

Remarks on INVESTIGATION OF PROTECTED ELECTRONIC DATA

DRAFT CODE OF PRACTICE FOR PUBLIC CONSULTATION

Prepared by Dr C. H. Lindsey
(chl@clerew.man.ac.uk)

This latest draft is a considerable improvement on the draft issued in 2000. It is clear that you received much input from many sources (myself included) which has been taken on board. I am pleased to see that many of the matters I raised have been attended to, and that you have even adopted some of my suggested texts.

However, there are still a few matters which need attention.

Protected Information

3.5

Within the scope of section 49(1)(e) of the Act:

- acquired lawfully by any of the intelligence services¹, the police, Serious Organised Crime Agency (SOCA) or HM Revenue and Customs (HMRC) without using statutory powers, including information voluntarily disclosed to a public authority by a member of the public.

Actually, under 49(1)(e), that only applies to the bodies listed and not just to any “public authority”. So information voluntarily disclosed to a trading standards officer would not count. So change “a public authority” to “any of those bodies”.

Description of a key

3.10 The key to the data means any key, code, password, algorithm or other data the use of which, by itself or with another key or keys:

That definition is circular (“... key, ... means any key”) (and yes, the Act was just as bad). If it said “... means any (physical) key, ...” it would at least make some sense.

3.12 ... A key can comprise more complex material such as algorithms for either or both encryption and decryption of data, and take the form of computer code (in written, source or executable form) or a functional description of the algorithm or code.

I think that needs to exclude any code or algorithm which is publicly available.

Electronic signature keys

3.1 Where there are reasonable grounds to believe that a key used as an electronic signature has also been used for confidentiality purposes, that key may be required to be disclosed under the terms of the Act.

It has hitherto been a very common practice for a single key to be used for both signature and confidentiality (there being thus far no good reason not to do so). So there needs to be some time limit on how far back it had been used for electronic signatures (e.g. since the coming into force of this part of the Act, or within the preceding 12 months, or somesuch).

Session keys

3.18 A session key is an encryption and decryption key that can be randomly generated to ensure the security of a single item of data, for example a file or a communication. Session keys are sometimes called symmetric keys, because the same key is used for both encryption and decryption.

It should rather say "... that has been randomly generated ...".

And that last sentence is totally wrong, and should be deleted. Whilst it is true that a session key is *usually* symmetric, there is no fundamental necessity for this, and the two terms are mostly *not* synonymous. The important feature of a session key is that it protects just a single item of data (well, occasionally a small number of related items perhaps), and that is adequately stated in the first sentence.

Possession of a key

Your sections 3.21, 3.22 and 3.23 seek to ensure that notices are served at the highest possible level within a company. These rules will work fine for a straightforward company, but in practice companies tend not to be straightforward. They may operate on multiple sites, they may have partially or wholly owned subsidiaries and one or more parent companies, and it may be hard to tell which company a particular employee works for (he may not even be aware of such fine detail himself). And the company may be a big multinational. But there may well be a Big Managing Director right at the top who has the right to know everything (and hence the right to demand to be given any key within the whole organization, even though he may be unaware of their existence), and he may well be located outside of the UK.

Now your rules do allow some flexibility (and for sure that Big Managing Director is the wrong guy), but I feel that you need to review the wording so as to give more guidance in these situations, otherwise officers are going to try to serve notices at too high a level

Format of notices

Please add a subsection to the effect that a Notice should draw attention to the obligations, set out in Section 8 of the code, on the person to whom the disclosure it to be made, as regards handling any keys or plaintext that is disclosed.

Description of the protected information

4.17 ... The information can be described by reference to file names, usernames, dates and times or by any other identifiers of data, storage media, software or hardware. ...

I think email addresses need to be included in that list (so that a notice can specify all the emails received from a specified address within a specified timescale).

4.18 In some cases, it may be appropriate in order to identify or to confirm the identification of the protected data to include in, attach to or accompany the notice some or all of the protected information or a copy of some or all of it.

After “attach to or accompany”, add “(possibly in electronic form)”.

And after “accompany the notice” add “by” (to make it grammatical).

But I think that “may be appropriate” is too weak in some cases, and I would like to see something like:

Where the notice requires disclosure of a key, a sufficient part of the protected information *should* be provided to enable identification of all keys (including any session key) which would enable it to be decrypted.

4.19 ... – although a fuller description may be provided subsequently in the form of a schedule to the original notice.

That “may” should be “should”.

Authenticity of section 49 notices

4.25 In addition to the statutory requirements¹³ all written notices must include ... a published contact telephone number using which the recipient of a notice may check its authenticity.

The one thing which can be said with certainty about a bogus notice is that it will contain a bogus telephone number.

Amending a notice

This section also needs to cover withdrawal and cancellation of a notice (or else point to wherever else in the code these are covered).

RULES ON THE EFFECT OF IMPOSING DISCLOSURE REQUIREMENTS

5.1 The effect of giving a notice to a person ... is that he (or she):

I think you need to add:

- may be required to provide evidence that the decryption is correct.

