

[Contractual Terms Between]
ISPs and Their Customers

Dr Richard Clayton



**UNIVERSITY OF
CAMBRIDGE**
Computer Laboratory

Communications
Research Network
London, 13 Nov 2006

Summary

- Many different viewpoints
 - historical, contractual, common law...
- Set in European context
 - and a worldwide peer relationship
 - and industry Best Current Practice documents
- Dealing with customers isn't easy
 - is “walled gardens” (sin bins) the future ?
- Monitoring isn't a panacea

An Historical View

- Early Internet users were invariably students or employees and were easily controlled
 - they would be disconnected if they misbehaved and thereby brought the institution into disrepute
 - and yes they were! (sysadmins are Gods!)
- This model continues into the commercial era. In theory an “outlaw” ISP will be shunned by its peers and cannot remain in business
 - albeit, very few examples of this in practice

A Contractual View

- ISP contracts to provide connectivity (and other services such as email/webpace)
- Customer contracts to “behave”
 - not send spam or “hack” other systems
 - not defame people or breach copyright
 - not to send material that is “grossly offensive or of an indecent, obscene or menacing character” or that causes “annoyance, inconvenience or needless anxiety” (s127 CA 2003 & earlier)

A Confidential View

- ISPs handle customer emails and other communications in confidence
 - seldom explicitly stated, but clearly understood
- It is to be expected that this confidence will extend to the entire customer/ISP relationship
 - so considerable limits to what an ISP ought to disclose about a customer without legal compulsion
- Where customer is an individual then personal data is covered by provisions of the DPA 1998

The European View

- E-Commerce Directive gives ISPs the freedoms they need to underpin the network society
 - provisions were carefully thought through
- ISPs have significant immunities as a “mere conduit” (related to “common carrier” ideas)
 - ISP must avoid selecting or altering traffic
 - unlike “hosting” or “caching” there’s no “notice and take down” regime for “mere conduit”
- Also, ISP has “no obligation to monitor”

An abuse@ view

- Necessary to deal with reports of outgoing “spam” or all email will be blocked
 - same team will deal with many other issues (hacking, port scanning, defamation etc, etc)
- ISP’s “acceptable use policy” (AUP) gives formal basis for taking action
 - however, these days the customer isn’t the spammer; their machine has been hijacked usually (these days) without them noticing

A Barrack-room View

- In principle customers could be “framed”
- In practice this never happens!
 - anyway, header forgery is hard (some email spam tries to do this to mislead reporting systems) and can be rapidly detected
 - currently most DDoS attacks eschew IP address spoofing (it’s an unnecessary complication and requires more work – especially with XP SP2)
- Trust given to “feedback loops” and some lists

The Accountant's View

- ISP's currently sell mainly on price
- ISP's only marginally profitable (if that!)
- Major variable costs are bandwidth (can be charged back to customers) and support (can be provided on pay-per-use basis)
- Abuse team is pure overhead
 - significant pressure to keep headcount down
 - no tradition of charging customers for abuse

An Industry View

- LINX Best Current Practice documents
 - capture the industry consensus
 - educates **abuse@** teams at smaller ISPs
 - provides consistent information to customers
 - regulators/legislators see a responsible approach
- ✓ Bulk Unsolicited Email (1999, revised 2004)
- ✓ Operating Mailing Lists (2001)
- ✓ User Privacy (2001)

A Practical View

Q: what is it like at the sharp end when you try to deal with customers with “abuse” problems ???

A: complex and time consuming ☹️

Getting the Customer's Attention

- ISP email may not be received or read
 - `postmaster@subdomain.isp.co.uk`
- Telephone contact details may be inadequate
 - customer has moved, or doesn't keep office hours
- Cutting the customer off means they call you!
 - but only eventually!
 - excellent way of losing their business!
 - customers object to pay-per-minute helplines

Fixing the Customer's Problem

- Customer must identify and remove malware
 - essential to be online to get the fixes
 - modern malware prevents access to AV sites
 - AV systems struggling to keep up with detection
 - simplest solution may be to reformat disk
 - US Consumer Reports data:
 - 39% had virus infection in past two years
 - 34% had reformatted hard drive
 - 8% had replaced the machine

Walled Gardens (sin bins)

- Idea is to allow customers online, but stop access to all but anti-virus (etc) sites
 - gets the customer's attention ! (eventually)
 - allows them access to appropriate resources
 - ensures that they cannot do any more damage
 - permit self-release (reducing call centre load)
- Expensive to set up and run
 - & expect next generation malware to self-release!

Monitoring

- Illegal to intercept traffic (s1 RIP Act 2000)
 - exceptions for network protection reasons
 - wise to get customer permission for spam filtering
- Experience of monitoring email traffic is that there are HUGE variations between customers (viz: you will get a lot of false positives)
- Existing abusive traffic quite easy to spot by monitoring. But no need to hide at present, so don't base policy on this being inherently so.

Conclusions

- “Unwanted traffic” continues to be a significant and growing problem
- UK ISPs are (almost entirely) dealing with “innocent” customers who are unaware of the problems their machines are causing
- Fixing these problems is expensive and time consuming for all concerned
- Monitoring is unlikely to work in long term

ISPs and Their Customers

`http://www.cl.cam.ac.uk/~rnc1/`

`https://www.linux.net/bcp/`



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory