ECommerce

Computer Science Tripos Part II

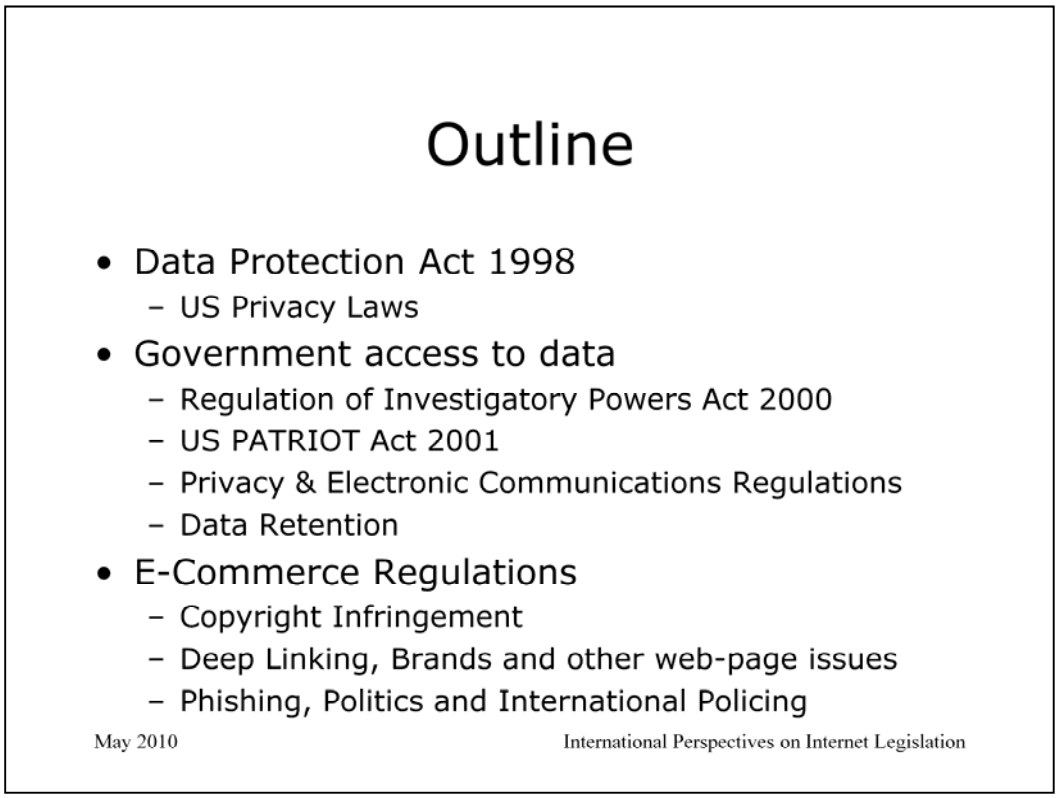
International Perspectives on Internet Legislation

Easter Term 2010

Richard Clayton

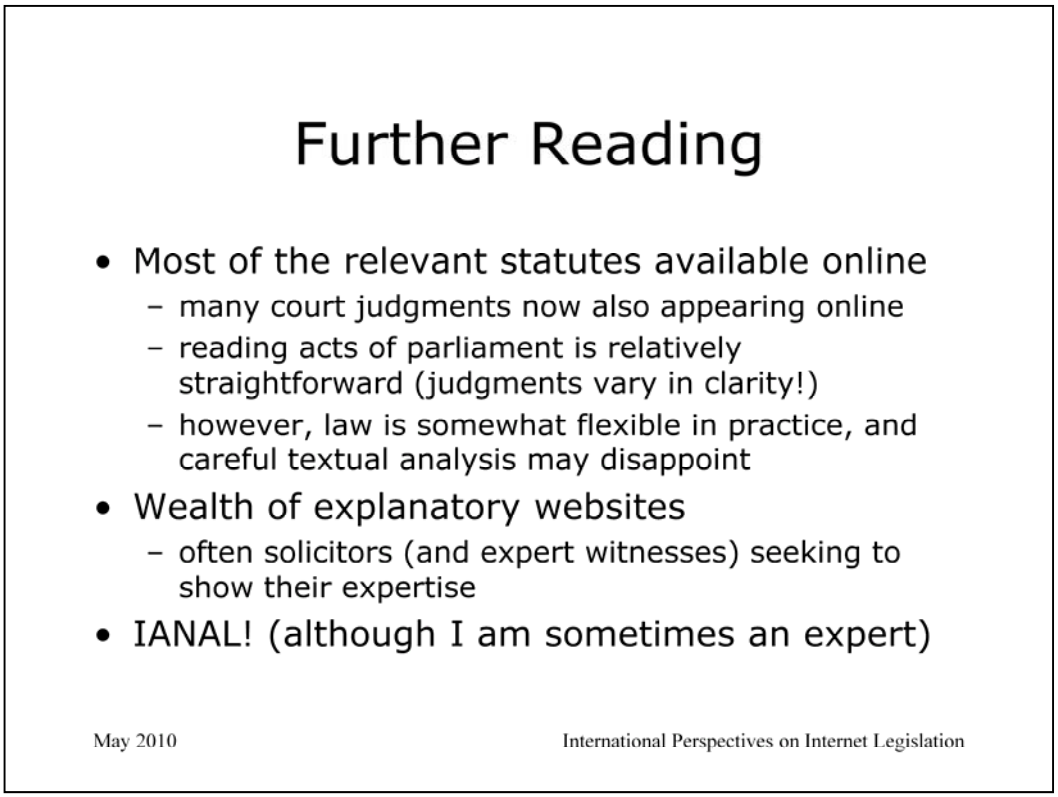
These lecture notes were specially prepared for the Cambridge University Computer Science "ECommerce" course, Easter Term 2010.

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!

