hacking tools is (since 2008) illegal

✶ The Act can be found online at:
http://www.legislation.gov.uk/ukpga/1990/18/contents

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

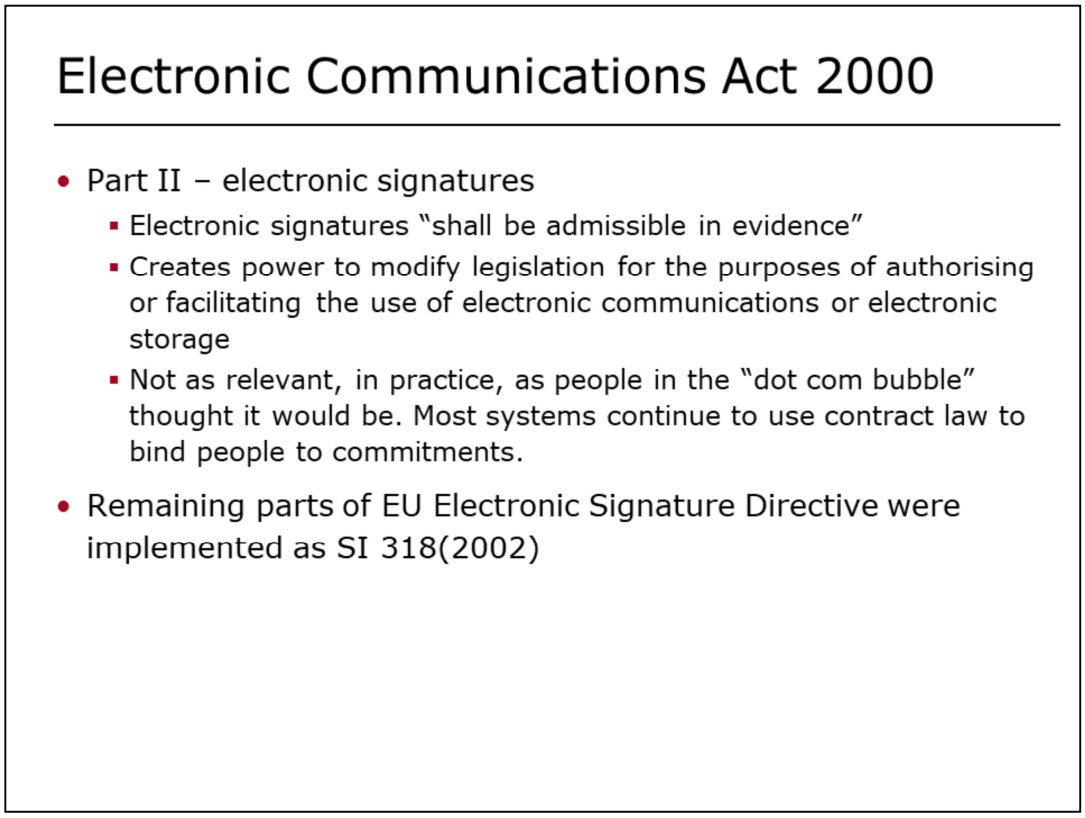
✶ There have been convictions for "denial of service" – the person who attacked the University of Cambridge (plus Oxford & perhaps more significantly Kent Police) got a two year sentence (albeit for other wickedness as well).
http://www.tcs.cam.ac.uk/news/0028180-cambridge-university-website-hacker-pleads-guilty-to-nine-charges.html

✶ The Council of Europe Convention on Cybercrime (aka the Budapest Convention) has been signed and ratified by the UK:
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". Since these 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

Computer Misuse Act 1990 III

- Important to clearly indicate when access is not authorised
- Case law is chequered
  - Fines have often been small compared with damage caused
  - Only around 20 cases a year (but many charges under Fraud Act)
  - 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 and received custodial sentence for writing viruses
  - "AMEX" case shows multi-level access can matter
  - Wimbledon case (Lennon): after an appeal it was found that "mail bombing" is a s3 offence – test of unauthorised becomes "if I were to ask, would they say 'yes'"
  - Cuthbert ("tsunami hacker") convicted of s1 offence for trying out `../../../` URLs

- 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.`
- Hutchings maintains a list of recent ecrime cases in the Cambridge Computer Crime database:
  `https://www.cl.cam.ac.uk/~ah793/cccd.html`
- *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 ~5 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 2 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.legislation.gov.uk/ukpga/2000/7/contents

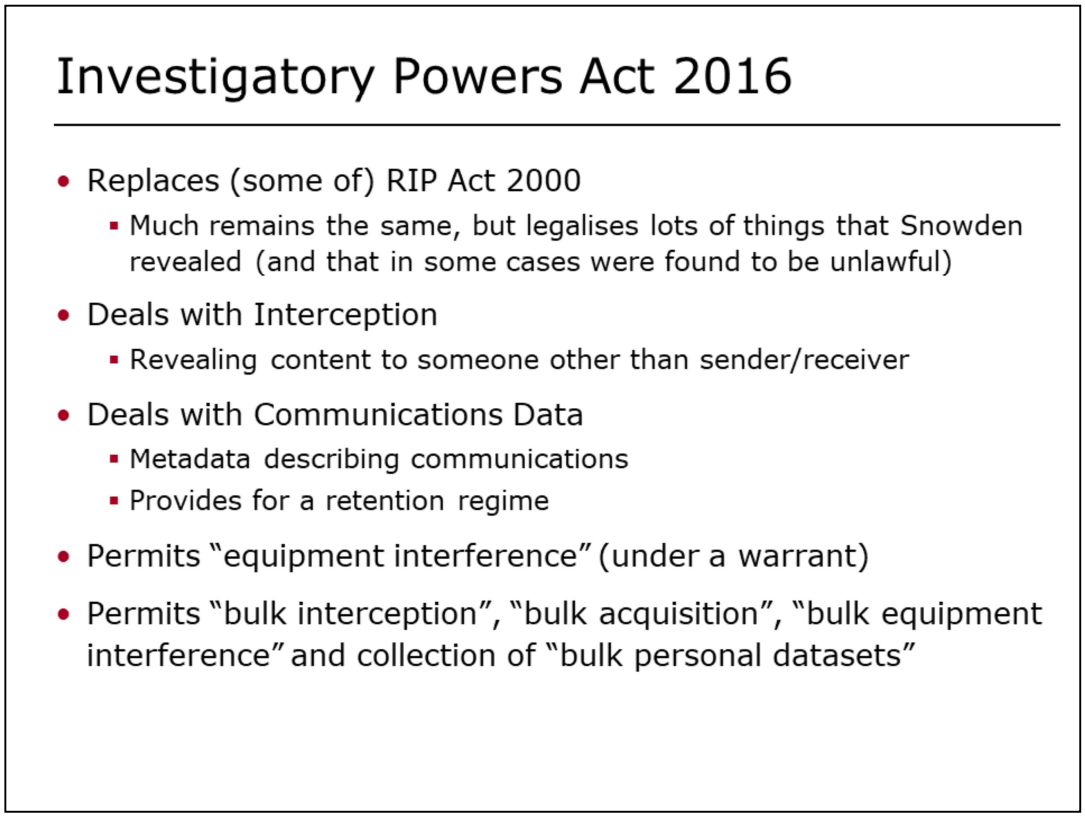
✶ The voluntary licensing scheme in Part I was the last vestige of the "key escrow" proposals of the mid 1990s when the NSA (and others) tried to grab the world's keys to mitigate the effects of the use of encryption upon their snooping activities. This part of the Act fell under a "sunset clause" on 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. A project by HM Land Registry for electronic conveyancing of land was abandoned in 2011 – since users were unconvinced it could be made secure.

