RIPping into ISPs

Presented to: SFS2000

22nd March 2000

by Richard Clayton
Internet Expert
Thus plc

What ISPs don’t care about (much)

- Part II - informers, stakeouts and buggers
- Part III - seizing plaintext & encryption keys
  - We won’t be holding keys
  - What we sell will be end-to-end encryption
    What the customer needs
    Experts will not carp
    We can’t afford the premiums!
  - But, we want a proper “techie” defence in 50(8)

What ISPs do care about (a lot)

- Part I - Chapter I
  - Interception & interception warrants
  - Section 12 notices

- Part I - Chapter II
  - “Communications data”
  - Section 21 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 *13*

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` *20(4)(c)*
- Lists of calls that were made *20(4)(b)*
- Addresses - defined as anything attached to messages for the purposes of the system. So includes: MAIL FROM, RCPT TO, Received: IP Address, Port number, Protocol… *20(4)(a)*
- This is “traffic analysis” or COMINT and will be *de rigeur* in the encrypted future

Chapter II: Safeguards ?

- No central control of the scope *24(3)*
- No protection of seized data *n/a*
- No test of practicality *n/a*
- No public/private distinction *24*
- No payments guaranteed *23(1)*
- No standards for notices *22(1)(a)*
- Any crime or even just “disorder” *21(2)*

Where are we now ?

- *Chapter I*: Waiting for Regulations

  Experience shows us that we shall need at least TWO rounds of consultation

- *Chapter II*: Waiting for some common-sense

  Unfettered powers will lead to significant costs to ISPs and significant loss of privacy to users