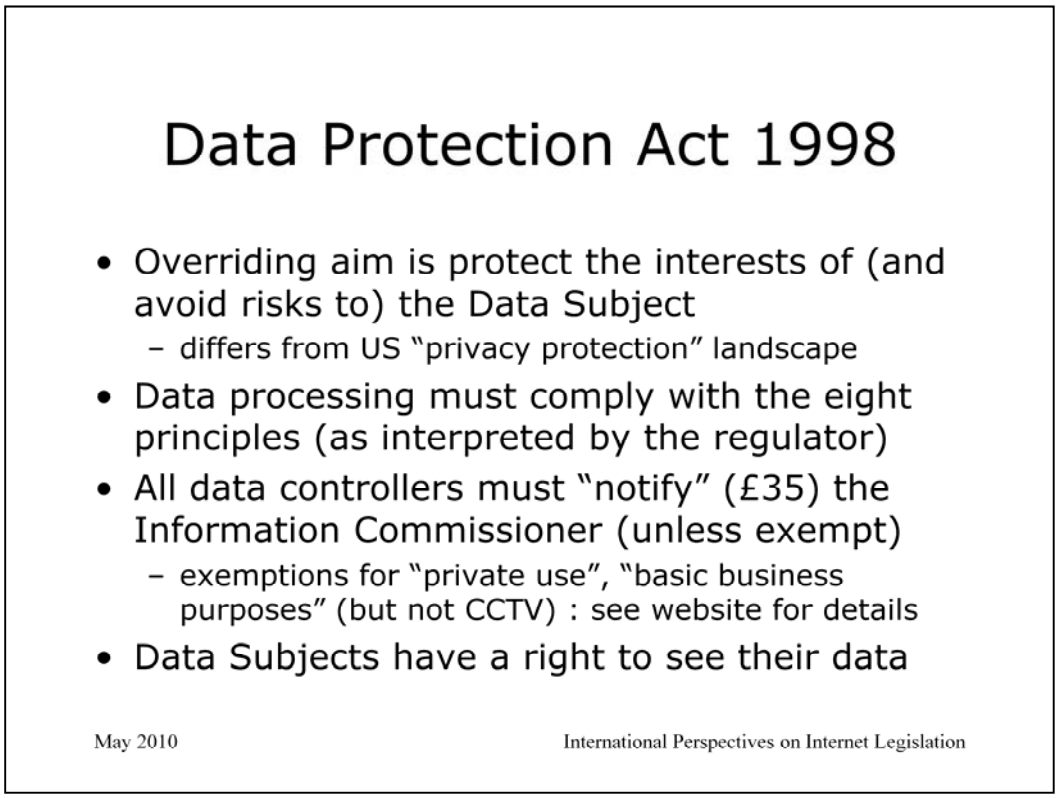


Raw statutes, from 1988 onwards (and statutory instruments from 1987) are published at:

`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/`



✶ 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/`

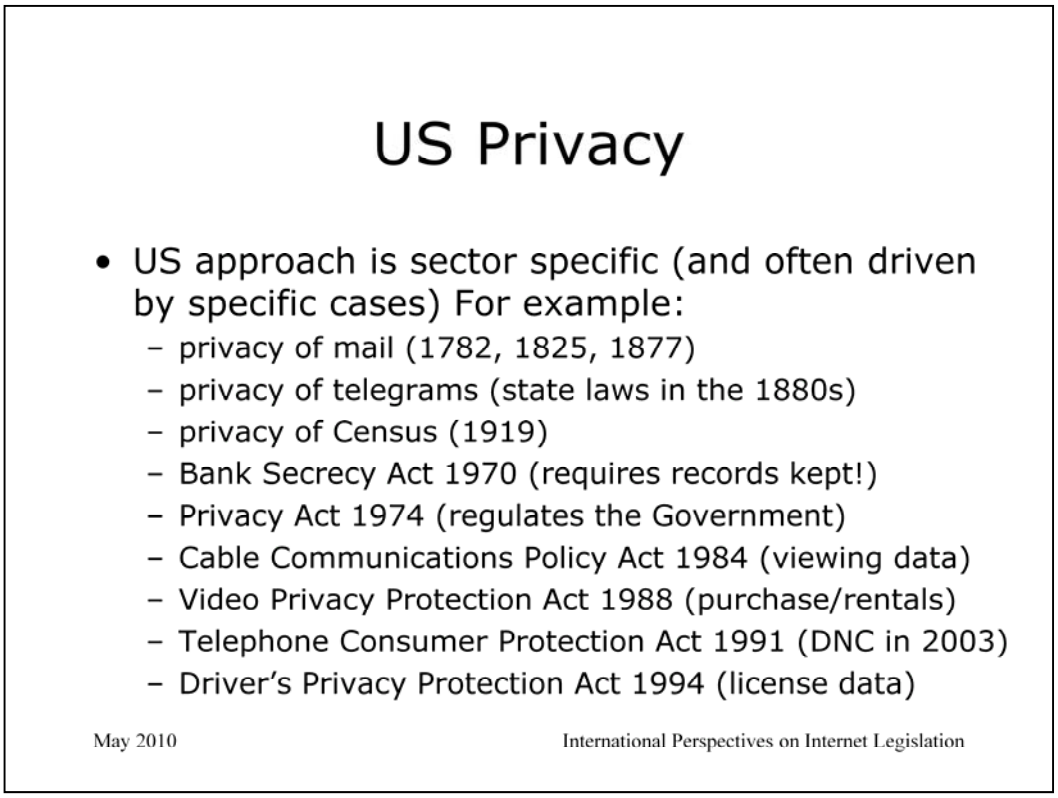
✶ Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- 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.



