Living with R.I.P.

by Charles H. Lindsey

chl@clw.cs.man.ac.uk

ex University of Manchester

Cambridge, 14 November 2000

Section 49 Notices

When can they be given?

1. *Protected Information* needs a key/password to 56(1)
   - *access* it, or
   - to *intelligiblize* it

2. They must have some *Protected Information* in their possession (or be likely to have it) 49(1)
   - By *Seizure*, e.g. under a Magistrate's Warrant (whole computer, floppies, tapes, smartcards, ...)
   - By Warranted *Interception*
   - By lawful (statutory) *request*
   - By falling off the back of a lorry

     (but only for the Police, etc.)

3. They must *reasonably believe* you have a key/password, **and**
   - they must be concerned over
     national security
     crime
     the economic well-being of the U.K.

     or hold some other statutory power
   - the damage to you must be *proportionate* to the benefit to them
   - they can't get the plaintext any other way

4. For a *corporate key*, the notice must be served on 49(5,6)
   - a director, manager, secretary, etc. of a company
   - a partner or most senior available person of a firm

   (assuming he has "right" to the key, & is not a suspect 56(2))

What must you do?

Normally, the Notice will ask for *plaintext*

1. Give them the *plaintext* (or *access* to the data)
   - in "*intelligible*" form
     which means the form it was in before encryption 56(3))
   - if the format is not intelligible enough, they need a P.A.C.E. warrant

2. If you can't
   - you must disclose anything you have which would help them
     e.g. a part key, tell them where key is hidden, or who has it, ...
     50(8,9)

3. If you won't
   i.e. you "knowingly" fail to comply
   - you can claim you no longer have the key 53(2)
     they have to prove that you had it (once)
     you just have to raise a "reasonable doubt" that you no longer have it
   - or you can claim they didn't give you enough time
   - otherwise: 2 years in jail for an individual
     a stiff fine for a company
     (but directors, etc. of company are immune 79(1))

4. The Secretary of State will reimburse your expenses
   ("if he thinks fit") 52(1)

Disclosure of Keys

When can they demand the <u>Key</u> (as opposed to plaintext)

There are extra Safeguards and Hoops: 51

1. The Notice must be expressly approved by Chief Officer of Police

2. It must not be a *signature-only* key 49(9)

3. There must be "*Special Circumstances*"
   - there is no other way to get what they want
   - the extra damage to you is *proportionate* to the benefit to them
   - taking into account other data protected by the same key
   - taking into account the effects on your business

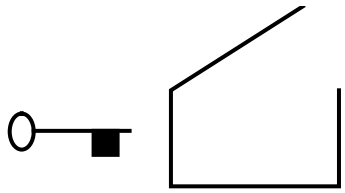
4. They must inform the Chief Surveillance Commissioner within 7 days

5. It is **your choice** which key to disclose (assuming there are several that would do the decryption). 50(5,6)
   Hence you would normally choose to disclose a *Session Key*.

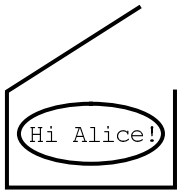
Session Keys

How Bob sends a message to Alice

Bob creates a brand new temporary conventional box with its own unique key

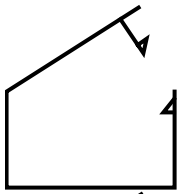


He puts the message in the temporary box

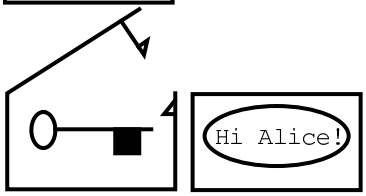


and locks it with his key

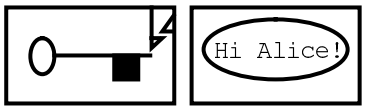
Then he obtains an Alice's Public Box



puts his key inside it

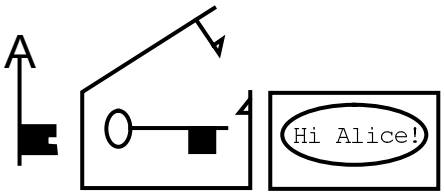


and locks it
(with a nice click)

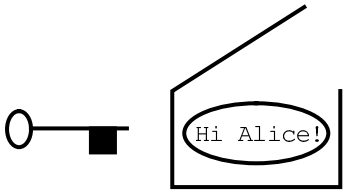


and sends the whole lot to Alice.

Alice opens the first box with her Private Key



and uses the key inside to unlock the second box



Thus revealing the message

What are the "*Special Circumstances*"?

1. They don't believe your plaintext
   - This will be by far the commonest "circumstance"
   - But this machinery is too heavy

2. They want it quickly
   - But if you insist on your right to disclose a Session Key, they won't get it any quicker than the plaintext

3. You don't (any longer) have the Protected Information, **and** they refuse to let you see it (perhaps it would breach some confidentiality, or disclose details of their investigation)
   - Alert! Lord Lucas's Lacuna
     All those Safeguards and Hoops no longer apply
     (well 49(9) and 50(5,6) still do)

4. Several keys are needed – you only have one (some), **and** they refuse to let you ask the other keyholders to help (because it might "tip them off")
   - All those Safeguards and Hoops no longer apply (ditto)

5. Anything else they can dream up
   - though Lord Bassam couldn't think of any other cases
   - there was a promise it would all be spelled out in the Code of Practice (but it hasn't been yet)

Tipping Off

1. You can be ordered not to tell anyone about the Notice [54]
   - but if you need to tell someone (your geek) in order to comply, then you can ask for him to be added to the list of Exceptions in the Notice
   - hence the importance of the notice being served at the highest level within the company

2. You can't tell your priest, or your psychiatrist, or your mother, but you can tell your lawyer or the Interception of Communications Commissioner

3. The penalty is 5 years (or a stiff fine for the company – directors are personally immune as before)

4. You <u>can</u> write software that broadcasts widely the fact that a key has been extracted from its storage space

5. You <u>can</u> publicly revoke a compromised key

6. You <u>can</u> give the game away by conspicuously keeping your mouth shut

Wise Precautions for Prudent businesses

1. Ensure you have no dual encryption/signature keys
   - i.e. all certificates should identify signature keys as ‘not for encryption’
   - many (most?) certificates issued by secure web sites do not meet this

2. For 1-to-1 communications, don’t use Public Key Cryptography
   - use Diffie-Hellman key exchange
   - snag: both parties need to be online at the same time
   - Public Key signatures are still needed to check the identity of the other party

3. For many-to-one communications (e.g. with your customers) Public Key Cryptography is appropriate,
   - ensure that your software can supply the Session Keys on demand
   - you will need to lean on your suppliers to get this capability

4. Ensure that all secret keys used by employees are *Company Property*
   - i.e. the highest levels of management must have the *right* to see them
   - this ensures that all Notices get served at the management level
   - (don’t be so foolish as to try to exercise that *right*)

5. Ensure all Web Browsers support the *Diffie-Hellman* SSL option
   - most don't

6. Ensure all Web Servers support the *Diffie-Hellman* SSL option
   - most do
   - but ensure they use this option as first preference whenever possible
   - this means you cannot be made to decrypt SSL sessions which Plod has intercepted, or to disclose the keys to same

7. Keep all important Company Keys in a *tamper-proof* iron box
   - "tamper proof" means it is *impossible* to get them out
   - always take data to be encrypted *to* the key, never the key to the data

8. Do not give backup keys to *Trusted Third Parties*
   - keep them within the company

9. Split backup keys into multiple parts, and store them in multiple jurisdictions
   - but be sure that the various keyholders have absolute discretion as to whether or not to disclose

10. If you have software that automatically discloses when keys are extracted from storage, ensure that it is *impossible* to override it

Code of Practice

Part III of the Act is not coming into effect for 1 year.
A Code of Practice will need to be published, discussed and agreed before then. The preliminary draft was a total shambles (as opposed to the draft code for Part I, which was actually quite good)

Things to watch out for

1. A fix to Lord Lucas's Lacuna, making all the safeguards and hoops apply in all cases

2. Explicitly recognised distinction between *session keys* and *multi-use* (e.g. public/private) keys

3. Codification of the "economic well-being" grounds

4. Proper interpretation of "proportionality"

5. Explicit procedures to deal with multiple holders of part-keys
   - allowing keyholders to cooperate to deliver plaintext
   - with tipping off requirements in exceptional cases only

6. Clear rules for identifying protected information in Notices
   - including obligation to supply it to the noticee (to avoid the lacuna)

7. The "Special Circumstances" to be spelled out explicitly

8. Time limit (e.g. 12 months) on how long ago a signature key might have previously been used for decryption

9. Clarification that revoking a key, and conspicuously remaining silent do not amount to “tipping off”

10. Prohibition of making copies of seized keys, or of taking them outside of secure storage managed by GTAC
    - i.e. the government too must practice *taking the data to the key*, rather than vice versa

11. Plug a loophole in Schedule 2

Lawful Business Practice Regulations

The Act makes *interception of communications* unlawful.
These Regulations make them lawful again for certain purposes within "businesses" 4(2).

When "interception" is not interception

1. Keeping logs of who emailed whom, or of websites accessed, or of telephone calls sent/received is not interception
   - because it is "traffic data" 2(5), 2(9)
   - but there may still be implications under the Data Protection Act

2. Interception by the sender or the recipient in person is not interception (because no 3rd party is involved 2(2))
   - so you can record your *own* telephone calls
   - BUT who is the recipient of a communication addressed to an individual within a company?

3. Automatic filtering (e.g. to avoid spam) is not interception
   - because no "person" gets to see the filtered material

4. Looking into someone's mailbox is not interception
   - because it is then no longer "in the course of its transmission"
   - cf. the "Doctrine of Lord Bassam's Doormat"

5. Interception by the *system administrator* in connection with the operation of the system is OK

Additional interception allowed by the Regulations

1. Monitoring (incl. recording) within a *private telecommunications system*
   - of transactions or other factual data
   - for quality control, training, compliance with regulatory practices
   - to prevent or detect crime or unauthorised use
   - to secure effective system operation

   provided
   - all users within the business are informed
   - but no need to inform outside callers

2. Monitoring (but **not** recording)
   - to determine whether communications are business or personal ones
   - communications to anonymous helplines

3. Does this allow employers to “snoop” on private email?
   - Yes, but only if the Company has promulgated a clear policy on the use of its equipment for private purposes
   - it may only monitor, not record or make use of data obtained

Snags

1. What, exactly, constitutes a “business”?

2. When is a message addressed to the Company?
   - in particular, when addressed to an individual but concerning company business

3. Can you automatically divert Mr Smith’s mail to Mr Jones, when Mr Smith is on holiday?
   - no
   - but this is not the same as letting Mr Jones look into Mr Smith’s mailbox

4. If a Private Telecommunication System incorporates features (lines, exchange capacity) hired from a Public Telecommunications Operator, is it still a Private System?
   - That is a Good Question