FIPR Response to the Home Office:
"Consultation on the Revised Statutory Code for Acquisition and Disclosure of Communications Data – Chapter II of Part I of the Regulation of Investigatory Powers Act 2000"

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We welcome this belated consultation on the Code of Practice for Part I Chapter II of the Regulation of Investigatory Powers Act 2000. The current operation of this part of the Act without a Code of Practice, and – at least in 2004 – with the Interception Commissioner reporting in his annual report that he has insufficient resources to oversee it is scandalous.

We trust that this situation will not recur. We have noted the commitments by Simon Watkin at the "Scrambling for Safety" meeting on the 14th August 2006 that RIP Part III will not start to be operated without a Code of Practice being approved by Parliament beforehand, but, given the previous experience with Part I Chapter I as well, we would be more reassured by a ministerial statement to that effect.

We have a number of detailed comments upon the Code of Practice:

- In #1.3 we approve of the clear guidance that "legacy powers" should no longer be used by those who have been granted powers under RIP.

  However, we are very disappointed to discover that the Government has not taken this opportunity to coerce all Departments into using the RIP framework. The most notable absentee is the Department of Work and Pensions, but there are doubtless others. We cannot see why a single framework cannot be applied to all official requests for communications data and believe that should become explicit Government-wide policy.

- At s21(4)(c) the RIP Act sets out a category of communications data that is essentially defined by exclusion. It is data held or obtained "in relation to persons to whom he provides the service" by a communications service provider, but excluding the data defined in s22(a) and s22(b). This definition is extremely wide.

  Disappointingly, the Code of Practice does not seem to limit this scope, giving only examples of what it might include. However in the last bullet point of #2.25 there is a limitation in that a "password" is not to be included – except when national security is involved.

We are completely unable to understand this strange formulation and are unable to locate a statutory basis for this. Where the password permits access to undelivered messages we believe that a s8 warrant would be required, and where a delivered message is involved then a PACE warrant would be necessary. Whatever the Home Office has in mind here, it can only enhance the utility of the Code of Practice to go into considerable more detail.

- In s21(6) the RIP Act contains the "big browser" wording that was added to ensure that this part of the Act was not rejected by Parliament:

  > *"but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored."*

  In #2.19 the Code of Practice attempts to explain this as:

  > *"this means traffic data stops at the apparatus within which files or programmes are stored, so that traffic data may identify a server but not a website or page".*

  This cannot be exactly what the Act "means" since the words are different. It may perhaps be intended to restrict how the Act is to be interpreted – in which case it is far from adequate in doing so and will just lead to more confusion. All sorts of different architectures are used for servers and it would be far more useful to explain how the restriction applies to each – in particular, it is extremely common for many websites to be hosted on a single physical server. In practice, this means that to conform to the requirements of the Act, all web access logs at other sites would need to be processed to convert domains into IP addresses before being handed over. Equally, the web logs at the hosting site must be processed to remove all detail of what was accessed and only the remote client IP identification and a timestamp can remain.

  This need to perform significant filtering on this type of log may not be immediately apparent to all CSPs on whom s22 notices are served. Therefore, there should be a requirement placed upon the server of the notice to ensure that appropriate boilerplate text is included within the notice to warn the CSP of the limited information that may lawfully be sought, and the obligations of the CSP to do the work to avoid providing "too much".

  This boiler-plate could also usefully be used to caution the CSP about revealing more general forms of "content", email subject lines etc.

- The Code of Practice is entirely inadequate in its discussion (#3.18 *et seq*) of what types of specific conduct can be specified within an "authorisation".

  If law enforcement officers are to be permitted to trespass on private property, or make forcible entry then we assume that appropriate paperwork under RIP Part II will be essential. This should be made clear in the Code of Practice.

It would also be desirable, mainly for the benefit of the CSP, to discuss the relationship between an authorisation and the provisions of s10 of the Computer Misuse Act 1990. In passing, one notes that the amendments made by s162 of the Criminal Justice and Public Order Act 1994 are seldom applied to copies of the Act that are readily available by searching the web.

- The provisions for oral notices or authorisations (#3.48 *et seq*) appear to eschew the statutory provision to give such an item:

  "in a manner that produces a record of its having been given".

  Whilst appreciating that there is sometimes a need for rapid action, leaving detailed paperwork till later, once again we cannot see that the Code is capable of overriding the will of Parliament – because we cannot see that the outlined procedures will meet this requirement.

  We suggest that the Code should make far clearer that the oral process can only be permitted when recording equipment is being used, or other contemporaneous logs are being created – as is standard practice in operational control rooms anyway. We do not believe that having officials dredge their memories to create the paperwork the following day will meet the statutory requirement.

  We also strongly recommend that the Interception Commissioner should be formally advised (on an annual basis) by any statutory body that they wish to make use the oral process and it should otherwise be forbidden. We cannot see how any of the groups authorised by RIP outside of the traditional "emergency services" would ever have a need for this procedure, but if it is to be used the Interception Commissioner will be able to advise on the arrangements to be used to keep records and when the process is inspected, special steps can be taken to monitor compliance.

- We do not believe that the provisions relating to subject access rights in #7.3 *et seq* are fit for purpose.

  The onus is placed on CSPs to second guess law enforcement's needs and we predict that this will lead to different CSPs acting differently – so that data that should be revealed is not revealed and vice versa.

  It is open to the Secretary of State under s56(8) of the Data Protection Act 1998 to deal with records of subject access requests in a similar way to other police activity and we recommend that this should be done.

  Individuals should not look to receive data about s22 notices from the CSP in subject access requests at all (the DPA order would make that lawful) – but should seek that data from the law enforcement organisations instead – who will then release or suppress the information on the same basis as they currently treat other information they hold about individuals.

- The Code of Practice completely omits to require public authorities to create disciplinary procedures for dealing with deliberate "errors" in the creation of notices. These procedures should include taking steps towards criminal prosecutions in appropriate circumstances.

  Without this clear indication that misbehaviour by officials is intended to be punished, we do not believe that the Code of Practice addresses the considerable disquiet that this part of the Act continues to evoke, not least because of the considerable history of misuse of police powers to access communications data for personal reasons and to illegally assist "private investigators".

Turning now to minutiae:

- The drafting of #1.10 is poor. It is clearly intended to follow on from #1.9, but since many other paragraphs are stand-alone, this relationship is unclear with the current wording.

- The Act specifically talks of computer "programs". Spelling this (completely counter to current practice) as "programme" in #2.19 merely serves to confuse.

- In #2.25 we cannot see why the Home Office wishes to provide free publicity to ANY-Web Ltd (company number 3739786) the owners of the `anyisp.co.uk` domain. We do not consider this advertising to be appropriate within an official document of this type.

- In #3.5 the acronym "SPOC" is introduced with no indication of its meaning. It is probably meant to be a "single point of contact" which is first met in #3.9 and is thereafter called a "SPoC".

- In #3.33 the notice is required to specify a time period when it is to be more than ten days. However, in #3.32 the default period is to be ten days but is not to be included in the actual notice (so the CSP is aware of it) – the requirements in #3.29 merely saying that the notice is to contain a time period "where appropriate". There seems no value in making the presence of the time period within the notice to be anything other than mandatory.

FIPR
1st September 2006