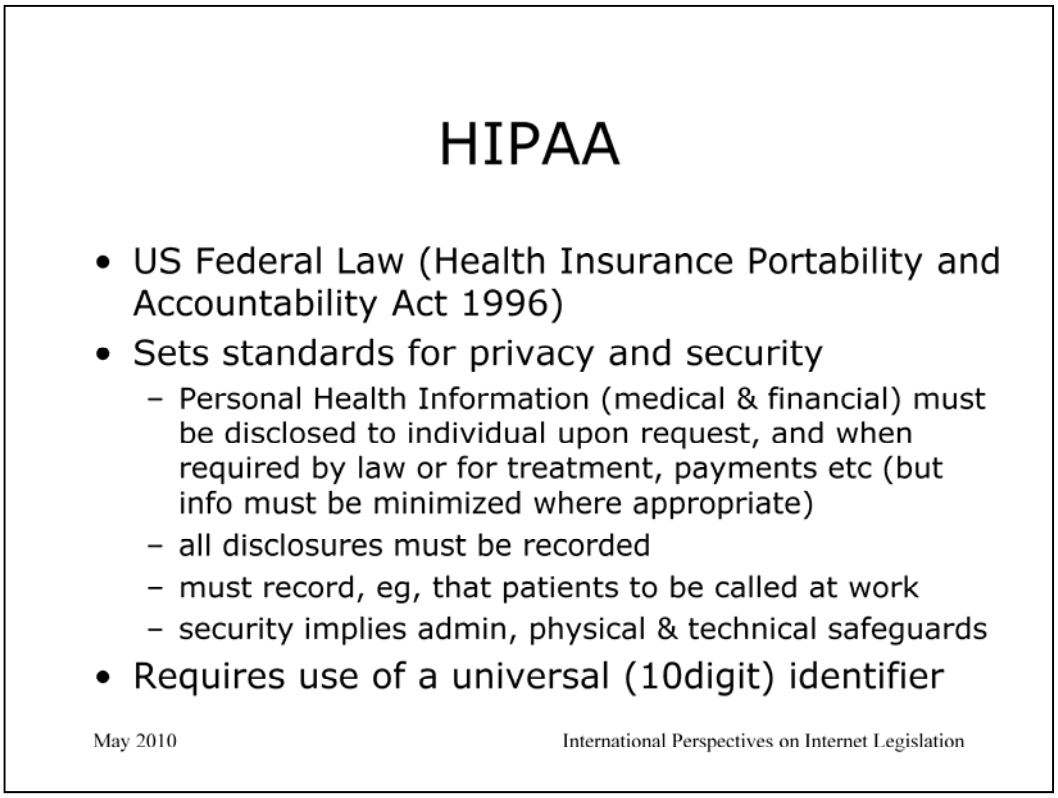
✶ The US does not have the same idea of Data Protection as does Europe, but it does have a formal notion of privacy, and a patchwork of Acts addressing disclosure of personal information in specific sectors.

✶ The Privacy Act applies many of the Data Protection principles to the Federal Government (but not to private industry, and there are significant exceptions).

✶ The Video Privacy Protection Act was passed following Judge Robert Bork's video rental records being released when he was being considered for appointment to the Supreme Court.

✶ There is an overview of all the various statutes at:

`http://www.cdt.org/privacy/guide/protect/laws.php`

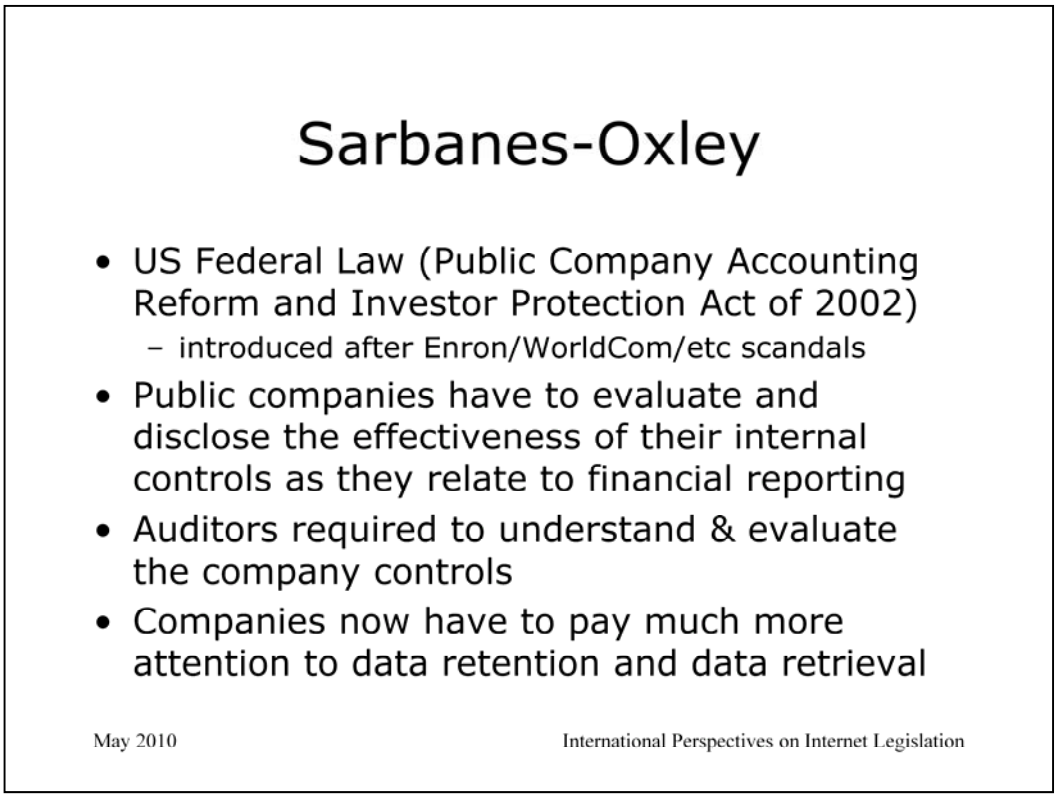


✶ At the heart of HIPAA is a "Privacy Rule" that it takes a 25 page PDF to summarise!

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

✶ The official site explaining HIPAA is at:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html



✶ Sarbanes Oxley (SOX) is a complex collection of provisions, that are intended to restore confidence in corporate America following some very high profile scandals that cost investors billions.

✶ Drawing on analysis on why those scandals occurred, there are now specific rules about conflict of interest for auditors and security analysts.

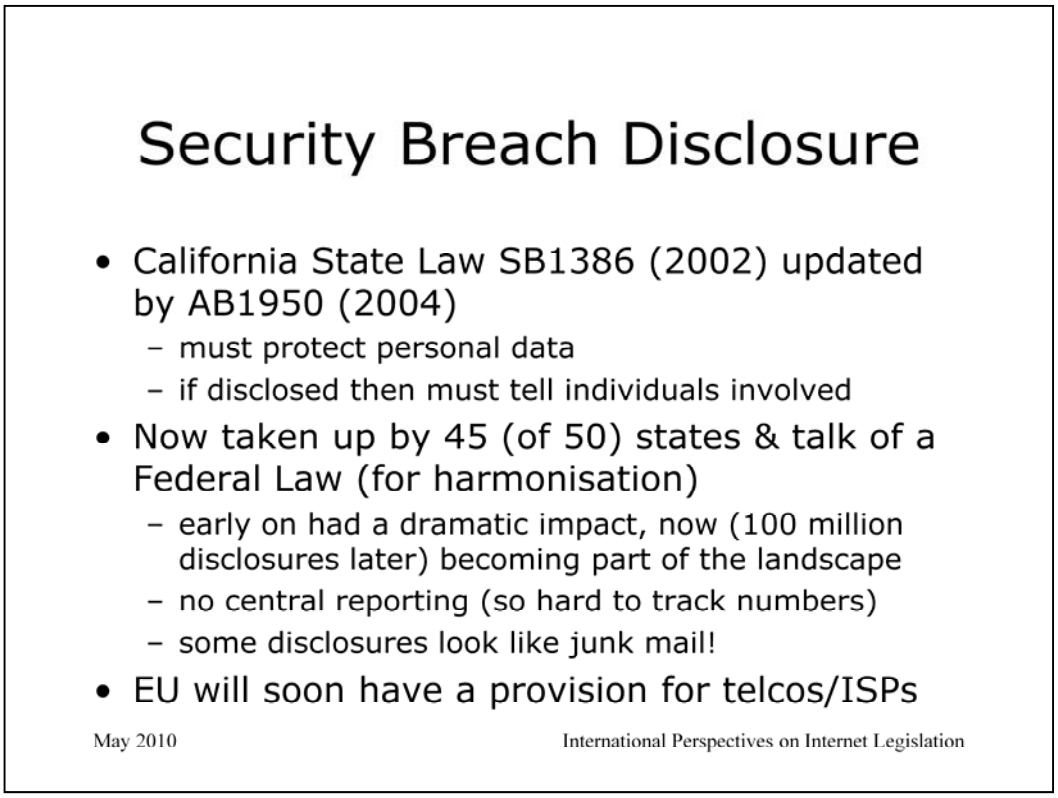
✶ Senior executives in public corporations must take individual responsibility for the accuracy and completeness of financial reports and they have new requirements to report personal stock transactions.

✶ The requirements on effective internal controls have been implemented through the Public Company Accounting Oversight Board (PCAOB), and in essence through the major accounting firms. Where existing accounting systems were chaotic, manual or decentralised, costs have been high, which has led to considerable criticism.

✶ There is some evidence of smaller firms avoiding stock market listings in New York to reduce their costs, and the SOX regime is regularly being tinkered with to try and avoid excess expense.

✶ For the text of the law see:

http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

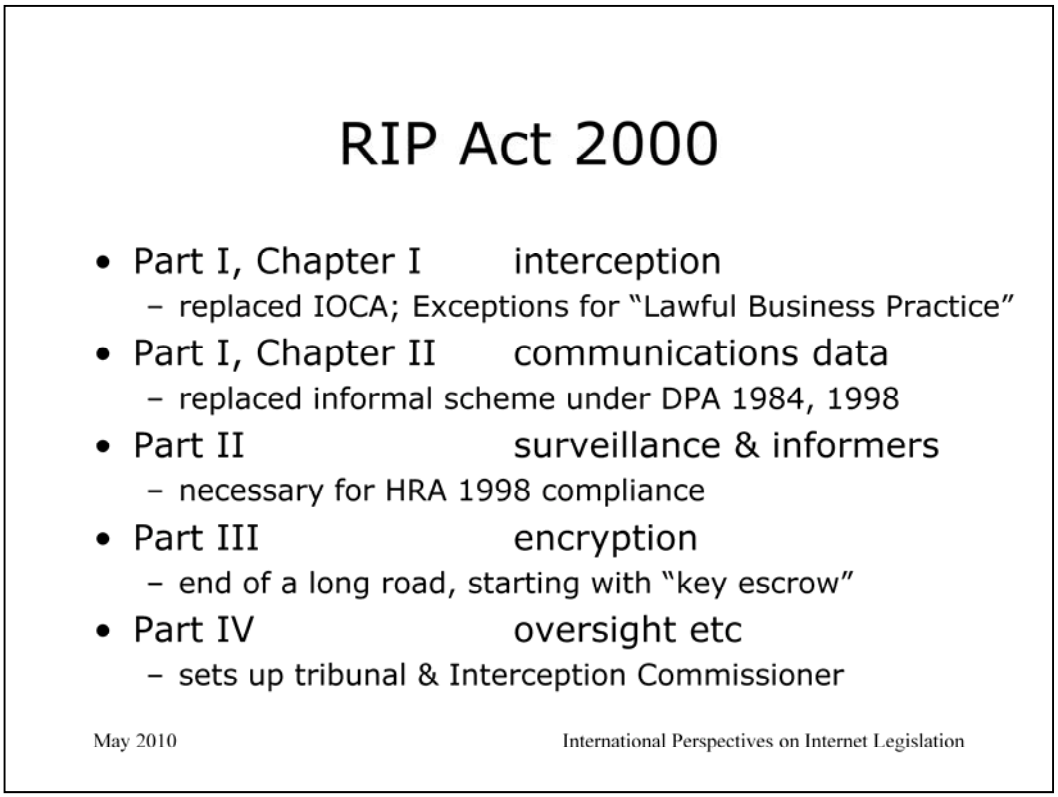


✶ For a list of all the various state laws (there is similar language in all of them, but all sorts of complex differences) see the NCSL website:

http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

✶ The EU included a security breach disclosure requirement in the reworking of the Telecoms Directives. The new scheme must be transposed into national law by May 2011. It will apply to telcos and ISPs (but NOT to "information service providers") where there is a security breach affecting information held for "the provision of electronic communication services".

Note that even if the data was encrypted you will have to tell your national authority!



