III: "Regulating"

Abuse, Bulk email, Cryptography, Defamation and Everything else

25th January 2002

Richard Clayton

These lecture notes were specially prepared for the Cambridge University Computer Science "Additional Topics" course, Michaelmas Term 2002.

richard.clayton@cl.cam.ac.uk

Outline

- The classic self-regulation approach
- Child pornography and other nasty things
- Unsolicited bulk email
- Spam on Usenet
- Regulating cryptography
- Data preservation
- What about national borders ?
- Defamation
- The ECommerce Directive

29th November 2002 Regulating

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

- E-Policy
  - Security Engineering : Anderson
  - Crypto : Steven Levy
  - http://www.eff.org/
  - http://www.fipr.org/
- Nasty things
  - http://www.iwf.org.uk/
  - http://www.cyber-rights.org/
  - http://www.fiawol.demon.co.uk/FAC/back.htm
- "Spam"
  - http://www.cauce.org/

29th November 2002 Regulating

✶ Since almost everything covered in this lecture has happened in the past six years it probably isn't surprising to find very few books on the topic. However, almost all the original documents are still available online along with detailed records of the many discussions through which people came to understand the meaning of what was happening.

✶ Ross Anderson's book covers slightly different areas than this lecture, reflecting in each case where we each had first hand experience. Where the issues overlap it is usually because the Foundation for Information Policy Research (a high-tech policy "think tank") was involved. Ross chairs this organisation and I play my part on its Advisory Council.

✶ Steven Levy's book tells the story of crypto regulation in the USA, majoring on the role played by the NSA. It's American in style (stressing "personalities" over events), but very readable. Since the UK's line on these issues has followed the US (with a lag of a couple of years and taking no notice of the failure of the policy in the US), it is of considerable relevance.

✶ *Like all histories, the importance and significance of various events will be chosen by the presenter. You should approach this lecture as a biased account of what really happened, from which some truths may emerge.*

Classical Self-Regulation

- The Internet is a network of networks many of which are not in the U.S.A. ! This realisation, married to the type of users of the early Internet, led to a culture of tolerance.
- "Abuse of the Net", not "Abuse on the Net"
- Worked well where sysops could discipline students – but challenging for commercial ISPs
- Can still be seen in operation for most day-to-day abusive behaviour (port scans, bulk email, Usenet spam…)

29th November 2002 Regulating

✶ The original culture of the Internet (back in the days before the endless September of 1993 when AOL properly connected their users) was a laid back tolerance of differences, codified by a few clear thinkers who could match principles with detailed rationales. Flaming people for being unable to spell was not only intolerant, it was also deeply embarrassing when you discovered that you were conversing with a paraplegic typing with a stick gripped between their teeth. The connection of networks from other countries outside the USA led people to realise, perhaps for the first time, that US laws and the US Constitution were not universally applicable. This was promptly misunderstood by many as meaning that no law applied to the Internet – a source of confusion to this day.

✶ The lack of universal law led to the concept that the true crime was to abuse the network itself; abuse "on the net" (telling correspondents what you thought of their mental abilities, parentage or personal habits) was tolerated because the clear thinkers saw that there was no practical way to draw a universal line between acceptable and unacceptable.

✶ Most users of the Net were connected via their employer or university, who were in a position to take effective local action (usually disconnection) against anyone who offended against community standards. Abuse "of the net" therefore stopped quite rapidly once complained about.

✶ For a 1994 view of Internet culture see:
http://www.cosy.sbg.ac.at/doc/eegtti/eeg_268.html#SEC269
or read an early edition of Kehoe's "Zen and the Art of the Internet".

Nasty Things on the Net : 1

- Most 1980s users were, male, single and under 30; not surprising to find strange things being swapped behind the virtual bikesheds
- 16 Aug 1996 "French letter" (Charing X C&V)
  - lists 130+ groups containing "pornographic material"
  - "publication of obscene articles is an offence"
- 25 Aug 1996 "Observer article"
  - "the pedlars of child abuse"
  - implausible claim that 90% of child porn went through anon.penet.fi

29th November 2002 Regulating

✶ See "The Great Renaming FAQ"

http://www.uncommon-sense.net/interests/usenet/renaming-faq/

for the history of how sex, drugs (and the artistically necessary rock-and-roll) got their own parts of Usenet in the late 1980s.