It is probably better to give him a chance to do that before resorting to the ultimate sanction of requiring him to deliver a key.

Special circumstances requiring disclosure of a key

6.7 Although the special circumstances for giving direction to require the disclosure of a key will vary with each case as will the proportionality of doing so, such a requirement may be appropriate where:

No! That “may be appropriate” is far too weak. Ministers gave explicit promises on several occasions that the circumstances justifying disclosure of a key would be set out explicitly in the Code of Practice. Something like “such a requirement should not be made unless:” would accord better with those promises.

- the content of the intelligible information is an issue – where the person required to make the disclosure might find the intelligible form of the material offensive, obscene or otherwise distressing or it is important in the interests of justice that they do not view or be reminded of the material;

That goes well beyond what Lord Bassam said (Col 1057). Remove it. The person required to make the disclosure is best placed to decide whether loss of his key is a more onerous burden than being offended or distressed. If not, then he can choose to disclose the key voluntarily.

- the key itself has evidential value – where there is reasonable belief that the key may provide evidence linking a person or persons to an offence or offences, for example where a person seeks to deny responsibility for protected information in their possession but a password or pass-phrase for the key is personal to the person being served the notice or is indicative of the material it protects;

I find it hard to decipher the intended meaning of that sentence, but in any case it clearly goes well beyond what Lord Bassam said (Col 1057).

- practicality is an issue – where the key is divided into split-keys and it is not practicable or possible for the holders of the split-keys, or sufficient number of them, to act together to provide access to protected information or to disclose it in an intelligible form it may be necessary to require disclosure of one or more split-keys.

After “to act together” you need “within some reasonable time”. But then it just comes down to a matter of timeliness as discussed in section 4.23. But the people best able to judge whether the plaintext could be provided on the required timescale are the owners of the keys, and they should always be given the chance to do that before this ultimate sanction is imposed. Gathering the various split keys together will usually be what takes the time, and the

additional time to use them to decrypt the protected information may well be small in comparison.

Notices requiring disclosure of a key

6.9 Where a direction has been given that a notice can be complied with only by disclosure of a key, the notice must clearly state that the person on whom the notice is served may choose which key to disclose. ...

His attention should be explicitly drawn to this possibility and, in particular, to the possibility of disclosing a session key. Moreover, sections 4.17-4.19 still apply – even more so than in the usual case (see also my earlier remarks concerning 4.19).

6.10 Where a disclosure requirement is imposed on any person by a section 49 notice and:

- that person is not in possession of the information (either because they do not have the information, have not acquired the information or cannot be given possession);

Change “information” to “protected information”.

But I still do not understand the intent here. We are talking about notices requiring disclosure of a key, are we not? In which case this bullet (and the following one) are unnecessary. Or, if this section is intended to cover the case of a notice calling for disclosure in intelligible form, then the heading under which it appears is wrong, and in any case it should be appearing under section 5, rather than here under section 6.

- that person is incapable, without the use of a key that is not in his (or her) possession, of obtaining access to the information and of disclosing it in an intelligible form (or so disclosing it), or

If the key is not in his possession, then what is the point of serving a notice requiring him to disclose it?

6.14 The person given notice is able to comply with a requirement to disclose a key without disclosing all of the keys in his (or her) possession and where there are different keys, or combinations of keys, that would enable compliance with the notice, the person given notice may choose which key or combination of keys to disclose.

That is all well and good, but hasn't it been said already elsewhere?

Procedures for dealing with disclosed key material

- that the number of persons ... putting the protected information in an intelligible form;

Change “in an” to “into an”.

- that any disclosed key is stored, for as long as it is retained, in a secure manner. ...

It should also state that it should only be stored on some physically removable medium. Otherwise, it is likely to get copied onto backup tapes which are likely to hang around indefinitely. See also section 8.5 (even laptops get backed up onto tape).

8.7 Where keys or copies of keys are made available to a person other than the person to whom the key was disclosed a full audit trail must be maintained and be available for inspection by the appropriate Commissioner.

In fact it should go further than that by saying that, other than in truly exceptional circumstances, keys and copies thereof should *never* be given to another person. And it should state that the correct procedure, if further protected information is to be decrypted with the same key, is to give that information to the person holding the key, and to get him to decrypt it.

8.10 Under normal circumstances where protected information is put into an intelligible form using a disclosed key, and that intelligible information is used in evidence or is disclosed in criminal proceedings, copies of the key will similarly be required for evidential or disclosure purposes.

No, that is quite wrong. The most that will be required for evidential purposes is the session key (in cases where that exists). Normal practice should be for the person holding the key to testify. If counsel for the defence really want to check it for themselves (and assuming their client is the original owner of the key), then I suppose they should be given it. Otherwise, you get the actual original owner of the key to testify. The point is that in well designed cryptographic systems it is impossible to have two different keys that will decrypt the same protected information into two different meaningful plaintexts. Granted that a “one time pad” does not have this property, but then the evidential burden lies in proving that the alleged key is the one that was actually used to create the protected information, and that is going to be exceedingly difficult whatever the circumstances.

Procedures for dealing with disclosed intelligible material

8.12 Intelligible information which is disclosed in compliance with a notice should be handled with the same care and attention as other material that has been obtained by means of a statutory power to seize or otherwise require the production of documents or other property.

Given the space devoted to handling disclosed keys, that paragraph seems lamentably brief. There should be provisions for storing disclosed material similar to those for storing keys (e.g. it should be ensured that it never gets onto backup tapes); there should be proper audit trails; and so on.

Generally speaking, the intelligible form of the material is not more or less valuable than the session key which originally protected it (or of any key used to re-encrypt it whilst in possession of the authorities). Hence the provisions for dealing with disclosed information should be broadly comparable with the provisions for dealing with session keys.

APPROPRIATE PERMISSION FOR THE GIVING OF NOTICES

You have made a brave attempt to describe these rules which, given the complexities of Schedule 2 of the Act, is a virtually impossible task. I think what it now needs is a little more explanatory information to help the reader follow it correctly.

9.4 Public authorities may always seek appropriate permission for giving a section 49 notice from a judicial authority. ...

It would be useful to add that this is all subject to the constraints in 9.6–9.9.

Appropriate permission granted by a person holding judicial office

It might be better to rewrite this heading as “Constraints where permission is granted by a person holding judicial authority” perhaps with a remark that they (mostly) relate to situations where a related warrant has been issued.

Appropriate permission granted by an authorising officer

It might be useful to add “in connection with the Police Act 1997”.

Also, it is not clear why section 9.17 is here, since it does not appear to apply only when permission was granted by an “authorising officer” (e.g., as written, it could apply equally well when permission was granted by the Secretary of State).

Appropriate permission granted by a person exercising a statutory function

9.20 In these circumstances, if a section 49 notice is to require disclosure, such permission may be given in line with the general requirements relating to appropriate permission.

Please add an explicit reference to sections 9.22–9.24 here

9.21 Otherwise a person shall not have the appropriate permission unless he is the person:

But there is a big hole in the Code here (and admittedly it is a big hole in the Act).

If you are a member of the police, HM Forces, etc., then you have to be a Superintendent or a Lieutenant Colonel in order to give permission. But if you are a humble Trading Standards Officer and have a statutory duty to perform, then there is no such requirement – you can apparently give permission to yourself.

I would suggest, therefore, that the Code of Practice should close this hole, by requiring each public authority to designate some senior official for the purpose – rather like SOCA and HMRC are required to do in section 9.24.

General requirements relating to appropriate permission

Actually, those requirements are not as “general” as that heading implies. For example, they do not apply when permission is given by a Judge, or by the Secretary of State. The heading should be rewritten to make this clear (in fact, it only seems to apply when the Police Act or some statutory function is involved).

9.22 Paragraph 6 of Schedule 2 to the Act sets out general requirements relating to persons having appropriate permission in the police, SOCA, HMRC and who are members of HM Forces. ...

That should be “... *or* who are members of HM Forces”.

9.24 Where protected information has come into the possession of the police, SOCA, HMRC or a member of HM Forces, a person shall not have appropriate permission unless that person holds certain rank or designation:

Actually, as I read paragraph 6 of Schedule 2, these are the ranks of people who may *grant* permission to their subordinates (with the understanding that they may, in effect, permit themselves if they are going to issue the notice themselves). The wording, as written, does not cover that case.

- Police – superintendent or above;

I think “superintendent” should be capitalized – we don’t want Superintendents to think themselves less important than Lieutenant Colonels!

And, oddly, it seems that a Judge cannot give permission to an Inspector, whereas a Superintendent can.

Tipping off

10.10 Any public authorities other than those specified in section 54 may not include a secrecy requirement in their disclosure notices

Some examples of excluded bodies would be handy.

10.11 In imposing any secrecy requirement it is enough for any person giving consent for that requirement or giving a notice including such a requirement to have considered that there is a particular person from whom it is reasonable to withhold the information.

Is it not possible to issue a notice forbidding disclosure only to Person X? Section 10.19 seems to imply that it could be, in which case some clarification would help.

Authorised disclosure

10.18 It is not the intention of the Act to penalise individuals within organisations who, for example, have been given a notice imposing a disclosure requirement but need the assistance of another colleague in order to comply with the notice.

Please add that the notice should invite the noticee to seek permission (as in 10.19) in such a case.

Also, there needs to be a clear statement (as not being the “intention of the Act) in the following form:

A public declaration that a key has been revoked (with no reason given) does not constitute tipping off, neither does failure to perform some act that might otherwise have been performed.

Revocation of compromised keys is a perfectly normal procedure. If that gives some guilty party a clue that a notice may have been issued, then tough! That is the way it has to be.