✶ The Regulation of Investigatory Powers Act 2000 can be found online at;
http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm

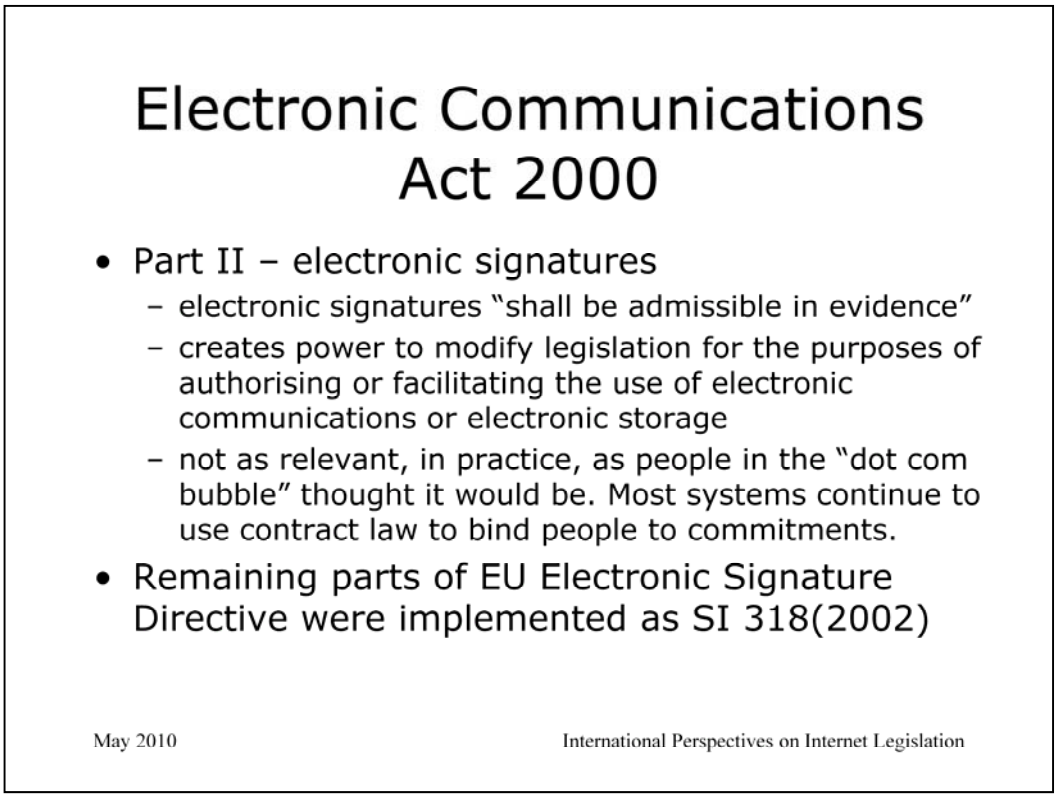
✶ A history of interception in the UK (from 1663 onwards) can be found at:
http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/oicd/intera.htm

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 at that time 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).



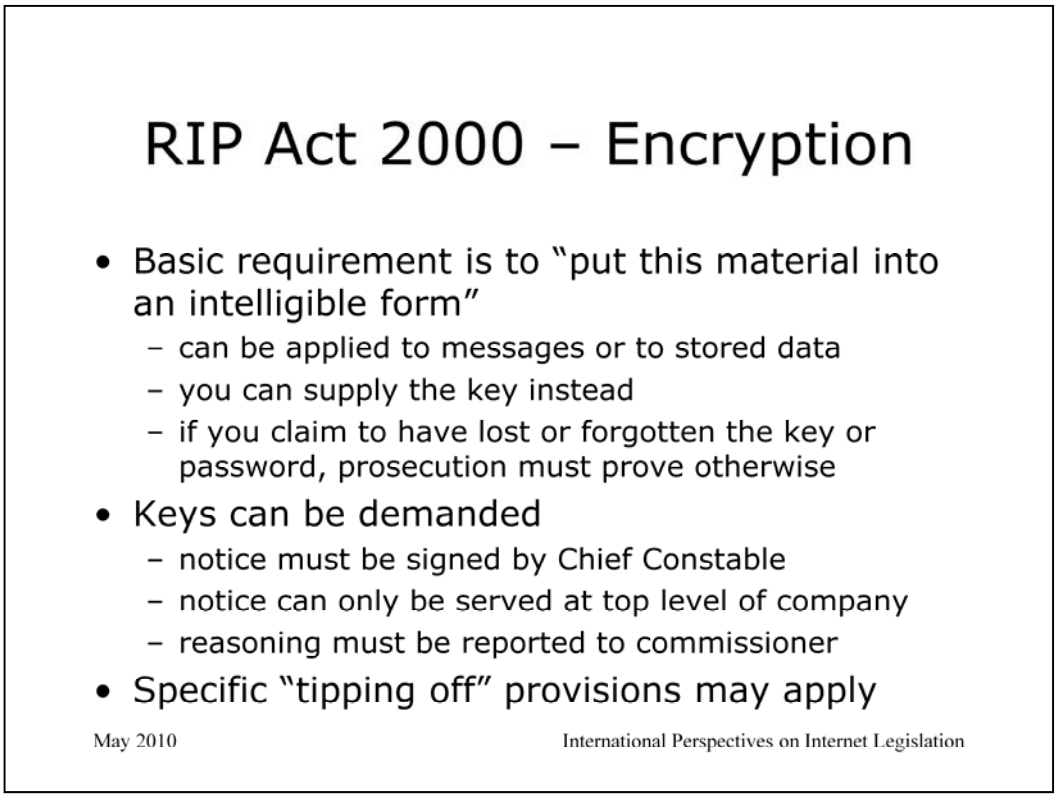
✶ The Electronic Communications Act 2000 is online at:
http://www.hmso.gov.uk/acts/acts2000/20000007.htm

✶ 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 on the horizon (perhaps with a pilot in October 2007).

