It’s time to repeal Internet Legislation

BILETA 2009

23rd April 2009, Winchester, UK.

Richard Clayton

richard.clayton@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Outline

- IANAL!
- Computer Evidence
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- E-Commerce Regulations (2000 & 2002)
- Privacy & Electronic Communications Regulations 2003
- The Data Retention (EC Directive) Regulations 2009
- Policing the Internet

IANAL

- Background as a software developer
  - running a small software house, so learn to read contracts
- Company was sold to Demon Internet, UK's largest ISP
  - did the technical legwork on Godfrey v Demon Internet cases
  - expounded ISP industry views to DTI then Home Office
- Trustee of Foundation for Information Policy Research (FIPR)
  - campaigning on RIPA and other Internet legislation
- Academic since October 2000
  - PhD thesis (2005) looked at Internet traceability (which mainly works, except for all the corner cases)
  - have also researched content blocking systems, Internet censorship, effectiveness of take-down policies, spam &c
- Remain at Computer Laboratory, University of Cambridge

Computer Evidence

- Civil Evidence Act 1968
  - people used to be worried about “hearsay” issues
  - 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 – the banks found that the branch manager wasn’t quite the right person to do this!
  - does a faulty breathalyzer clock matter ? (DPP v McKeown)
  - s69 now repealed (1999) and replaced by a presumption that a computer system is operating correctly, but if this is disputed then relying party must demonstrate correct action
- So dumb (Red Flag Act) laws can be repealed...

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 (“the procrustean attempt” to make the facts fit the statute was disliked by the court)
- So failure of existing legislation to be effective led to specific legislation to cover “hacking”, virus propagation etc
- Why didn’t it lead to less specific definitions of fraud, forgery, misleading machines etc ? We had to wait until 2006 for the Fraud Act to see complexity reduced and the underlying principles established.

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 with intent to commit another serious offence
  - A sop to the 6 month maximum for Section 1 offences ?
- Section 3
  - Unauthorised modification
  - Intended to make virus writing illegal
  - Wording is remarkably opaque

Computer Misuse Act 1990

- Case law is extremely chequered
  - Fines have been small compared with damage caused, but courts have regularly imposed custodial sentences
  - Bedworth got off on an “addiction” defence (1991) whereas the other two pleaded guilty (albeit he was charged with conspiracy)
  - Whitaker convicted (but conditional discharge) for not disclosing a time-lock that froze bespoke software when client was late in making payments (1993)
  - Pile convicted of writing viruses and got 18 months (1995)
  - “AMEX” case (1999) is rather subtly distinguished from Bignell (1997), and apparently shows that multi-level access matters
  - Lennon (2005) [the Wimbledon case] gave us ruling that “mail bombing” is a s3 offence
  - Cuthbert (2005) [the tsunami hacker] was convicted of a s1 offence for some “../../../” URLs

CMA Revision

- Police and Justice Act 2006 revises CMA 1990
  - but then re-revised by Serious Crime Act because inchoate offences generalised, so delayed until October 2008 (except in Scotland)
- New tariffs, and timelimits removed
  - s1 to be maximum 2 years, s3 maximum 10 years
- s3 offence now covers denial of service
  - offence is “any unauthorised act” with intent to “impair the operation” or “prevent or hinder access” or “impair reliability of data”; NB: “act includes a series of acts”
- New offences for “hacking tools”
  - problem is that almost all such tools are “dual use”
  - DPP guidance on “distribution” illuminates little or nothing
  - at least the continental concept of “without right” is meaningful

Electronic Communications Act 2000

- Part II – electronic signatures
  - Electronic signatures “shall be admissible in evidence” (but they almost certainly were anyway, except in Scotland that had foolishly legislated otherwise)
  - Creates power to modify legislation for the purposes of authorising or facilitating the use of electronic communications or electronic storage (which hasn’t been used all that much)
  - Not as relevant, in practice, as people in the “dot com bubble” thought it would be. Most deployed systems continue to use contract law to bind people to commitments. Indeed Swiss Bank found that national signature laws more of a hindrance than a help.
- Remaining parts of EU Electronic Signature Directive were implemented as SI 318(2002)
- Rest of ECA vanished in a puff of sunset smoke

RIP Act 2000

- Part I, Chapter I interception
  - replaced IOCA 1985 (which had to be revised after Halford)
- 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

RIP Act 2000 – 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
  - techies running a network that need to peek at traffic
  - delivered data and stored data that can be accessed by production order (though the NPL case showed the flaws in this)
  - “Lawful business practice” (albeit only businesses)
- However...
  - you can’t do behavioural advertising using DPI
  - “passive DNS” may not be lawful

RIP Act 2000 – Encryption

- Basic requirement is to put 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 – but no caselaw yet
- Keys can be demanded (which frightens the horses)
  - 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 (perverting the course of justice is apparently not good enough!)
- In practice only being used on stored data; and in some cases retrospectively! Guidance on asking for keys is problematic.

