An ISP Perspective

Presented to: ECLIP workshop

24th January 2001

by Richard Clayton
Internet Expert
Thus plc

Outline

- The “current” landscape
- What ISPs don’t care about
- Interception (tapping)
- Section 12 and the TAB
- Communications data
- The Telco experience
- Where we are today

“Current” landscape I

- ISPs on the side of law enforcement; but want to get on with running their businesses
- DPA 1998 S29(3) notices put onus on the ISP to check validity of request. Optional to respond, but “Best Practice” to do so.
- IWF (1996 onwards) is part of a “unspoken deal” to avoid ISP liability. But specialist area, expensive to run and so doesn’t scale.

“Current” Landscape II

- Totally unclear to what extent IOCA 1985 covered email.
- Some said that email was seizable with a PACE production order.
- RIP 2000 is supposed to clear up the confusion - but, perhaps not unexpectedly, is currently adding to it.

Some of RIP is irrelevant to ISPs

- Part II - informers, stakeouts and buggers
- Part III - seizing plaintext & encryption keys
  - ISPs won't be holding keys
  - What ISPs sell will be end-to-end encryption

    What the customer needs
    Experts will not carp
    ISPs can't afford the premiums!
- Part IV - tribunals etc

What ISPs do care about (a lot)

- Part I - Chapter I
  - Interception & interception warrants
  - Section 12 notices
  - Technical Advisory Board (TAB)
- Part I - Chapter II
  - “Communications data”
  - Section 22 notices

Interception (Chapter I)

- Everyone must co-operate, whether a public or a private system *5(1)(a)*
- Don’t have to do anything impractical *11(5)*
- SoS will say what is required of **public** systems using a Section 12 notice *12*
- Practical includes anything the SoS said *11(6)*
- SoS can pay, but is not required to *14*

Section 12 notices

- Formal consultation in progress
- Informal consultation with some ISPs
- Money on the table - for deserving cases
- There were threats to move offshore
- Not keeping machines in the UK may be a straightforward business decision
- In the long term, expect all to be encrypted

Technical Advisory Board

- Result of Government defeat in the Lords
- ? Six from LEAs and six from CSPs ?
- ? Independent chairman + expert panel ?

- Duty to advise on S12 order
- Main purpose is to hear appeals on notices served on CSPs under S12

Value for Money ?

- Police want email - but techies raise the stakes by looking for 100% solutions
- Pre-set requirements likely to involve pre-positioning of kit
- Cost is not just the kit but also the opportunity cost
- Interception of IP streams is best done in the Telco domain (usually known & fixed)

Communications Data (Chapter II)

- Day to day interactions with the police
- Real world addresses … `MrWobbly@thus.net` *21(4)(c)*
- Logs (and itemised bills) *21(4)(b)*
- The parts of the message (or an intercepted IP stream) that are not “content” , so called “traffic data”. Does not extend to a full URL *21(4)(a)*
- This is “traffic analysis” or COMINT and will be *de rigeur* in the encrypted future

Lessons from the telcos ?

- Itemised bills lead to nets of contacts
  - Customs & Excise 18834 subscriber details
    [Jan-Mar 2000] 549 itemised bills *2.9%*
    [Bassam, Lords debate] 57 special services
  - Metropolitan Police 63590 subscriber details
    [NCIS document] 4256 itemised bills *6.7%*
- Insisting on SPOCs
- Insisting on payment

Where are we now ?

- *Chapter I* Waiting for Code of Practice
- Section 12 Consulting
- TAB Consulting
- *Chapter II* Waiting for Consultation

Experience shows us that we shall need at least TWO rounds of consultation - unclear if we shall get this on any of these items.

Conclusion

- This is diverting attention from our business
- Still the prospect of significant expense

- Unclear that it will catch more criminals
  real advances are in police training
  and the methods they are using