RIP: There’s someone at the door...

16th November 2000

by Richard Clayton

IANAL!
Summary

• Outline of the RIP Act
• Interception
• Communications Data
• S49 : putting into an intelligible form
• S51 : only a key will do
• S54 : tipping off
• Which key ?

16th November 2000

There’s someone at the door...
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

16th November 2000
There’s someone at the door...
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
- A “newsroom” issue rather than “personal”?  

16th November 2000

There’s someone at the door...
Echelon

- S8(4) warrant
- External communications only (which is rather a complicated concept)
- Expressed as data to be sought, rather than a person or premises
- Expected to be served on large telcos and “carrier carriers”
Illegal interception

• Interception is defined as making some or all of a communication available to 3rd party without consent of sender and recipient
• Doesn’t apply once delivered (whatever that may mean)
• Lawful business practices are lawful!
Communications data

- “Big browser” was REMOVED
- Access only by police, customs, taxman and the intelligence services
- 22(3) authorisation - internal paperwork
- 22(4) notice - no judicial input
- again a “reasonably practical” test
- can be served in private networks
Scope of a S49 (Pt III) notice

• S49 notice applies to material
  – that has been statutorily seized
  – that results from lawful intercepted
  – that was obtained as communications data
  – that was disclosed as a statutory duty
  – otherwise lawfully obtained by police etc

• "OR IS LIKELY TO DO SO"
S49 notice creation

- By a judge
- OR by a policeman, customs officer, intelligence officer etc etc
  basic idea… if they have the material lawfully then they can create the notice
- Gory details are in Schedule 2
S49 - tests to be applied

• There is a “key”
• Disclosure is “necessary”
  - national security
  - preventing or detecting crime
  - economic well-being of the UK
  OR exercise/performance of statutory duties
• Imposition of requirement is “proportionate”
• Not “reasonably practical” to obtain the information without serving a S49 notice
S49 - contents of notice

- In writing (or so as to create a record)
- Must describe the protected information
- Must say why notice is necessary
- Must say who issued it & their rank
- Must explain why it can be issued
- Must set a specific deadline
- Must set out what is wanted
S49 - special cases

• You cannot (usually) serve S49 notices on the office boy - need to find a director
  – applies when multiple holders of keys
  – added at late stage to calm down industry

• You cannot request a signature key
  – unfortunately signature keys do not always differ all that much from encryption keys at present (an issue with PGP)
It’s valid - what now?

• You’re entitled to use your “key”
  – you can then disclose the information in “an intelligible form” (ie give them the plaintext)
  – only applies if you have info and key

• OR you can hand over the key

• BUT if you don’t have the info…
  – you must hand over any key you have
S51 - only the key will do

• Must say so in the notice
• Must come from Chief Constable, Brigadier or Commissioners of Customs & Excise
• There must be special circumstances
• There must be consideration of the effects upon your business
• The oversight Commissioner must be told
S52 & S53 - upside/downside

• S52 - you might get paid for complying!
• S53 - you may get locked up
  – up to two years (and/or a fine)
  – if you “knowingly” fail to comply with notice
  – provided they can prove you had the key
    • NB: burden of proof is now the “right way”
  – and didn’t meet the timescale (or ASAP)
S54 - secrets

- If the police/customs/spooks wish to maintain effectiveness of an operation (or their general techniques)
- then they can require secrecy about the S49 notice (and things done in pursuance of it)
- Five years for “tipping off”
- Can tell your lawyer (if they’re honest!)
S54 - lies

• You can change your public key
  – read S54 carefully
  – read Hansard
• BUT you cannot (if S54 applies) say why

• BUT with current systems it may be unwise to rely upon people noticing
S49 - which key?

• You can hand over the plaintext. Code of Practice will cover whether they quibble!

• If you have several keys that would disclose the information then you can disclose any

• For messages (not storage) this means that you can disclose a session key if the description of the information permits
What’s a session key?

- Public key crypto is slow
- Hence a random bulk encryption key is used to encipher the text (IDEA, CAST, 3DES)
- The bulk key is then protected by the public key algorithm (RSA, Diffie-Hellman)
- Handing over the bulk key allows decryption of just one message
- Look for useful tools next year
There’s someone at the door...

- Is there a S49 notice?
- What does your lawyer say?
- Can you tell anyone else?
- Is the notice valid?
- Is it “necessary” and “proportionate”?
- Can you hand over plaintext?
- Can you hand over a session key?

16th November 2000
I want to warn someone...

• Is there a S54 provision?
• Is it valid?
• Is it reasonable?
• Are you obstructing the course of justice?

• Will changing your key actually work?
  Will people check?
I don’t want to comply...

- Saunders (ECHR) case suggests that forcing people to testify against themselves will result in a mistrial
- Human Rights Act may be applicable
- Journalistic material may be extra-protected
- I want to write a book about Brixton as seen from the inside
Conclusion

• Lots of powers, but lots of small print
• Code of Practice will not appear for a while
• Lots of promises in Parliament
• Special status of journalists may assist in Human Rights style challenges
• Technical fix will eventually be “plausible deniability” for storage & “perfect forward secrecy” for messages