✶ In August 1996 some ISP representatives attended a seminar at New Scotland Yard on illegal material on the Internet. The "French Letter" was sent by Chief Inspector Stephen French of the West End Clubs & Vice unit (based at Charing Cross police station). It was rapidly leaked, causing a furore.

http://groups.google.com/groups?selm=4v23g7$kea@news.ox.ac.uk

✶ Later in the month the Observer ran an article claiming that ISPs in general and Demon Internet in particular were "the pedlars of child abuse". They also blamed Helsingius (anon.penet.fi) for 90% of the pornography on Usenet (though since the maximum message size was 16K and only 10 articles per person per day were allowed, this was patent nonsense).

✶ Helsingius shut down anon.penet.fi shortly afterwards, but this was all to do with the Scientologists and nothing to do with the Observer.

Nasty Things on the Net : 2

- "R3" Safety-Net agreement (Sept 1996)
  - "Rating, Reporting, Responsibility"
  - Government (DTI, Home Office)
  - Police
  - ISPs (ISPA, LINX, Peter Dawe)
- Safety-Net Foundation renamed as the Internet Watch Foundation
  - runs a reporting hotline
  - distributes reports of illegal material
  - researches into rating systems (RSACi, ICRA &c)

29th November 2002 Regulating

✶ As a result of the fuss in August, an agreement was rapidly reached in September 1996 to set up a body to deal with illegal material on the Internet.

✶ Under UK law, it is not illegal to possess pornography though you can commit an offence under the Obscene Publications Act for publishing it or selling it (and Customs can confiscate it if you import it).

However, mere possession of child pornography (defined, roughly, as indecent photographs or pseudo-photographs of children under 18 or appearing to be under 18) is a serious arrestable offence. For this you could get 6 months in gaol in 1996, up to 5 years now. (Distribution of child pornography had a maximum sentence of 3 years, now 10).

✶ The possession offence is absolute, in that there is no defence (unless you discard it immediately upon receiving it). The R3 agreement was, in effect, though this was never written down, that ISPs would not be prosecuted if they funded the IWF. The IWF would run a reporting system that would collate information about child pornography and then distribute the reports to ISPs. ISPs would then remove the material (from web sites or from Usenet).

✶ A second strand of IWF action would be to help develop rating systems so that adult material could be labelled and thus kept away from children.

Nasty Things on the Net : 3

- Rating
  - ICRA (http://www.icra.org/) sinking without trace although the EU still believes in it
- Reporting
  - IWF hotline is big success & is copied worldwide
- Responsibility
  - IWF structure reviewed in 1999 and governance extended to include "Children's charities"
  - UK ISPs now "recommended" to remove newsgroups that regularly contain child pornography and must now also remove those that "advertise" its presence

29th November 2002 Regulating

✶ Looking at the IWF today, we can see the following results:

- Some 40,000 illegal Usenet articles have been detected and removed along with many child pornography websites, both in the UK & abroad
- No ISP has had their news server seized by the police (as has actually happened in the USA)
- Government ministers continue to endorse it as a wonderful example of self-regulation (though it's not really a regulator in the normal sense).
- Other countries have copied the hotline idea (and they have created an umbrella organisation called INHOPE).
- The original RSACi rating system has been further developed as "ICRA" and a handful of sites are rated using it.

✶ A review in 1999 changed the structure to reduce the influence of the ISPs on the IWF board and to create an independent chair.

✶ The IWF finds that much of the illegal material occurs in a handful of newsgroups and is now recommending that ISPs drop whole newsgroups rather than individual articles. Also, new legal advice is that where names suggest that illegal material is present (whether or not it actually is) then carrying the newsgroup means committing an offence under s1(1) of the Protection of Children Act 1978.