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
- E-Commerce Directive (2002)
  - 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
- Needs significant revision to stop SMEs being caught in a cross-jurisdictional mess (ROME II and other initiatives may help)

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
  - does not prevent spamming of UK businesses
  - 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
  - although cookies got the politicians all excited, in practice there has been no enforcement whatsoever, and rules are ignored
  - most privacy policies are written using a little IBM program

Data Retention

- Anti-Terrorism, Crime & Security Act 2001
  - RagBag Act of everything buried at midnight at the crossroads
  - S47(1)(a) is an offence of knowingly causing a nuclear explosion
  - Part 11 has voluntary scheme for data retention by "communication service providers"
    - **compulsion threat was in an (eventually) sunsetting clause: cf: "The Retention of Communications Data (Extension of Initial Period) Order 2003"** & "**The Retention of Communications Data (Further Extension of Initial Period) Order 2005"**
- EU Data Retention Directive now transposed for ISPs
  - Directive often gibberish (blame the Swedes and Charles Clarke)
  - EU law says applies to all public CSPs
  - UK law says that only applies as and when the SoS tells you, and that the SoS must tell everyone it should apply to (so Brussels is happy, so are the police, and so is the Treasury, but not the RIAA)

Access to Retained Data

- EU envisaged retained data only used for serious crimes
- Home Office view is that once it is retained it can be accessed for any reason, the only tests being “necessary & proportionate”
- Interception Modernisation Programme will extend reach
  - and will trawling be allowed ? “We can find all visitors to lolita.com”
- Expect to see a growth in use in civil cases:
  - copyright infringement (most caselaw involves this)
  - defamation (Totalise v Motley Fool had website records...)
  - detecting whistleblowers (cf Hewlett Packard case)
  - messy divorces (Mellon case involved illegal interception, but why would a High Court judge refuse to grant Norwich Pharmacal orders to access communications data? and could legislation prevent such orders being made ?)

What’s missing ? [so no need of repeal]

- Effective anti-spam laws
  - cf: Marine Broadcasting Offences Act 1967
- Security breach notification
  - almost all US states have this
  - Pounder argues that DPA says this anyway
  - Government operating a de facto scheme
- ISP liability for ignoring abuse
  - an economists argument : need incentives to fix behaviour
- Software Liability
  - you can’t sell hamburgers that make people ill…
- Single market online (iTunes, trademarks, eBanking)
  - physical goods can be grey imported from Sofia…
  - …but you try paying for your iTunes in Euros!

Jeux sans Frontieres

- The Internet doesn’t have borders (duh!)
- You can’t even assume that a “.uk” website is within the UK
    - you can’t even assume a “.nl” website is in Holland
- To deal with wicked foreigners, the approach has been to try and harmonise laws (and penalties)
    - pressure put on countries to harmonise child sexual abuse image laws (Japan didn’t make them illegal until 1999);
    - BUT still a lot of inconsistency about possession, grooming, computer generated images, drawings and text
    - progress on “hacking” and “viruses” has been extremely slow; Twelve EU Member States have not yet ratified the Convention on Cybercrime (including the UK; took till October 2008 to fix tariffs)
    - much of the later sections of the Convention (on trap and trace for example) is really just wishful thinking

Fragmented Laws & Policing

- BUT real problem isn't laws but enforcement across borders
  - harmonising legislation is how the US dealt with bank robbers who fled across state lines. They made bank robbery (& auto theft) into Federal offences; but it only worked because the FBI existed
- There is no pan-European (let alone worldwide) policing
  - Interpol just a fax relay system
  - MLAT makes glaciers look quick
  - "joint operations" used for drugs, but seldom for Internet crimes
- ENISA Report "Security Economics and the Internal Market" (Anderson, Bohme, Clayton, Moore, Feb 2008)
  - **Recommendation 14: "**We recommend the establishment of a EU-wide body charged with facilitating international cooperation on cyber-crime, using NATO as a model"
  - not picked up by ENISA, and not even on Home Office radar

Conclusions

- Most crimes on the Internet never needed special laws (death threats, extortion &c) “If it’s illegal offline, it’s illegal online”
- So why did we get special rules for computer hacking, viruses, denial of service, ownership of attack tools, etc ?
- Seems to have come from too great an emphasis on legal theory, can you “steal” data ? can you “defraud a machine” ?
- Instead of generalising old notions, we’ve seen ever more specific legislation for computers and cyberspace
- Also Governments seem to have been wary of making new crimes “serious” (so CMA offence tariffs started quite low)
- So it’s past time to repeal all these specific laws and generalise the harms (as the Theft Act 1968 and Fraud Act 2006 achieve)

More..

ENISA Report (and comments)

http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm

Cambridge Security Group Blog

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory