[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

cc [REDACTION] for info & return
EB 19/05/04

Home Office

Legal Adviser's Branch

806, 50 Queen Anne's Gate, London SW1H 9AT
Switchboard 0870 0001585 Fax 0171 273 3629 Direct Line [REDACTION]
E-mail [REDACTION]@homeoffice.gsi.gov.uk www.homeoffice.gov.uk

Sir Swinton Thomas
Interception of Communications
Commissioner
C/o Room 1022 Queen Anne's Gate

Our Ref
Your Ref
Date 14th May 2004

Dear Sir Swinton
The database

1. The purpose of this letter is to inform you of a Security Service proposal and to seek your views on our analysis of the appropriate legal framework, in particular with regard to the ECHR.

2. Please find attached as an annex to this letter an explanation of the Security Service proposal, codenamed ***the database*** project.

3. The implementation and operation of ***the database*** project involves two distinct stages. The first is the transfer of the data by the communications service providers (CSPs) to ***the database***; the second is the retrieval of specified data from the database by the Security Service.

Transfer to database

4. We intend that the first stage should be achieved by the Secretary of State giving a direction to the relevant CSPs under section 94(2) of the Telecommunications Act 1984 c.12). The Secretary of State may make such a direction only if he believes it necessary in the interests of national security. Further, he must believe that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct. We believe that the requirements of necessity and proportionality are met (the reasons for this are set out in the annex - we would be happy to provide further information if that would be helpful). As permitted by section 94(4), we would not intend the direction to be laid before both Houses of Parliament on the basis that disclosure of the direction would be against the interests of national security.

[REDACTION]

EMBARGOED UNTIL 6 JUNE 13:00 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

5. We do not think that the transfer of the data engages either Article 1 of Protocol No.1 or Article 8 of the ECHR (or any other right guaranteed by the ECHR).

6. The Article 1 of Protocol No.1 issue might be thought to arise because the effect of the direction will be to require the transfer of data belonging to the CSPs (Article 1 of Protocol No.1 expressly protects legal persons as well as natural persons). However, it is questionable whether the ownership of data constitutes a property right such as falls within the scope of Article 1 of Protocol No.1. Even if it does, we would argue that the section 94 direction does not interfere with the CSPs' right to peaceful enjoyment of the data - the direction only requires them to make a copy of the data, rather than handing it over, and the exercise will be cost-neutral for them - and therefore Article 1of Protocol No.1 is not engaged.

7. Nor do we think that Article 8 is engaged by the transfer of data to ***the database*** and its storage there. Although the transfer and storage of data may in principle engage Article 8 (even if it is not accessed), the data in question must be personal data. In the case of ***the database***, the data will not include any information which on its own would enable a link to a particular individual to be established.

Retrieval of information from the database

8. The second stage [REDACTION] involves retrieval by the Security Service of specified data from the database. In some cases (depending on the information that it already holds or is able to obtain), the Security Service will at this point be able to link the data to a particular individual. Accordingly, we think that this is the first point at which the Service's conduct engages Article 8. In order to ensure that there is no infringement of Article 8, retrieval of the data from the database must meet the requirements of necessity, proportionality and being in accordance with the law.

9. In the case of *Malone v the United Kingdom* (1984) 7 EHRR 14, the European Court of Human Rights considered whether the practice of "metering" whereby the Post Office registered numbers dialled on a particular telephone line and the time and duration of each call could give rise to an infringement of Article 8. The information gathered through "metering" will be included amongst the information which will be held on ***the database*** (see annex). The Court held that the release of information to the police without the consent of the subscriber amounted to an interference with Article 8 (see paragraph 84 of the judgment). Presumably, this was because, once in the hands of the police, the information could be linked to particular individuals and thus became personal information.

10. We intend that the Security Service should apply Chapter II of Part I of the Regulation of Investigatory Powers 2000 (c.23) (RIPA) when accessing the data held on ***the database***, just as it would if it were accessing communications data in the possession of a CSP. Thus a designated person within the Security Service will grant an authorisation under section 22(3) of RIPA to other people within the

EMBARGOED UNTIL 6 JUNE 1600 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

organisation to access the data if he believes that it is necessary on one of the grounds set out at section 22(2)(a) to (c) and he believes that accessing the data is proportionate to what is sought to be achieved. The authorisation will have to comply with section 23.

11. Section 22(3) provides that the authorisation is "to engage in any conduct to which this Chapter applies". Conduct to which the Chapter applies is defined in section 21 (1). Section 21 (1)(a) seems the relevant limb since the authorisation granted under section 22(3) will authorise the person in question to obtain data from ***the database*** (rather than authorising him to disclose it which would be covered by section 21(1)(b). It might be thought that it is somewhat awkward to fit the second stage [REDACTION] within section 21(1)(a) because the data is already owned by the Security Service but, subject to your views, we think it works (we explain below why we think it necessary to fit the second stage [REDACTION] within Chapter II). The two potential problems are as follows. Firstly, section 21(1)(a) applies to the obtaining of communications data., and it might be argued that the data held in ***the database*** is not being obtained because it is already in the possession of the Security Service. We think this is an unduly technical argument. Given that the data will be stored [REDACTION] and only accessed when it is needed, it seems natural to describe this as "obtaining" data. The second potential problem is that the conduct must be in relation to a telecommunication system. A telecommunication system is defined at section 2(1) of RIPA. It might be argued that the conduct involved in the second stage [REDACTION] is simply conduct for obtaining communications data, and the conduct has no relationship to the original telecommunication system. But, taken to its logical extreme, the same argument might apply to communications data held on a database owned by a CSP. We think a wide view must be taken of "in relation to" such that conduct in relation to something which derives from a telecommunication system for obtaining communications data is covered by section 21(1)(a).

12. The reason why we are concerned that the second stage [REDACTION] should be governed by Chapter II is that we think it necessary for Article 8 purposes. As explained above, accessing the data will amount to a prima facie infringement of Article 8. Although the Security Service could ensure that any individual decision to access was only taken if it was necessary and proportionate to do so, if Chapter II did not apply, we find it difficult to see how the "in accordance with the law" requirement would be met.

GCHQ

13. We understand that at your last warrantry review with GCHQ the ways in which GCHQ acquires its communications data were explained to you, including the fact that GCHQ does not rely on Chapter II of Part I of RIPA for accessing data acquired under a section 94 direction. This is clearly an approach that is different from that described above. However, we do not think that the two approaches are necessarily incompatible, principally because of the way in which GCHQ's present system and that which is proposed for ***the database*** differ.

[REDACTION]

EMBARGOED UNTIL 9 JUNE 2000 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

14. Most communications data obtained by GCHQ is held in a single database. The majority of this data (approximately 90%) is acquired under the authority of "section 8(4)" interception warrants issued to GCHQ. The remaining 10% of data held in this database is acquired under a section 94 direction. The database does not differentiate between, or in any way flag up, the origins of the data with the result that anyone accessing the data will be unaware of the legal authority under which it has been obtained. To reconfigure the database to allow for such differentiation is not an option because of the technical difficulties and expense that this would entail.

15. However, the long term goal is for a database to be constructed which would allow data obtained under a section 94 direction to be accessed using Chapter II of Part I of RIPA (although the nature of the authorisations will not necessarily be identical to those used for *the database*).

16. A copy of this letter goes to [REDACTION] (Home Office) [REDACTION] (Security Service) and [REDACTION] (GCHQ).

Yours sincerely,
[REDACTION]

[REDACTION]
Home Office Legal Adviser's Branch

EMBARGOED UNTIL 6 JUNE 13:00 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

ANNEX

The database is a project that would give the Security Service an enhanced capability to acquire and analyse communications data and to act on intelligence derived from that data.

Analysis of communications data is a vital investigative technique for the Security Service, particularly in its work to protect national security from the threat posed by international terrorism. **The majority of targets of Security Service investigations use phones**, and the Service acquires communications data from CSPs under Chapter II of Part I of RIPA.

Communications data can provide crucial intelligence about the behaviour and associations of targets [REDACTION]. This data is used to great success but the Security Service is constrained by the resources with which CSPs have to respond to disclosure requirements.

[REDACTION]

Under **the database project**, CSPs would transfer to a Security Service database [REDACTION] **traffic data and service use information** [REDACTION]. The data transferred would always be data already held by the CSPs for, for example, billing purposes and would always be anonymous. The data would be transferred **on a regular basis**. The Security Service would retain the data for six months. Initially **the database project** would involve only selected CSPs although the concept could be expanded [REDACTION].

The database would provide a database of communications data to which the Security Service would have direct access [REDACTION].

Technical safeguards would ensure that data could be retrieved from ***in the database*** only in response to a lawful RIPA authorisation for disclosure meeting the criteria of a specific search. [REDACTION] The vast majority of data held ***in the database*** would never fall within the parameters of a search and never be drawn from the database or viewed by an analyst. To the extent that data was drawn from the database, in many instances it would never be linked to an identified individual. Where a link were made to an identified individual, this would be done using information already held by the Service or subsequently obtained by the Service, for example, by obtaining subscriber information from a CSP using a Notice under RIPA.

EMBARGOED UNTIL 6 JUNE 1600 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

Copies to DO
16/08/04
[REDACTION]

copied to [REDACTION] on
23/6/04
[REDACTION]
noted
[REDACTION]

cc [REDACTION]

From the Interception of Communications Commissioner:
The Rt. Hon. Sir Swinton Thomas
c/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

[REDACTION]
Home Office
Legal Adviser's Branch
Room 806
50 Queen Anne's Gate
London SW1H 9AT

Our ref: IPS/04 I/1/1

Date: 8 June 2004

Dear [REDACTION],

The database

Thank you for your letter of the 14th May. ***The database*** scheme raises interesting and quite difficult issues. However, I am confident that if there are any problems, they can be overcome.

My reservations relate to the first stage, the transfer to the database. It is proposed that the Secretary of State should give a direction to the CSPs under Section 94(2) of the Telecommunications Act 1984. So far, so good. But I think that since the coming into force of Chapter II of Part I of RIPA this legislation is engaged in such a direction when, as here, communications data are being acquired. It is said that in giving a direction under Section 94(2) the Secretary of State must be satisfied that what is sought to be achieved is proportionate. I am not clear as to where this comes from. It is certainly not in Section 94(2) itself. It may be simply that this is now regarded as a general underlying legal requirement of the acquisition of communications data since the coming into force of Chapter II. If so I am doubtful if that argument would succeed if it was challenged, unless the requirements of Chapter II are also complied with. I do not doubt that the requirements of necessity and proportionality are in fact complied with.

I would hesitate to express an opinion as to whether the ownership of data constitutes a property right. I do not think that this matters. It should be noted that the body of Article 1 of Protocol Number 1 refers to "the peaceful enjoyment of his possessions".

[REDACTION]

EMBARGOED UNTIL 6 JUNE 1300 BST

{NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD. DOUBLE-UNDERLINED AND ITALICS}

[REDACTION]

I agree that it is doubtful whether the proposed Section 94 direction interferes with the CSPs' right of peaceful enjoyment. In any event, providing the legal requirements of the legislation are complied with the reservations in the Protocol:

(a) No-one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law .....
(b) The preceding provision shall not, however, in any way impair the right of the State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest .....

provide ample protection to the Agencies and the CSPs.

I agree that Article 8 is not engaged in the transfer of data to ***the database*** for the reasons set out in your letter.

The problem which troubles me at the moment is that it seems to me that if Section 21 of Chapter II is engaged in the transfer to the database, then its provisions must be followed and the various requirements of Chapter II complied with. If this is right, and I am happy to be persuaded that it is not, this should not cause any great difficulty, although I accept that it is rather cumbersome when allied to the subsequent retrieval of the data from the database.

