RIP: its legal effects upon ISPs

Presented to: ISPA

20th October 2000

by Richard Clayton, Thus plc
IANAL!

Summary:

- Outline of the RIP Act
- Interception
- Communications Data
- What happens to 29(3) forms ?
- A brief word about the IUPF

Outline of the RIP Act

- Part 1 - Chapter I — Interception
- Part 1 - Chapter II — Comms Data
- Part II — Surveillance
- Part III — Encryption Keys
- Part IV — Oversight
- Part V — Miscellaneous
- Schedules — Lists

Warranted Interception

- Warrant signed by Secretary of State
- You must assist unless “not reasonably practical”
- You must keep it secret
- Serious penalties for not helping or letting information leak

Interception capability

- Section 12 allows SoS to create an order to ensure that interception is practical
- Notices may be served under this order
- Non compliance means civil action PLUS it changes definition of “reasonably practical”
- You can appeal a notice to the “Technical Advisory Board”

Money!

- SoS must ensure you get a “fair contribution” towards cost of complying with warrants and complying with a S12 notice
- £20 million is set aside over 3 years for S12

Echelon

- S8(4) warrant
- External communications only (a complicated concept)
- Expressed as data to be sought, rather than a person or premises
- Unlikely to be served on an ISP ?

Illegal interception

- Interception is defined as making some or all of a communication available to 3rd party without consent of sender and recipient
- Exception in 2(5)(a) for traffic data
- Exception in 3(3)(b) for an ISP if it relates to “provision or operation” of the service
- Need to review procedures for looking at customer email - even if they are “hackers”

Communications data

- “Big browser” was REMOVED
- Access only by police, customs, taxman and the intelligence services
- 22(3) authorisation - internal paperwork
- 22(4) notice - served on ISPs
- again a “reasonably practical” test
- and “appropriate contributions” to costs

Differences from 29(3) forms

- Obliged to comply
- Not given information about the crime
- Can require ongoing information (up to a month, though is renewable)

- Details in the Code of Practice (sometime)
- Not yet in force (first half of 2001)

Internet User Privacy Forum www.iupf.org.uk

- Producing a “Best Practice” document on user privacy
- Key recommendation is a “confidential relationship”
- You cannot honour 29(3) forms once this is in place, but RIP Chapter II will override

Summary

- Part I Chapter I already in force
- Interception warrants are needed for email
- Expect to see some this year
- Still no clarity on S12 notices
- Still no clarity on Chapter II activities
- Part III (encryption keys) is even further off