✶ Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures: **http://eu-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.legislation.gov.uk/uksi/2002/318/contents/made



✶ The Investigatory Powers Act 2016 can be found online at;
http://www.legislation.gov.uk/ukpga/2016/25/contents

✶ 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.

✶ The Regulation of Investigatory Powers Act 2000 was that revision. It also formalised access to communications data which previously done using the exemptions provided by s28 of DPA 1984 (s29 in DPA 1998). Furthermore, 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").

✶ Communications data (which RIPA provided mechanisms to access) were required to be retained under an EU Directive (implemented as a statutory instrument in the UK). However, the CJEU struck down this Directive so the UK rapidly passed the Data Retention and Investigatory Powers Act 2014. However, this was found unlawful by the High Court and in December 2016 the CJEU agreed. However, the IPA 2016 replaces DRIPA and the High Court ruled on that in April 2018. The Government has now amended the retention regime to remove some reasons for access to data, restricting it to "serious" crime and introducing an independent element to authorisations for access.

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 (currently) admissible in court
  - GCHQ can scan international communications for "factors"
- Some sensible exceptions exist
  - Delivered data
  - Permission from BOTH sender and receiver
  - Stored data that can be accessed by production order
  - Techies running a network
  - "Lawful business practice"

✶ `s4(1) ... a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if— (a) the person does a relevant act in relation to the system, and (b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication. (2) ... "relevant act", in relation to a telecommunication system, means- (a) modifying, or interfering with, the system or its operation; (b) monitoring transmissions made by means of the system; (c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.`

✶ NB 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 (or as journalists discovered, voice mails).

✶ Interception is lawful if both the sender and recipient have given permission s44(1); or, s44(2), if the recipient has and the police have a RIPA Part II warrant (this is the "tap the kidnapper's call" scenario).

✶ Techies working for the communications service provider can lawfully intercept [s45] if what they're doing is required for the provision or operation of the service. Filtering for viruses is explicitly lawful, as is sniffing 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 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/IPA Acts. They **do not** specify how to avoid problems with data protection legislation or other relevant laws
  - 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

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

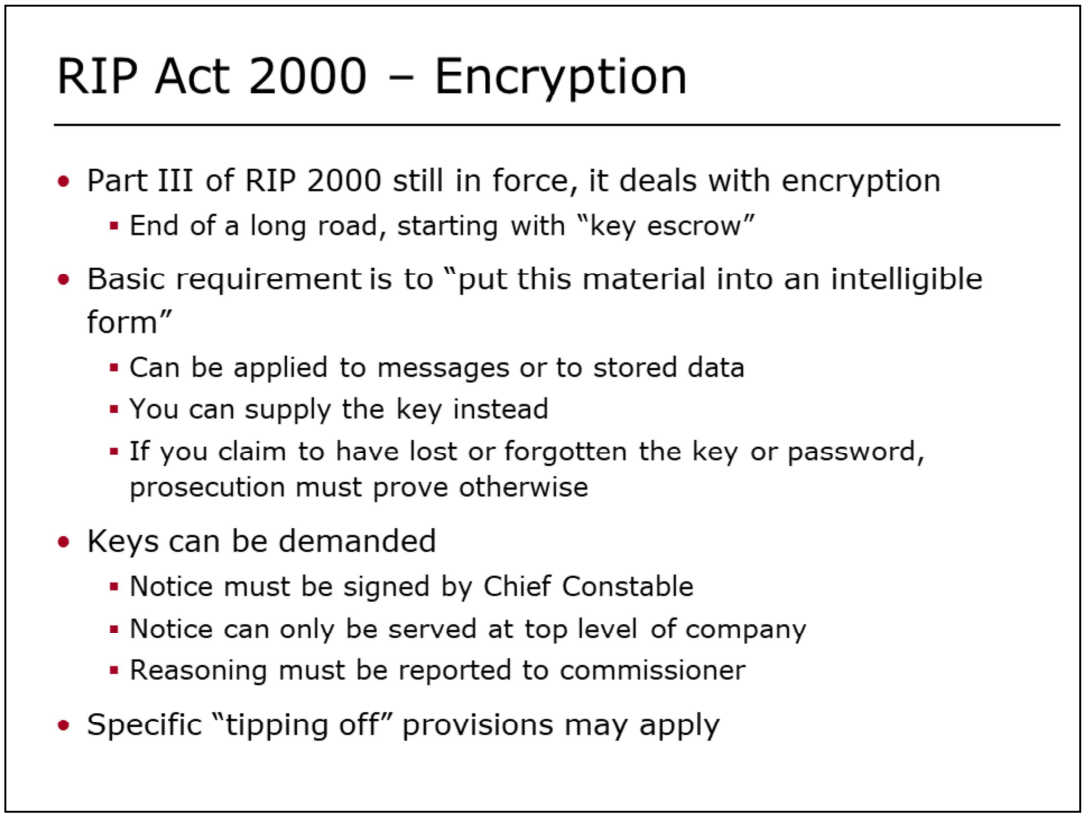
http://www.legislation.gov.uk/uksi/2000/2699/contents/made

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

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

and there are links to other employer-relevant documents at:

https://ico.org.uk/for-organisations/guide-to-data- protection/employment/



✶ The Regulation of Investigatory Powers Act 2000 can be found online at; **http://www.legislation.gov.uk/ukpga/2000/23/contents**

Note Part I and much of Part IV is repealed by the IPA 2016

✶ Part III deals with encryption and 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 and industry might move systems abroad to meet a perceived Government Access to Keys (GAK) threat.

- The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations SI 2013 No 3134:
  http://www.legislation.gov.uk/uksi/2013/3134/contents/made
  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. There is a useful set of bullet points at:
  https://www.gov.uk/online-and-distance-selling-for-businesses
  consumer viewpoint:
  https://which.co.uk/consumer-rights/regulation/consumer-contracts-regulations
- The Electronic Commerce (EC Directive) Regulations SI 2002 No 2013
  http://www.legislation.hmso.gov.uk/si/si2002/20022013.htm
- The Rome Convention (1980) – revised as Rome II from 2007 – addresses which country's law applies. B2B contract will say, otherwise it will be the law where the damage occurs. However, for product liability, if the product is not marketed into a particular country (eg: website in local language, pricing in appropriate currency) then country of purchase is relevant.
  http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/l16027_en.htm
- The Brussels Regulation (and Brussels Convention and Lugano Convention !) address which court it will be heard in. Similar rules as above:
  http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/l33054_en.htm

Privacy & Electronic Communications

- Implementing EU Directive 2002/58/EC
- Replaces previous Directive (& corresponding UK Regulations)
- Rules on phone directories, location info etc
- Bans unsolicited marketing email ("spam") to natural persons; but not to legal persons)
  - BUT see your ISP's "acceptable use policy"
- Controls on the use of "cookies" now superseded by 2010 legislation (ICO has issued detailed guidance):
  - Must give "clear and comprehensive" information
  - AND must have consent (devil in the details here) …
  - …. unless cookies are "strictly necessary" (read as "essential") for provision of an information society service that has been requested
- Was intended to be replaced by time GDPR is in force!

✶ 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.legislation.gov.uk/uksi/2003/2426/contents/made

✶ 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. Note that most ISP contracts will apply a more rigorous interpretation of what is acceptable behaviour:
https://www.linx.net/good/bcpindex.html

✶ The ICO is taking the view that cookies may be used without permission:
- to make shopping carts work;
- for security purposes eg on banking websites;
- to assist in load balancing systems.

But that you need permission
- for first and third party advertising cookies;
- for analytics;
- for personalisation.

https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

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
- Processing personal data must be planned for & documented
- Hacking is illegal!
- Interception is illegal
  - though there are sensible exceptions, provided you jump through the appropriate hoops
- Serving cookies inappropriately can get you into trouble
- 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!

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)