Retrieval of information *from the database*

I agree that Article 8 is now engaged and so must meet the requirements of necessity, proportionality, and being in accordance with the law. However clearly that can readily be achieved. I also agree that the appropriate way to achieve this is by the service of a Section 22(3) authorisation. Although it may, as I have said above, appear to be cumbersome and rather strange to go through the same, or at least a similar exercise twice, there is a logic about it, because the first stage is an acquisition of communications data obtained by notice, and the second is a disclosure obtained by an authorisation. I agree with what you say in the second half of paragraph 11 of your letter that, although at first sight it may be awkward to fit the second stage into Section 21(1)(a) it is in fact logical to do so, and is certainly necessary to fulfil the spirit of the legislation.

GCHQ

I have no difficulty with the data obtained and disclosed under a "Section 8(4) authority". However, I think that in relation to the remaining 10% the same problem may arise as that outlined above.

I will, of course, as always, be happy to discuss these issues with you and others if you wish to do so.

Yours sincerely,
Swinton Thomas

Sir Swinton Thomas

[REDACTION]

EMBARGOED UNTIL 13:00 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

Copied to [REDACTION]
on 5/8/04

[REDACTION]

copied to DO
16/08/04
[REDACTION]

Noted
[REDACTION]
306/04

EMBARGOED UNTIL 6 JUNE 13:00 BST

Home Office

Legal Adviser's Branch

806, 50 Queen Anne's Gate, London SW1H 9AT
Switchboard 0870 0001585 Fax 0171 273 3629 Direct Line [REDACTION]
E-mail [REDACTION]@homeoffice.gsi.gov.uk www.homeoffice.gov.uk

The Rt. Hon. Sir Swinton Thomas
Interception of Communications
Commissioner
C/o Room 1022
50 Queen Anne's Gate
London
SW1h 9AT

Our Ref
Your Ref
Date 22nd June 2004

Dear Sir Swinton

The database

1. Thank you very much for your letter of 8th June. This letter relates to the reservations that you have about the first stage [REDACTION] namely the transfer to the database

2. You say that if section 21 of Chapter II is engaged in the transfer to the database, then its provisions must be followed and the various requirements of Chapter II complied with. Although we agree that Chapter II could be used in relation to the transfer to the database, we do not think that that means it must be used. The purpose of Chapter II is to make lawful the acquisition and disclosure of communications data which would otherwise be unlawful. But if a direction had been made under section 94 of the Telecommunications Act 1984 (the 1984 Act), the acquisition of the [REDACTION] data would already be lawful (to the extent necessary to deal with any Article 1 of Protocol No.1 ECHR issue) and there would therefore be no need to use Chapter II[1]. In our view, the transfer to the database could be made lawful either by the issue of notices under Chapter II or by a direction under section 94 of the 1984 Act.

[1] You question where the requirement for proportionality in section 94 of the 1984 Act comes from. The answer is section 94(2A) which was inserted into the 1984 Act by paragraph 70(4) of Schedule 17 to the Communications Act 2003 (c.21).

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

The only practical difference between the two sets of provisions is that, if Chapter II were used, a new notice would need to be issued every month in accordance with the renewal provisions of section 23, involving a fresh consideration of the necessity and proportionality issues. This would not be the case under section 94. However, if the section 94 route were used, the Security Service would undertake regularly to review the necessity and proportionality of the direction with a view to cancelling it if these tests were no longer met.

3. It seems to us that the issue of whether to use Chapter II or a section 94 direction is essentially a matter of policy/presentation. In favour of using a section 94 direction are the following two factors.

4. Firstly, under section 94, the direction would be given by the Home Secretary. Under Chapter II, the notice could be issued at a fairly low level (in accordance with the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172)). Even if the notice were in practice issued at a much higher level, it would always be issued by an official rather than a politician (even if its issue were in fact approved by a politician). Arguably, a decision of this significance ought to be taken by a politician who is directly accountable to Parliament, rather than by an official.

5. Secondly, although there is nothing to stop Chapter II being used for transfers of data of the type envisaged by ***the database***, it has not in practice been used in this way to date. If the Security Service could use Chapter II in this way, then in principle so could all the other public authorities that have access to communications data if they could comply with the necessity and proportionality tests. We understand that some communications service providers are concerned that law enforcement authorities might try to set up their own version of ***the database***. Their perception is that, if Chapter II were used for ***the database***, it would make it more likely that law enforcement authorities would attempt to do something similar using their powers under Chapter II.

6. We would be happy to discuss these issues with you if you think that would be helpful.

7. A copy of this letter goes to [REDACTION] (Home Office), [REDACTION] (Security Service) and [REDACTION] (GCHQ).

Yours sincerely,
[REDACTION]

[REDACTION]
Home Office Legal Adviser's Branch

[REDACTION]

EMBARGOED UNTIL 13:00 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

Interception of Communications Commissioner
The Rt Hon. Sir Swinton Thomas
C/O Room 1022
50 Queen Anne's Gate
London
SW1H 9AT
Telephone: [REDACTION]

[REDACTION]
Home Office Legal Adviser's Branch
Room 806
50 Queen Anne's Gate
London
SW1H 9AT

Date: 6th July 2004

Dear [REDACTION],

Thank you for your letter of the 22nd June. In particular, thank you for drawing my attention to Paragraph 70(4) of Schedule 17 of the Communications Act 2003. One of the problems of working in the outposts of the Empire is that one tends not to be informed of changes in the law, and has to rely on bumping into them by chance- as here!

On the issue of transferring data to the database this raises an interesting but, in the end, perhaps not over-important point. I agree that the provisions of both the Telecommunications Act 1984, and Chapter II of Part I of RIPA 2000, make the acquisition of communications data lawful. The question that arises is whether on the enactment of Chapter II, it became mandatory to follow the procedures set out in Chapter II in all cases of acquisition of data under any enactment, or whether the procedure applied only to data acquired pursuant to RIPA. When I wrote to you on the 8th June I was inclined to the former view, but on re-consideration and in the light of your letter, I have revised that view, and can see that there is a strong case for arguing that the procedure should only apply in Chapter II cases. I am also impressed by the considerable and, if possible to be avoided, inconvenience in following the Chapter II procedure in ***the database*** proposals.

In these circumstances, I am content that you should proceed in the way that is suggested. I have assumed that this is in line with the views of the appropriate advisers within the Agencies concerned.

Yours sincerely,
Swinton Thomas

Sir Swinton Thomas

[REDACTION]

EMBARGOED UNTIL 6 JUNE 0800 BST

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

From the Interception of Communications Commissioner:
The Rt. Hon. Sir Swinton Thomas
C/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

[REDACTION]
Home Office
Legal Adviser's Branch
Room 806
50 Queen Anne's Gate
London, SW1H 9AT

July 2004

Dear [REDACTION]

The Database

This letter follows my letter of 6th July 2004.

When I visited the Security Service on 6th July, I was told that there is a suggestion being floated that bulk transfers of communications data might be obtained by Law Enforcement Agencies by means of a RIPA Notice only without the intervention of Section 94 of the Telecommunications Act, 1984.

Needless to say I have no settled view about this at the moment, but I think that I would be concerned about this being done without Ministerial intervention, and if there is any fixed proposal to this effect, I would be grateful if I could be consulted about it.

Yours sincerely,
Swinton Thomas

Swinton Thomas

[REDACTION]

EMBARGOED UNTIL 6 JUNE 13:00 BST

[redacted]

GCHQ
Hubble Road
Cheltenham
GL51 0EX

[redacted]
Title LA2

Tel: 01242 221491 Ext: [redacted]
Brent: 01242 540088
Fax: 01242 709053
GTN: 1366 Ext: [redacted]
E-mail:

Sir Swinton Thomas
Interception Commissioner
Home Office
50 Queen Anne's Gate
London SW1H 9AT

GCHQ Reference: LA2/0534/6/3/19
Your Reference:

Date: 18TH October 2004

Dear Sir Swinton,

COMMUNICATIONS DATA – ACQUISITION AND DISCLOSURE

1. Following your visit to GCHQ in July 2004 and our discussion in London on 14th October 2004, this letter discusses the GCHQ procedures for handling communications data and seeks to confirm your view of their fitness for purpose.

2. Communications data is an increasingly important tool in GCHQ, especially in the fight against global terrorism and serious crime. About 250 staff are involved in its analysis and about 40% of End Product Reports are derived directly or indirectly from the analysis of communications data.

3. The communications data is stored in GCHQ databases. Huge volumes of data are acquired (about 40 million bits of data per day). There are two databases at GCHQ holding communications data acquired in 'bulk' – known as [redacted] Ideally all the material would be held on a single database, but the data is configured differently by the CSPs and resource constraints in GCHQ have meant that it is not feasible, at this point in time, to re-configure and hold all the data in a single database.

4. The [redacted] database holds computer-to-computer [redacted] communications data all of which originates from sources authorised by the RIPA 8(4) warrants. The [redacted] database contains communications data relating to telephony. About 90% of the data stored on the [redacted] database originates from sources authorised by the RIPA 8(4) external warrants and about 10% from section 94 directions.

5. The data held on the [redacted] database is not separated by reference to the legal instrument under which it was obtained for the following reasons:

- To date, GCHQ has relied on legal advice previously tendered (coupled with the requirements of the process described at para 9 below) that such separation, in legal terms, is unnecessary;

EMBARGOED UNTIL 0 JUNE 13:00 BST

POSITIVE ABOUT DISABLED PEOPLE

[redacted]

INVESTOR IN PEOPLE

[redacted]

- In the interests of security and commercial confidentiality, GCHQ prefers to keep all the telephony material together in one database (rather than separate it) to disguise its source, as the origins of some of the material is extremely sensitive;

- The combining of all telephony-related communications data in a single database makes analysis of such data much quicker and more reliable; this is particularly so with pattern analysis which relies on exploiting large quantities of data.

6. The origin of the material is not consistently flagged, so an analyst cannot tell whether a particular bit of communications data originates from a warrant or a direction.

7. Communications data is currently retained for [redacted].

8. The mechanics of facilitating access by GCHQ staff to communications data obtained by GCHQ in reliance on either its RIPA section 8(4) warrant or the section 94 directions issued to it are the same and were demonstrated to you on your recent visit to Cheltenham but, for ease of reference, are reproduced below:

9. The databases are searchable. To access the communications data databases the analyst is required to log on and an audit log is automatically created. The log records who accessed the database, the date, time on and time off. It also records the JIC requirement underpinning the request (national security, EWB and/or serious crime), a [redacted] number (which is a GCHQ system providing a higher level of granularity taken from the JIC R&P) and a specific justification. We consider that the provision of this information is sufficient to protect an individual's Article 8 rights (in that information may not be accessed unless it is for a proper purpose), and to ensure that GCHQ can respond appropriately should an individual complain to the Investigatory Powers Tribunal.

Legal analysis:

10. Communications data may be acquired under a number of different legal instruments:

- Section 8(4), or section 8(1) RIPA warrants. Section 5(6)(b) of RIPA provides that an interception warrant may authorise the obtaining of related communications data;

- Section 94 directions under the Telecommunications Act 1984 (as amended by the Communications Act 2003);

- Notices or authorisations given under sections 21 to 25 RIPA (Part 1, Chapter II).

EMBARGOED UNTIL 0 JUNE 13:00 BST

POSITIVE ABOUT DISABLED PEOPLE

[redacted]

INVESTOR IN PEOPLE

[redacted]

(It is also the case that occasionally, e.g. immediately post 9/11, communications service providers voluntarily provide communications data to GCHQ for analysis.)

11. It has always been GCHQ's position that each of the three methods of acquisition listed above is equally valid in law and GCHQ presently relies upon all three types of legal instrument when acquiring communications data. This being so, we welcome the views that you express in your letter to [redacted] dated 6 July 2004.

12. We would contend (and from what you have said in your correspondence with [redacted] we believe that you concur) that the transfer of data to our databases pursuant to section 94 directions is in accordance with the law provided that the Secretary for State responsible for signing such directions is able to properly consider necessity and proportionality issues.

13. Turning now to the legal position relating to accessing the data obtained under the directions, GCHQ does not presently adopt the RIPA Part I Chapter II authorisation process to access data on its [redacted] databases. Hitherto, we have taken the view that s.94 (when coupled with the access procedures described in para 9 above) has operated in such a way so as to make the accessing of any data held on the database in accordance with the law. We are aware that you have previously expressed some reservations about this interpretation of the effect of s.94, and this brings us to the crux of this letter. Whilst we accept that it is *arguable* that s.94 is insufficiently precise so as to make the access of any data obtained pursuant to any directions issued under that section not in accordance with the law, GCHQ would favour the interpretation that it presently relies on, i.e. that s.94 operates to the effect that access to the data obtained under any direction is in accordance with the law (particularly when taken in conjunction with our current access procedures).

14. There are very real practical difficulties in GCHQ being required to obtain a RIPA Part I Chapter II authorisation in respect of accessing any data that it had obtained in reliance on section 94 directions. This is because it is not possible to identify which of the small percentage of the total communications data held on the [redacted] database has been acquired under section 94 directions. This being the case, if an authorisation was required to access any data held on [redacted] that was obtained pursuant to s.94 directions it would be necessary to obtain an authorisation in each and every case that communications data was accessed on this database – even if the data had been obtained in reliance on a RIPA section 8(4) warrant. At present, our staff make about 2,000 queries of the [redacted] database each week. In a proportion of these cases, the analyst will not have any information about the identity of the entity and may be undertaking target profiling work looking for calling patterns that are associated with known terrorist behaviour rather than a particular entity.

EMBARGOED UNTIL 0001 13 DEC RST

POSITIVE ABOUT DISABLED PEOPLE

INVESTOR IN PEOPLE

[redacted]

15. However, taking into account the fact that the Secretary of State would have made a judgement as to necessity and proportionality when issuing the directions authorising the acquisition of the data, we believe that the requirements that have to be fulfilled by GCHQ staff when communications data is accessed by them on the [redacted] database are such that the spirit of RIPA (insofar as the tests of justification, necessity and proportionality are met) is fully adhered to. In addition, an unintended consequence of requiring the RIPA process would be to create an inconsistency between the authorisation regime for communications data and that required for intercept selected under a RIPA 8(4) warrant. A higher level of protection would be provided for communications data than for such selected material. This seems odd given that taking action on communications data is agreed to be intrinsically less intrusive into privacy.

16. Given the contents of your 6 July letter to [redacted] and the comments you made when you last visited Cheltenham (when, if we understood you correctly, you seemed to suggest that adherence to the spirit of the legislation was an important factor when considering whether the necessary legal requirements for accessing the data held on the [redacted] database had been met), and those you made when we met in London on the 14th, are you content with the processes currently adopted by GCHQ for its staff to access communications data held on its [redacted] database and that such access is in accordance with the law? If you are not content with our current interpretation of s.94 and our practices/processes, then we would welcome the opportunity to discuss this with you further.

Yours sincerely,

[redacted]

pp. [redacted]
Legal Adviser

CC: [redacted]

EMBARGOED UNTIL 6 JUNE 13:00 BST

POSITIVE ABOUT DISABLED PEOPLE

[redacted]

INVESTOR IN PEOPLE

[redacted]

From the Interception of Communications Commissioner:
The Rt. Hon. Sir Swinton Thomas
c/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

[redacted]

Legal Adviser LA2
GCHQ
Hubble Road
Cheltenham
GL51 0EX

Your ref: LA2/0534/6/3/19

Our ref: IPS/04 1/1/1

Date: 17 November 2004

Dear [redacted]

COMMUNICATIONS DATA – ACQUISITION AND DISCLOSURE

Thank you for your letter of 18th October. I do not think that the problem of accessing communications data pursuant to a Section 94 direction is altogether easy or straightforward, and I have given it considerable thought.

When the Secretary of State makes a direction under Section 94(2) of the Telecommunications Act 1984 he must be satisfied that the requirements of necessity and proportionality are satisfied in relation to the acquisition of the data. When the data is accessed then, as is recognised, an individual's Article 8 rights are engaged. Whilst it is properly arguable that the Secretary of State impliedly authorises the accessing of the data when he gives the Section 94 direction, it would be very difficult to argue that he has considered the issues of necessity and proportionality in relation to the particular individual whose data is being retrieved. Thus, GCHQ must be able to show that the individual's rights are properly protected in that the data is being retrieved for a proper purpose and is proportionate and that the decision to retrieve it has been taken at an appropriate level. You tell me that these requirements are covered by the JIC requirement underpinning the request coupled with the record kept of the nature of the requirement in relation to each retrieval. I note that GCHQ takes the view that these safeguards would ensure that they could satisfy the Investigatory Powers Tribunal in the event of a complaint.

I have, therefore, reached the conclusion, not without some difficulty, that the present system for retrieval of data pursuant to a Section 94 direction is lawful. As you say, adhering to the spirit of the legislation is an important consideration, and I am also impressed by the fact that when armed with a Section 94 direction which clearly envisages both acquisition and retrieval, the requirement of a RIPA Section 22(3) authorisation would cause real difficulties which could not have been

[redacted]

EMBARGOED UNTIL 6 JUNE 15:00 BST

envisaged by Parliament when RIPA was enacted. I am, therefore, content that you should proceed as proposed.

Yours sincerely,

Swinton Thomas.

Sir Swinton Thomas

EMBARGOED UNTIL 6 JUNE 13:00 BST

[redacted]

GCHQ
Hubble Road
Cheltenham
GL51 0EX

[redacted]
Title LA2

Tel: 01242 221491 Ext: [redacted]
Brent: 01242 540958
Fax: 01242 709053
GTN: 1366 Ext: [redacted]
E-mail:

The Rt Hon Sir Swinton Thomas
Interception Commissioner
c/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

GCHQ Reference: LA2/0655/6/3/19
Your Reference: IPS/04 1/1/1

Date: 2nd December 2004

Dear Sir Swinton,

Re: Communications Data – Acquisition and Disclosure

Thank you for your letter of 17th November 2004. GCHQ very much welcomes the conclusion that you express in this letter.

For the sake of completeness I thought it appropriate to comment on part of your letter. You say,

"Whilst it is properly arguable that the Secretary of State impliedly authorises the accessing of data when he gives the Section 94 direction, it would be very difficult to argue that he has considered the issues of necessity and proportionality in relation to the particular individual where data is being retrieved".

Of course, whilst no particular individual whose data may be accessed is identified either in the Section 94 directions themselves or in the accompanying submission, the submission does itself contain a clear statement as to the manner in which any data obtained under the directions will be handled. The relevant extract from one of the submissions is as follows,

"Within GCHQ data will be handled in accordance with section 4 of the Intelligence Services Act 1994, and with additional safeguards designed to comply with the Human Rights Act 1998. These safeguards were included in the GCHQ Compliance Documentation ...."

This undertaking, combined with the limited purposes for which GCHQ can gather and use material and the adherence to the JIC requirements when requesting the data, we believe, allows GCHQ to demonstrate that an individuals rights are being properly protected. In addition, this extract, when coupled with the remainder of the submission, allows the Secretary of State to

EMBARGOED UNTIL 6 JUNE 10:30 BST

POSITIVE ABOUT DISABLED PEOPLE
INVESTOR IN PEOPLE

[redacted]

satisfy himself that GCHQ will obtain and subsequently handle the data in a justified and proportionate manner, notwithstanding that the individuals whose data may be accessed are not identified either in the directions themselves or in the accompanying submission.

GCHQ is not looking to re-open this issue, but I just thought it worthwhile to state our view as clearly as possible.

Yours sincerely,

[redacted]

[redacted]
Legal Adviser

EMBARGOED UNTIL 6 JUNE 13:00 BST

POSITIVE ABOUT DISABLED PEOPLE

INVESTOR IN PEOPLE