✶ 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

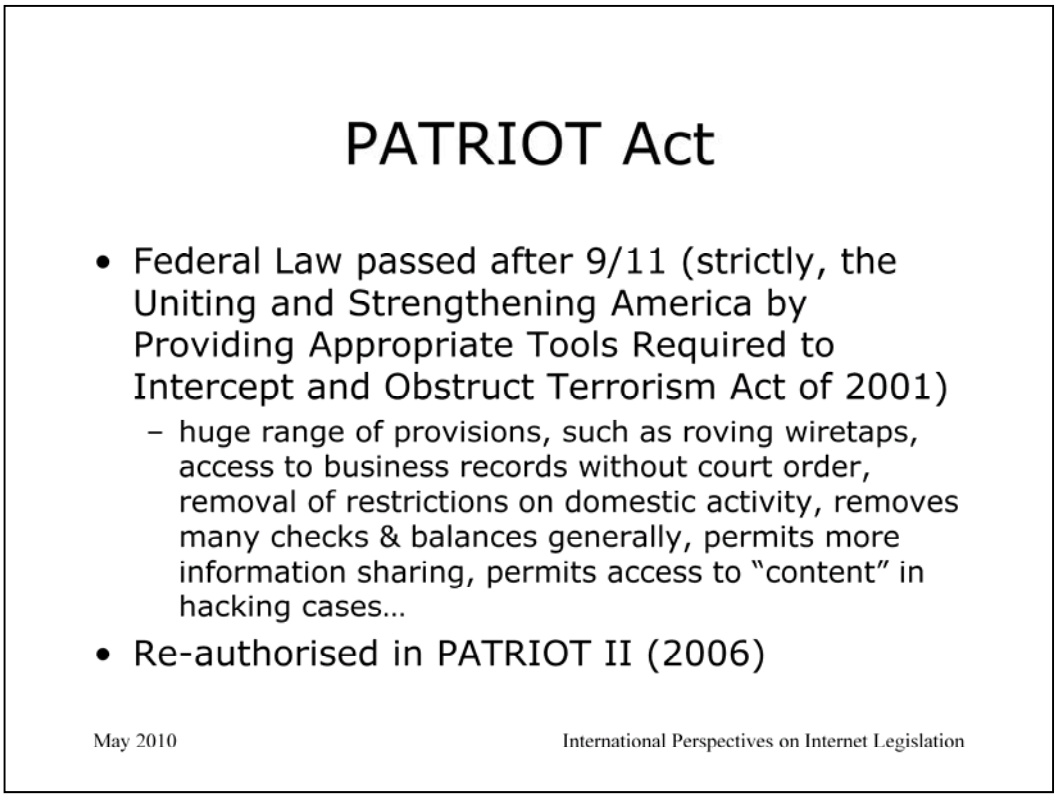


✶ Part III was eventually brought into force in October 2007.

✶ 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.



✶ For details of the PATRIOT Act, and the problems with it from a civil rights viewpoint see:

http://w2.eff.org/patriot/

✶ 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"

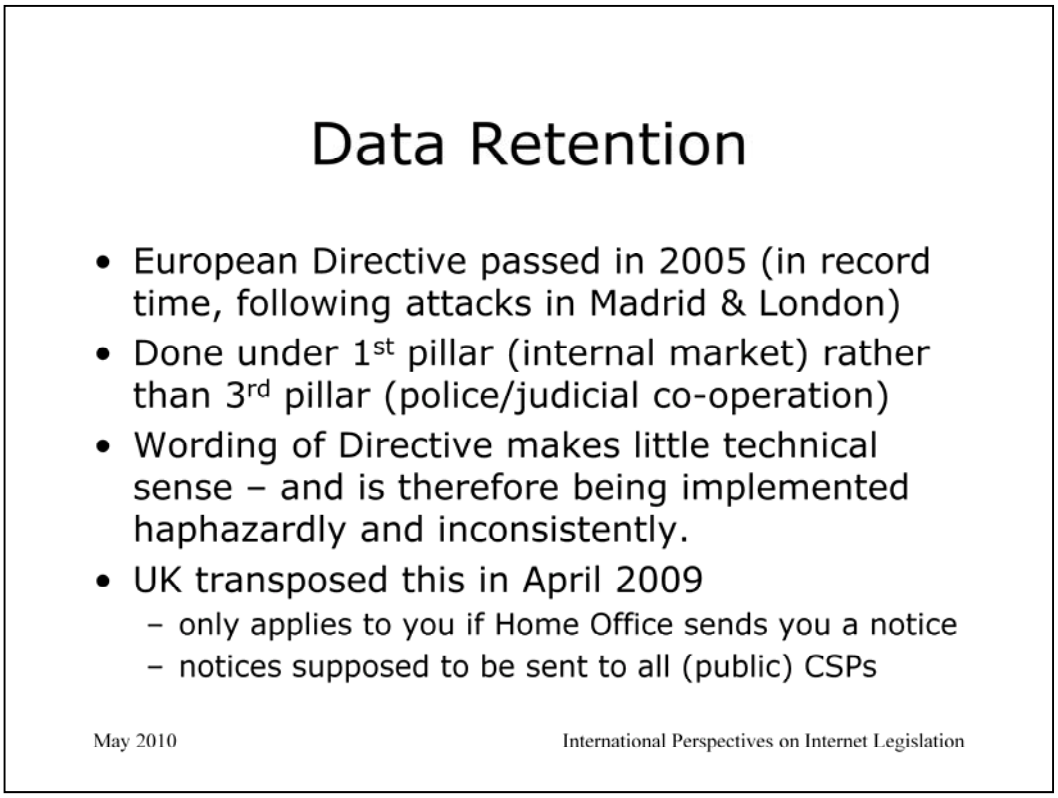
`http://www.hmso.gov.uk/si/si2003/20032426.htm`

✶ 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/www_public/community_involvement/bcp/ubebcp_v2`
`/bcp/bcp_operating_mailing_lists`

✶ 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`

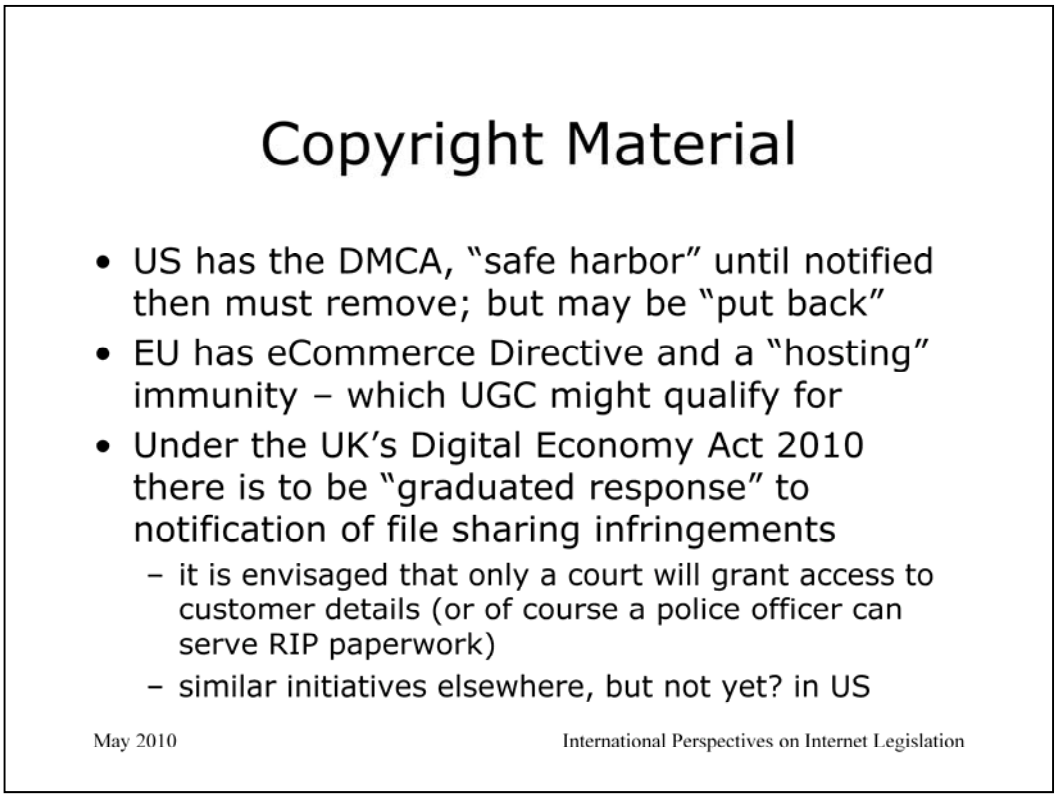


✶ Full title is: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

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

✶ As time goes on, more and more problems are being unearthed:

http://www.lightbluetouchpaper.org/2010/01/14/mobile-internet-access-data-retention-not/



✶ The Digital Millennium Copyright Act (1998) criminalises production or shipping of digital rights management (DRM) circumvention devices. It also sets up a scheme for dealing with copyright infringement on the Internet. ISPs are immune until notified, via a specific address that they must publish, and then they must remove infringing material. When there is a dispute the poster can have the material replaced, but must submit to the jurisdiction of a court who will decide the case. Note that infringement notices must meet specific requirements and be made "under penalty of perjury".

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf

✶ In the UK, Parliament has recently passed the Digital Economy Act. Where there is infringement via file sharing the rights owners will be able to require ISPs to communicate with their customers to tell them of their wrongdoing. The ISP must reveal the existence of persistent offenders, and the rights holders can then apply to the court for an order to have their names and addresses revealed. This is sometimes called "graduated response" or "three strikes". Much of the detail will be set out in secondary legislation that will be appearing over the next year or so.

✶ 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 DTI website:

`http://www.dti.gov.uk/sectors/ictpolicy/ecommsdirective/ecommsdirectiveguidance/page10142.html`

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

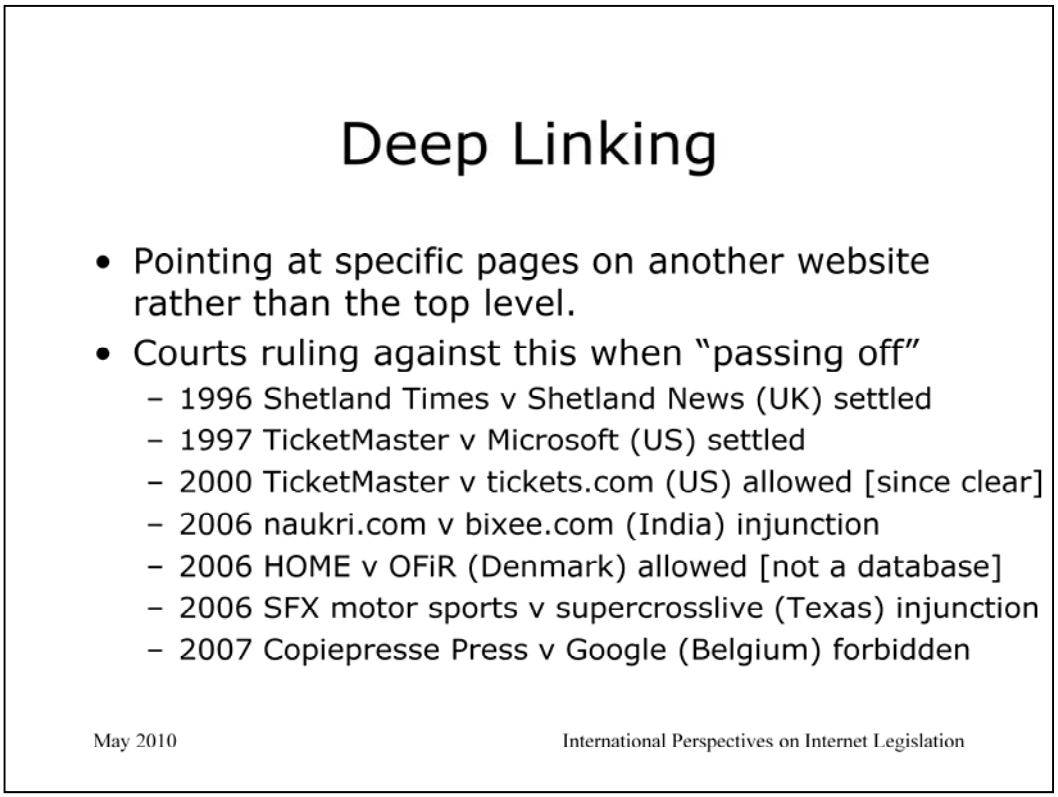
✶ The Rome Convention (1980) addresses which country's law applies. B2B contract will say, consumer's law will apply unless your website addresses a particular country (eg: multiple languages, prices in Euro etc).

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

✶ For information about fund-raising for UK political parties see:
http://www.electoralcommission.org.uk/party-finance



✶ Shetland News had headlines that pointed to stories within Shetland Times site. There was an interim injunction forbidding this (because the headlines were copied verbatim), but it settled before trial with the News agreeing to cease their previous practice.

`http://www.netlitigation.com/netlitigation/cases/shetland.htm`

✶ Microsoft's "Sidewalk" site linked direct to events on Ticketmaster's site. They settled out of court and the deep links were removed.

`http://www2.selu.edu/Academics/FacultyExcellence/Pattie/DeepLinking/cases.html`

✶ Tickets.com were linking into TicketMaster when they didn't handle an event, and the judge said it wasn't a copyright breach because there was no copying.

`http://www.politechbot.com/docs/ticketmaster-tickets-2000-03-27.txt`

✶ The aggregator naukri was enjoined from linking deep into the naukri jobs site (they were essentially presenting classified of their own).

`http://dqindia.ciol.com/content/industrymarket/focus/2006/106032304.asp`

✶ Real estate site bolig.ofir.dk was linking into a database of houses for sale at Home. The court overturned a previous DK ruling saying that search engines by "ordinary practice" provided deep links into websites.

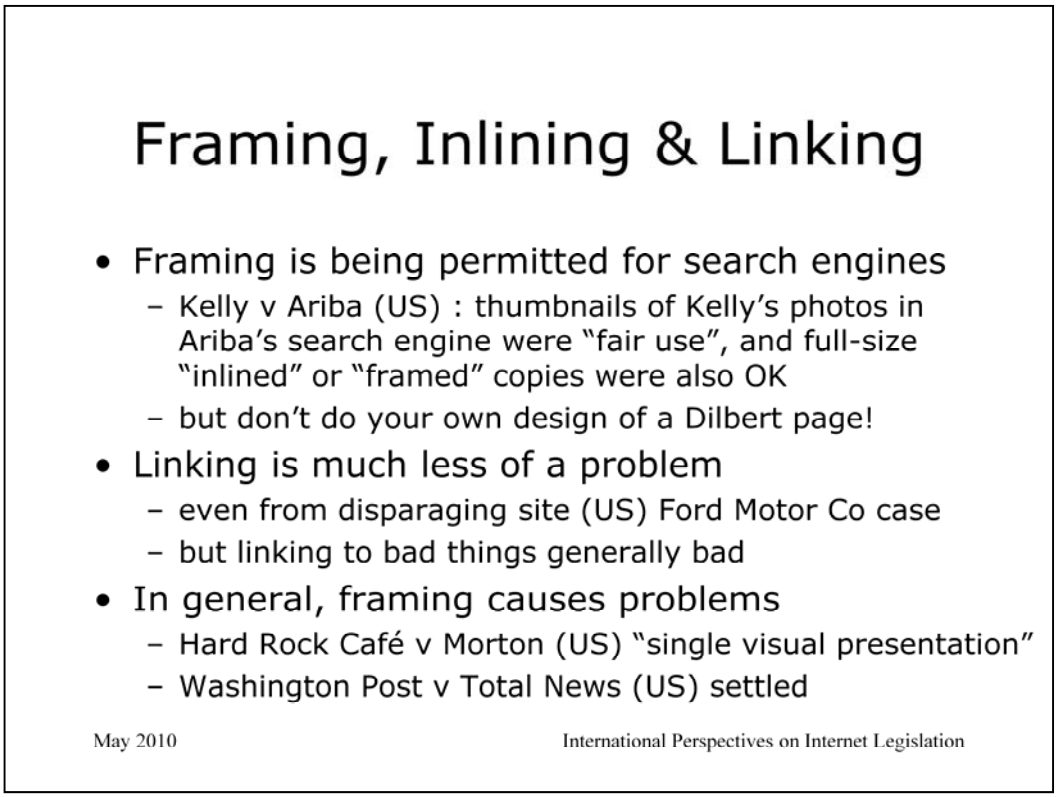
`http://www.edri.org/edrigram/number4.5/deeplinking`

✶ Supercrosslive linked to a live audio webcast at SFX. This was seen as copyright infringement. Worth noting that supercrosslive was a litigant in person.

`http://cyberlaw.stanford.edu/packet/200702/providing-unauthorized-link-live-audio-webcast-likely-constitutes-copy`

✶ The Belgian newspapers objected to Google News who provided headlines and small snippets of their stories.

`http://www.webpronews.com/topnews/2007/02/14/google-to-appeal-copiepresse-decision`



✶ Kelly was a photographer whose site was indexed by Ariba (an early image search engine). The court held that the thumbnails were allowed under US copyright law's "Fair Use" provisions. The appeal court initially held that when they framed images that were clicked on then this infringed, but revised their opinion and later said that was OK as well.

`http://www.eff.org/cases/kelly-v-arriba-soft`

✶ United Media get upset if you create your own page (with a better layout) and incorporate Dilbert strips within that.

`http://www.cs.rice.edu/~dwallach/dilbert/`

✶ Ford failed to get an injunction to prohibit a link from the disparaging website "fuckgeneralmotors.com"

`http://www.2600.com/news/122201-files/ford-dec.html`

✶ Morton sold his interest in the Hard Rock Café, except for the Hard Rock Casinos and Hotel. However, he also built a website that sold Hard Rock items, and that sold CDs via a framed copy of the Tunes website. The court held that since it looked like a Hard Rock Hotel site, and since selling CDs was a right Morton had sold, he was in breach of agreements.

`http://www.internetlibrary.com/cases/lib_case192.cfm`

✶ Total News linked to various news websites, presenting their content within a frame (full of their logo and their adverts). They settled out of court with the media companies – with Total News getting a license to link to the sites, but without a frame. Since settled, this doesn't settle anything!

`http://legal.web.aol.com/decisions/dlip/wash.html`

Brand Names

- Significant protection for brands in domain names
  - mikerowsoft.com settled, microsuck.com survived…
- Using other people's brand names in meta-tags doesn't usually survive legal challenge
- Many US rulings on "adwords" now occurring; if you just buy keyword then OK, but problems if use trademarks in ad copy, or on landing page
- Germany, UK, Austria following US line, France is not. ECJ have followed the US approach.

Phishing

- Sites clearly illegal (branded to look identical to real banks)
- Fraud Act 2006 ensures they can be illegal even if not yet operating
- Should you be concerned about what you are being asked to do, Fraud Act (& Serious Crime Bill) worth checking for a range of shiny new offences involving the creation of tools for fraud and offences of helping criminals…

International Policing

- Foreign police priorities differ (as do laws)
  - specialist advice is essential
- Police do not usually operate across borders
  - Interpol mainly a fax distribution centre
  - although we now have European Arrest Warrant
- Problem for searches of remote/cloud systems
  - once police become aware must use MLAT
  - MLAT allows the diplomats to consider the issues
  - but it often makes glaciers look quick
- Gambling, non-banks &c => no US holidays!

Review

- Important to understand difference between European Data Protection & US privacy
  - however, much common ground and ideas like security breach notification gaining traction
- Governments now grok computers and the Internet and are getting into data retention, traffic analysis &c in a major way
- Much still to be finally settled on the web
- Being a backroom boffin in serious crime is not as safe as it once was

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)