ECommerce
Computer Science Tripos Part II

International Perspectives on Internet Legislation

19th May 2009
Richard Clayton
Outline

• Data Protection Act 1998
  – US Privacy Laws

• Government access to data
  – US PATRIOT Act 2001
  – Privacy & Electronic Communications Regulations
  – Data Retention

• E-Commerce Regulations
  – Deep Linking and other web-page issues
  – Phishing, Gambling and International Policing
Further Reading

• Most of the relevant statutes available online
  – many court judgments now also appearing online
  – reading acts of parliament is relatively straightforward (judgments vary in clarity!)
  – however, law is somewhat flexible in practice, and careful textual analysis may disappoint

• Wealth of explanatory websites
  – often solicitors (and expert witnesses) seeking to show their expertise

• IANAL! (although I am sometimes an expert)
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 for “private use”, “basic business purposes” (but not CCTV) : see website for details
• Data Subjects have a right to see their data
US Privacy

- US approach is sector specific (and often driven by specific cases) For example:
  - privacy of mail (1782, 1825, 1877)
  - privacy of telegrams (state laws in the 1880s)
  - privacy of Census (1919)
  - Bank Secrecy Act 1970 (requires records kept!)
  - Privacy Act 1974 (regulates the Government)
  - Cable Communications Policy Act 1984 (viewing data)
  - Video Privacy Protection Act 1988 (purchase/rentals)
  - Driver’s Privacy Protection Act 1994 (license data)
HIPAA

- Sets standards for privacy and security
  - Personal Health Information (medical & financial) must be disclosed to individual upon request, and when required by law or for treatment, payments etc (but info must be minimized where appropriate)
  - all disclosures must be recorded
  - must record, eg, that patients to be called at work
  - security implies admin, physical & technical safeguards
- Requires use of a universal (10digit) identifier
Sarbanes-Oxley

  – introduced after Enron/WorldCom/etc scandals
• Public companies have to evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting
• Auditors required to understand & evaluate the company controls
• Companies now have to pay much more attention to data retention and data retrieval
Security Breach Disclosure

  – must protect personal data
  – if disclosed then must tell individuals involved

• Now taken up by over 30 states & talk of a Federal Law (for harmonisation)
  – early on had a dramatic impact, now (100 million disclosures later) becoming part of the landscape
  – no central reporting (so hard to track numbers)
  – some disclosures look like junk mail!

19th May 2009
International Perspectives on Internet Legislation
RIP Act 2000

- Part I, Chapter I interception
  - replaced IOCA; Exceptions for “Lawful Business Practice”
- 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

19th May 2009

International Perspectives on Internet Legislation
Electronic Communications
Act 2000

• 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
  – not as relevant, in practice, as people in the “dot com
    bubble” thought it would be. Most systems continue to
    use contract law to bind people to commitments.

• Remaining parts of EU Electronic Signature
  Directive were implemented as SI 318(2002)
RIP Act 2000 – 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
Patriot Act

- Federal Law passed after 9/11 (strictly, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)
  - huge range of provisions, such as roving wiretaps, access to business records without court order, removal of restrictions on domestic activity, removes many checks & balances generally, permits more information sharing, permits access to “content” in hacking cases...
- Re-authorised in PATRIOT II (2006)
Privacy & Electronic Communications

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

• European Directive passed in 2005 (in record time, following attacks in Madrid & London)
• Done under 1st pillar (internal market) rather than 3rd pillar (police/judicial co-operation)
• Wording of Directive makes little technical sense – and is therefore being implemented haphazardly and inconsistently.
• UK transposed this in April 2009
  – only applies to you if Home Office sends you a notice
  – notices supposed to be sent to all (public) CSPs
E-Commerce Law

• Distance Selling Regulations (2000)
  - remote seller must identify themselves
  - details of contract must be delivered (email is OK)
  - right to cancel (unless service already delivered)
  - contract VOID if conditions not met

  - restates much of the above
  - online selling and advertising is subject to UK law if you are established in the UK – whoever you sell to
  - significant complexities if selling to foreign consumers if you specifically marketed to them
Politics & Terrorism

• Mainstream politics is now following the extremists onto the web
  – especially Obama (but Howard Dean did it first)

• Many issues arise on content
  – defamation, incitement, anti-terror laws

• Raising money raises lots of issues for parties:
  – need to know identity if amount over £200
  – need to report if over £5000 (or even £1000)
  – need to identify “permissible donors”
  – raising money for terrorism forbidden (!)
Deep Linking

- Pointing at specific pages on another website rather than the top level.
- Courts ruling against this when “passing off”
  - 1996 Shetland Times v Shetland News (UK) settled
  - 1997 TicketMaster v Microsoft (US) settled
  - 2000 TicketMaster v tickets.com (US) allowed [since clear]
  - 2006 naukri.com v bixee.com (India) injunction
  - 2006 HOME v OFiR (Denmark) allowed [not a database]
  - 2006 SFX motor sports v supercrosslive (Texas) injunction
  - 2007 Copiepresse Press v Google (Belgium) forbidden

19th May 2009
International Perspectives on Internet Legislation
Framing, Inlining & Linking

• Inlining isn’t being permitted
  – Kelly v Ariba (US) : thumbnails of Kelly’s photos in Ariba’s search engine were “fair use” but full-size “inlined” copies were not
  – and don’t do your own design of a Dilbert page!

• Linking is much less of a problem
  – even from disparaging site (US) Ford Motor Co case
  – but linking to bad things generally bad

• In general, framing causes problems
  – Hard Rock Café v Morton (US) “single visual presentation”
  – Washington Post v Total News (US) settled
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. Netherlands have gone with US, but sent a number of questions to the ECJ for a final answer

19th May 2009
International Perspectives on Internet Legislation
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)