Nasty Things on the Net : 4

- June 1999: concern within ICF about IRC
  - "Chatwise, Streetwise" document March 2001
    http://www.internetcrimeforum.org.uk/
- early 2001: Carol Vorderman on "*Tonight with Trevor MacDonald*" & in "*News of the World*"
  - "your child is two clicks away from a paedophile"
- Apr 2001: Home Office Task Force created
  - reviewing law on "grooming"
  - running a parental education campaign
  - reviewing co-operation in this area
    http://www.homeoffice.gov.uk/cpg/internetask/

29th November 2002 Regulating

✶ More recently, attention has moved on from illegal images, to paedophiles "grooming" (a fancy word for soliciting) children in online chat rooms. There were a handful of cases of actual harm being done to children.

✶ The Internet Crime Forum (the new name for the ACPO/ISP liaison body) created a very informative document discussing the issues (and their complexity). In particular it showed that the problem wasn't just IRC (which needs ISP based servers to run) but web-based chat (which almost anyone can add to their site).

✶ The sentencing of the "Operation Cathedral" defendants led to Carol Vorderman producing a couple of reports shown on ITV's "*Tonight with Trevor MacDonald*" and running a campaign in the "*News of the World*". This focussed on how if one went into channels called such enticing names as "younger girls for older men" or "girls watching guys jerkoff" one was likely to be approached by people making indecent suggestions – or trying to build relationships that might lead to real world assignations.

See: http://www.zdnet.co.uk/news/specials/2001/03/netcrime/chatroom/

✶ The upcoming election put pressure on the politicians and in April 2001 Jack Straw, the Home Secretary at the time, announced a "Task Force" to look into the whole area. This body is still in existence; doing things!

Unsolicited Bulk Email : 1

- A very old problem (see RFC706, Postel 1975)
- Make Money Fast: "My name is Dave Rhodes. In September 1988 my car was reposessed and the bill collectors were hounding me like you wouldn't believe."
  - MMF still exists – but natural selection has changed it out of all recognition.
- Growth of other types of unsolicited email occurred in the 1990s with the arrival of the commercial Internet

29th November 2002 Regulating

✶ "On the junk mail problem", Jon Postel, RFC706, 1975

It would be useful for a Host to be able to decline messages from sources it believes are misbehaving or are simply annoying.

✶ The original "Make Money Fast"

http://www.cs.rutgers.edu/~watrous/txt/David.Rhodes.chain.letter

✶ For a list of variations (relatively old)

http://www.stopspam.org/usenet/mmf/mmf_variants.html

and also

http://www.mmfhoh.org

✶ Within a couple of clicks of the above two sites you'll find authoritative info on why MMF doesn't work (for the mathematically challenged) as well as pointers to the laws that make it illegal in many jurisdictions.

Unsolicited Bulk Email : 2

- To send in bulk, a permanent connection is needed (because remote sites can be slow)
  - using your own ISP's "smart host" will result in the loss of your account (hence various "whack-a-mole" activities by ISPs who cannot validate their users)
  - using insecure machines is unlawful, but effective. Currently a problem for Korea, South America, Japan (where documentation is harder to access)
  - carriers have fixed their contractual terms to avoid problems such as Cyber Promotions (Oct 1996) where Sanford Wallace had his leased line reinstated for two weeks.

29th November 2002 Regulating

✶ For general information about unsolicited bulk email see:

http://spam.abuse.net/

✶ For information about "open mail relays" see:

http://www.mail-abuse.org/tsi/

✶ For a short history of the Cyber Promotions story (written at the time)

http://news.cnet.com/news/0-1004-200-323154.html

Sanford Wallace is still around (and annoying people):

http://news.cnet.com/news/0-1005-201-4687442-0.html

but AGIS went bankrupt in 2000

http://www.internetnews.com/isp-news/article/0,,8_313771,00.html

Unsolicited Bulk Email : 3

- Various state laws in the USA – many aim to ensure that filtering works correctly, though some address the underlying nuisance.
- Still no US Federal Law – though in the past, some provisions have passed both Congress and the Senate. Either CAUCE or the DMA (or others) have lobbied enough to block change.
- The EU "Telecoms Data Protection Directive" 97/66/EC was supposed to outlaw junk email, but the UK looked too hard at the definition of a "call" and viewed email as *ultra vires*.

29th November 2002 Regulating

✶ An excellent survey of laws in the US and EU about unsolicited bulk email can be found at:

http://www.spamlaws.com/

✶ "Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector" can be found at:

http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

✶ UK Statutory Instrument 1999 No. 2093: "The Telecommunications (Data Protection and Privacy) Regulations 1999" can be found at:

http://www.hmso.gov.uk/si/si1999/19992093.htm

Unsolicited Bulk Email : 4

- The EU "Distance Selling Directive" 97/7/EC gave a choice between "opt in" and "opt out". The UK Government decided not to decide.
- The "Directive on Privacy and Electronic Communications" 2002/58/EC has "soft opt-in" and must be implemented by 31 Oct 2003.
  - Email addresses obtained from customers "in the context of the sale of a product or a service" can be used for direct marketing of your "own similar products or services" provided customers can opt out (for free) when the data is collected and also whenever a message is sent.

29th November 2002 Regulating

✶ There is specific jargon relating to various email policies:

- "opt out" means that the email can be sent unless people specifically request otherwise. This is usually expected to be in conjunction with a global preference register.
- "opt in" means that email can only be sent to people who specifically request that it be sent.
- "soft opt in" is "opt in" plus customers

Most consumers and ISPs want "opt in", most marketeers want "opt out".

Caution: some people use "opt in" and "opt out" to distinguish between data collection forms that require a positive tick to receive email or a positive tick not to receive email. This usage, in my view, confuses.

✶ "Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 On the Protection of Consumers in Respect of Distance Contracts" can be found online at:

http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf

✶ "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) is at:

http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Usenet "Spam"

- Jan 94 : Clarence Thomas IV posts a warning to all newsgroups of Jesus's imminent return
- Apr 94 : Canter & Siegel crosspost their "Green Card" lottery spam to all of Usenet
- 1994 : "Cancel Moose" starts cancelling spam (but decides NoCeM is a better scheme)
- Aug 97: first "active" UDP against UUNet
- Current situation is entirely self-regulatory; a steady-state with about 100,000 articles a day (~8%) cancelled by three activists.

✶ "Global Alert For All: Jesus Is Coming Soon"

http://groups.google.com/groups ?selm=9401191510.AA18576@jse.stat.ncsu.edu

✶ "Green Card Lottery– Final One?"

http://groups.google.com/groups ?selm=2odkr9$3r5@herald.indirect.com

✶ Cancel Moose home page

http://www.cm.org/

✶ Usenet Death Penalty FAQ

http://www.stopspam.org/usenet/faqs/udp.html

✶ Cancel statistics are posted daily to the *news.admin.net-abuse.bulletins* newsgroup. Details of the consensus view on cancels can be found in a FAQ at:

http://www.killfile.org/faqs/spam.html

Regulating Cryptography : 1

- Cryptographic systems long seen as munitions and this evolved into a "key length" regime
- In 1993 US proposed the Clipper Chip (EES), the "Escrowed Encryption Standard". Keys to encrypted phone calls would have a back door for use by Law Enforcement. Opposed by civil liberties groups and industry who wanted secure encryption systems. The Clinton administration backed down, and Clipper itself was a complete commercial flop.

29th November 2002 Regulating

✶ For a history of cryptography and its regulation (though with a US bias) see: "Crypto : Secrecy and Privacy in the New Code War", Steven Levy, Allen Lane The Penguin Press", 2001.

Levy's book has an entire chapter on Clipper. In summary, the NSA's idea was to create an key escrow system for encrypted voice communications. Encryption of telephone traffic would be encouraged, but Law Enforcement would be able to obtain the keys if they produced a suitable warrant.

The scheme was ambitious, involving a new block cipher (Skipjack) and a PKI (creating a system called Capstone). It was considered risky to keep the keys in software, so a special chip called "clipper" was to be created. The chips would be unique, with unique keys.

When a phone called was to be tapped a special LEAF (Law Enforcement Access Field) would be captured – this contained (in effect) the session key encrypted with the unique key for the chip. Law Enforcement would be able to obtain this key from a database and thereby listen to the conversation. The database would be split over two sites, so that two warrants were needed to access the keys.

Clipper was adopted by the incoming Clinton administration, but it was attacked from all sides, turned out to have technical flaws in that the LEAF field could be spoofed, and flopped in the marketplace (the chip was too slow, and the "back door" made it unattractive to companies that might wish to export it).

Regulating Cryptography : 2

- Meanwhile in Europe the issue became entangled with "digital signatures"
- John Major's government proposed what was effectively compulsory key escrow with "Trusted Third Parties" in Spring 1997 (& lost power in May).
- New Labour had opposed key escrow in opposition, but succumbed to the LEA's (and official's) view once in power…

✶ A very extensive collection of documents on cryptography regulation in the UK can be found at http://www.fipr.org/

✶ The DTI consultation paper can be found at:

http://www.fipr.org/polarch/ttp.html

The Government believes that the ***positive (and individual) licensing of TTPs*** […] is critical in allowing the initial assessment, monitoring and regulation of a TTP that would meet the requirements of consumer protection, trust in the market and security, intelligence and law enforcement access.

In terms of Key Recovery the proposed legislation is concerned solely with legal access to private encryption keys (which are used to protect the confidentiality of information) required by the authorities in connection with the lawful interception of communications (i.e. information on the move) or for lawful access to data stored and encrypted by the clients of licensed TTPs. There is, of course **no** intention for the Government to access private keys used for only integrity functions. Legal access to encryption keys will be permitted through serving warrants on TTPs.

✶ New Labour's position paper on encryption mysteriously disappeared from their website after their election. An archived copy can be found at:

http://www.fipr.org/polarch/labour.html

Regulating Cryptography : 3

- March 1999 : Blair rejects key escrow and sets up COJET to examine the consequences
- Draft ECommerce Bill still wanted to license cryptography service providers
- August 1999 : Home Office consultation on replacing IOCA 1985 (phone tapping)
- Lots of lobbying by industry – exploiting differences of opinion between Home Office and Department of Trade & Industry

29th November 2002 Regulating

✶ COJET, the Cabinet Office Joint Encryption Taskforce (assorted civil servants from the DTI, Home Office and the Security Services) talked to "industry"about what the landscape would be like with no key escrow. Their report, published under the guise of the Cabinet Office Performance and Innovation Unit (PIU) was called "Encryption and Law Enforcement"

http://www.fipr.org/polarch/piu.pdf

It recognised the new political reality of "no key escrow" and proposed voluntary licensing of TTPs, co-operation with industry, a technical assistance centre to handle encryption issues [this exists and is called NTAC], a statutory requirement for people to say where keys are held and international co-operation.

> "There is no 'silver bullet' policy that guarantees that the development of encryption will not affect law enforcement capabilities."

✶ Along with this was published a draft "Electronic Communications Bill"
http://www.fipr.org/polarch/draftbill99/

✶ The Home Office consultation on updating the Interception of Communications Act 1985 (IOCA) was issued in June 1999. Unlike the DTI, they keep old pages available:

http://www.homeoffice.gov.uk/oicd/interint.htm

Regulating Cryptography : 4

- Electronic Communications Act 2000
  - Part I : Licensing scheme for cryptographic service providers (suspended with 5 year sunset clause)
  - Part II : Electronic signatures admissible in evidence. Statutes concerned with "writing" can be amended
- Regulation of Investigatory Powers Act 2000
  - Part I Chapter I : Tapping
  - Part I Chapter II : Comms Data
  - Part III : "putting into an intelligible form"
  - much is yet to come into force and the detail is in Codes of Practice & SI's that do not yet exist

29th November 2002 Regulating

✶ The DTI and Home Office parted company and decided to put two separate bills through parliament. The DTI part was the Electronic Communications Act 2000. The regulation of cryptographic service providers was suspended (in the hope that a voluntary scheme would work) and the rest was, to a large extent, uncontentious. The statute can be found at:

http://www.hmso.gov.uk/acts/acts2000/20000007.htm

✶ The Home Office legislation (which became the RIP Act 2000) included in Part I, a revision of IOCA 85 and new powers to access "traffic data" which related to telecommunications. In Part II there was, for the first time, statutory control of surveillance, use of informants etc, which was required by the Human Rights Act. Part III contained the laws relating to encryption that had been in the previous year's draft Bill.

✶ RIP was extremely controversial. It was attacked by ISPs concerned about the cost of the new measures in Part I. It was also attacked by the civil liberties lobby for its "reversal of the burden of proof" in Part III (you had to prove that you didn't have an encryption key). In the event, the Government significantly modified it in the House of Lords (and the "burden of proof" issue was fixed). The Government was defeated over the ISP cost issue and a a "Technical Advisory Board" was added to address concerns on interception.

✶ Much of the detail is not in the Act at all, but will appear in Codes of Practice or Statutory Instruments and many do not yet exist (since they have turned out to be extremely hard to write). For the current state of play see:

http://www.homeoffice.gov.uk/ripa/ripact.htm

Data Retention

- Cybercrime Convention
  - Data Retention is having a logging system
  - Data Preservation is ensuring entries are kept
- Regulation of Investigatory Powers Act 2000
  - allows access to "traffic data"
- September 11th 2001
  - Maybe they used the Internet
  - Maybe there's some logs (maybe there isn't)
- Anti-Terrorism, Crime and Security Act 2001
  - Part 11 "Retention of communications data"

29th November 2002 Regulating

✶ The Convention on Cybercrime was created under the auspices of the Council of Europe. It started off as a law enforcement wishlist (with roots in the EUROPOL initiatives of the 1990s). In the event, pressure by civil liberties bodies has toned it down a little, but not much:

http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm

✶ The ATCS Act was created in a hurry after the events of Sept 11th 2001. It contains numerous measures that the Home Office had been considering for some time but were unable to find political endorsement for. The relevant part of the Act (for this lecture) relates to "retention of communications data".

http://www.hmso.gov.uk/acts/acts2001/20010024.htm

✶ As discussed in a previous lecture, logs can only be lawfully kept if there is a business need. The ATCS Act attempts to fix this (from the point of view of the LEAs) by creating a "Code of Practice" whereby all the nice ISPs will keep logs for the benefit of Law Enforcement

s102(3) A code of practice or agreement under this section may contain any such provision as appears to the Secretary of State to be necessary–
(a) for the purpose of safeguarding national security; or
(b) for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security.

✶ If the ISPs don't play ball then there are powers to make the Code of Practice compulsory. It is unclear how the "national security" aspect can be ascertained when the logs are first kept! The Information Commissioner has now derailed the process and there's been no progress since March 2002.

The "Snooper's Charter"

- Draft RIP (Communications Data: Additional Public Authorities) Order 2002 published
  - added 24 new types of authority to RIP Pt I Chap II eg Food Standards Agency and all local councils
- FIPR Press Release picked up by the Guardian
- By end of the week in all the papers & a great many people were faxing their MPs
- David Blunkett backed down the next week
- Consultation on revised proposals is expected

29th November 2002 Regulating

✶ The draft SI is preserved at http://www.fipr.org/press/SI20022322.html

✶ The FIPR press release (10 June 2002) can be read at:
http://www.fipr.org/press/020610snooping.html

✶ The Guardian story (11 June) "Government sweeps aside privacy rights" is at: http://www.guardian.co.uk/humanrights/story/0,7369,731074,00.html

✶ Most other papers campaigned on the issue. A lot of the general public told their MPs what they thought, particularly using a "fax your MP" system:
http://www.faxyourmp.com/

✶ The abandonment of the plans is reported by the BBC at:
http://news.bbc.co.uk/1/hi/uk_politics/2051117.stm
and Andrew Marr's report "quite a day in British politics" is at:
http://news.bbc.co.uk/media/video/38084000/rm/_38084144_privacy22_marr_vi.ram

✶ The Home Office have been doing some pre-consultation on the UKCrypto mailing list:
http://www.chiark.greenend.org.uk/pipermail/ukcrypto/2002-October/020853.html

The Monde Sans Frontières ?

- Governments are not yet ready to allow police forces to operate across national borders. Hence the idea of Mutual Legal Assistance
  - Cybercrime Convention's data preservation idea is to allow volatile data to be kept whilst the Foreign Office decides on national policy grounds whether to release it – complexities for "hot pursuit".
  - if police wish to assist they create a "joint operation"
- Legal judgments are hard to enforce across borders. The "Hague Convention on Private International Law" (2002) may change this

✶ The Hague Convention on Private and International Law is considering a future "Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters".

see: http://www.hcch.net/e/workprog/jdgm.html

The idea is to make civil judgments enforceable in other countries. This has significant implications for Internet commerce and also, because many of these matters are civil, for the protection of free speech and copyright matters.

Defamation

- Defamation Act 1996 provides a modern version of "innocent dissemination"
  - other defences include "justification" (it was true)
- Godfrey v Demon Internet (1997-9) showed that once "put on notice" ISPs had to remove defamatory material.
- Actions are still rare (despite the flame wars one sees on Usenet) but there seems to be a significant growth in the US by companies defending their reputation

29th November 2002 Regulating

✶ The Defamation Act 1996 does not treat ISPs specially, but does provide significant protection for an ISP that is unaware that it is publishing something defamatory:

s1(1) In defamation proceedings a person has a defence if he shows that […] (c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

see: http://www.hmso.gov.uk/acts/acts1996/1996031.htm

✶ For a discussion of Godfrey v Demon Internet see:

http://www.cl.cam.ac.uk/~rnc1/Judge_and_Jury.pdf

Please note that the account I give has been challenged by Dr. Godfrey, who takes issue with some of the detail and the way I present the material. You should not assume that it is a completely unbiased account of events.

The main point of the paper is to draw attention to complexities that arise with "notice and take down" regimes. These complexities extend far beyond defamation and represent a difficult problem for the ISP industry and for those concerned with "freedom of speech" issues.

✶ In May 1999 the Harvard Law Review considered defamation issues in (US) cyberspace:

http://www.harvardlawreview.org/issues/112/7_1610.htm

for a more up-to-date review of relevant cases:

http://www.phillipsnizer.com/internetlibrary.htm

The ECommerce Directive : 1

- Important EU Directive (00/31/EC)
  - topic put on "fast track" by Blair et al in Fiera Portugal, June 2000
- ECommerce is to work across national boundaries and should not be licensed. Some consumer protection is made mandatory.
- For ISPs key provisions are
  - Article 12 : Mere Conduit
  - Article 13 : Caching
  - Article 14 : Hosting
  - Article 15 : No obligation to monitor

✶ "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')" can be found at:

http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html

✶ This was transposed into UK Law as: "The Electronic Commerce (EC Directive) Regulations Statutory Instrument 2002 No 2013".

http://www.legislation.hmso.gov.uk/si/si2002/20022013.htm

The ECommerce Directive : 2

- Most of the ideas are sound, but the detail is complex and may obstruct progress
- Many key questions on national laws have not been fully answered.
- Thorny question of "actual knowledge" not yet resolved – EU Commission only beginning to understand complexities (not just defamation but other issues such as copyright)
- Article 7 requires unsolicited commercial email to be labelled – but envisages "opt out"

29th November 2002 Regulating

✶ Online selling and advertising is subject to UK law if you are established in the UK – whoever you sell to. However, there are significant complexities when selling to foreign consumers if you specially marketed to them. There's useful guidance from the DTI:

http://www.dti.gov.uk/cii/docs/ecommerce/smallbusinessguidance.pdf
http://www.dti.gov.uk/cii/docs/ecommerce/businessguidance.pdf

These 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/cacp/ca/policy/jurisdiction/rome.htm

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/cacp/ca/policy/jurisdiction/brussels.htm

✶ In practice, some provisions of the ECommerce Directive will be overridden by a later series of Directives relating to telecommunications that will come into force in June 2003. The Communications Bill that will shortly be before Parliament addresses the UK's obligations under these directives.

http://www.communicationsbill.gov.uk/

Review

- The Internet is still mainly self-regulating
- Governments have grasped the idea that normal laws apply in cyberspace
- Governments have not yet really understood how national boundaries have been eroded
- UK Regulation has mainly been in response to international pressure (from US & Brussels)
- Interest in hot topics (spam, porn etc) has led to self-regulation. This has meant flexibility

29th November 2002 Regulating

✶ If you are interested in these topics, then there is a great deal of online discussion of the issues. Particular attention is drawn to the UKCrypto and the Cyber-Rights-UK mailing lists:

http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto

http://www.cyber-rights.org/mailing.htm