INTELLIGENCE AND SECURITY COMMITTEE
35 Great Smith Street, London SW1P 3BQ

The Intelligence and Security Committee (ISC) has issued the following statement regarding the draft Communications Data Bill:

In June, the Government published a draft Communications Data Bill. Given the importance of communications data to the security and intelligence Agencies the ISC has examined the Bill. We wish to make clear that we have only considered communications data in relation to the intelligence Agencies. Lord Blencathra has chaired a Joint Committee of Parliament which considered the wider issues in the draft Bill and the impact on law enforcement agencies (who are the primary driver for the Bill and make the majority of requests for communications data). We have not sought to duplicate the work of the Joint Committee in any way but nevertheless hope that our work complements theirs.

We have taken detailed evidence, much of which is highly classified as it relates to the current capabilities – and lack of capabilities – of our intelligence Agencies. We have sent a classified report on our findings to the Prime Minister. However we are conscious that the question of access to communications data is one which is generating significant public debate – and rightly so, since any intrusion into an individual's personal life should not be done lightly. We are, therefore, intending to publish in due course as much of the content of that report as possible. We are today publishing a summary of the report and our conclusions.

GENERAL SUMMARY

1. Any proposals to intrude into the lives of citizens will, understandably, prove controversial and will, rightly, provoke debate. In the case of communications data, however, we accept that there is a serious problem that requires action.

2. The UK is not alone in facing the problem of the deteriorating access to communications data. We have held conversations with some of our 5-Eyes counterparts who are clearly facing the same issues, as are our European allies. Some EU countries have cited the EU Data Retention Directive as the driver for change. However the Data Retention Directive does not impose any obligations on Communications Service Providers to retain data they do not need to hold for business purposes, and therefore cannot be used to address the 'capability gap'. The UK is amongst countries such as France and Denmark who have therefore chosen to take both a forward-looking and transparent approach in seeking to introduce new legislation.

3. Our Inquiry has focussed on the problem as it relates to the UK's intelligence and security Agencies: we reiterate that we do not see it as our role to form a judgement on the wider application of the draft Bill.

4. The Agencies require access to communications data – in certain tightly controlled circumstances and with appropriate authorisation – in the interests of national security. We recognise that changing technology means that the Agencies are unable to access all the communications data they need, that the problem is getting worse, and that action is needed now. We accept that legislation to update the current arrangements governing retention of communications data offers the most appropriate way forward.

5. Turning to the draft Bill, we strongly recommend that more thought is given to the level of detail that is included in the Bill, in particular in relation to the Order-making power. Whilst the Bill does need to be future-proofed to a certain extent, and we accept that it must not reveal operational capability, serious consideration must be given as to whether there is any room for manoeuvre on this point: Parliament and the public will require more information if they are to be convinced.

6. We have similar concerns regarding the background information accompanying the Bill. Whilst we recognise the need to take action quickly, the current proposals require further work. In particular, there seems to have been insufficient consultation with the Communications Service Providers on practical implementation, as well as a lack of coherent communication about the way in which communications data is used and the safeguards that will be in place. These points must be addressed in advance of the Bill being introduced.

DETAILED CONCLUSIONS

The Agencies' use of communications data

It is clear to us from the evidence we have been given that communications data is integral to the work of the intelligence and security Agencies and, certainly in terms of the Security Service, it is used in all their investigations.

Whilst communications data can be used throughout an investigation, it can be particularly useful in the early stages, when the Agencies have to be able to determine whether those associating with the target are connected to the plot (and therefore require further investigation) or are innocent bystanders. The easiest, and least intrusive, way of doing so is through access to communications data.

If the Agencies cannot use communications data, then they would need to rely more heavily on other capabilities to provide coverage. However, these other capabilities - such as surveillance or the use of informants - are not like-for-like substitutes, are more intrusive and therefore not always justifiable, and are far more resource intensive. We therefore consider that it is essential that the Agencies maintain the ability to access communications data.

What is the current problem?

The fact that there is a problem regarding future access to communications data, if not its precise scale, is easily understood. If the Communications Service Providers are not retaining communications data for internal business reasons, then that data will not be available to the Agencies.

The current gap between the data required by the Agencies and that which the Communications Service Providers – both domestic and overseas – hold for their internal business reasons is significant and, without any action, will continue to grow.

We do not believe that there is any benefit in providing superficially precise estimates of the size of this 'capability gap': unless there is a demonstrable basis for such figures they can be misleading. They can also detract from consideration of the problem itself, which is not necessarily linked to the size of the gap – even a small gap could have a disproportionately large impact.

What impact will the problem have on the Agencies?

We have heard numerous examples from the Agencies of communications data playing a vital role in investigations, particularly Security Service counter-terrorism operations. If the availability of communications data continues to decline this will have a serious impact.

At present, the intelligence and security Agencies are able, to some extent, to work around the problem of declining communications data by obtaining intelligence using other national security capabilities which are not, in most cases, available to the police. This means that the Agencies are not facing as immediate a problem as that currently faced by the police and other authorities. Nonetheless, we believe that the decline of available

communications data will begin shortly to have a serious impact on the intelligence and security Agencies.

How to tackle the problem

We have examined the possibility of expanding the use of other investigatory tools to offset the decline in availability of communications data and also whether a voluntary approach might work: neither offers a solution, and indeed the Communications Service Providers themselves have said that they must have a legal foundation to retain data. While legislation is not a perfect solution, we believe it is the best available option.

Are the provisions workable?

We recognise that the Bill is deliberately broad in order both to permit future-proofing of the legislation against technological change and not to reveal gaps in operational capability. However this is causing considerable concern for the Communications Service Providers and also Parliament and the public. We therefore welcome the decision by the Home Office to make public information on the three core elements of the gap: subscriber details showing who is using an Internet Protocol address; data identifying which internet services or websites are being accessed; and data from overseas Communications Service Providers who provide services such as webmail and social networking to users in the UK. This is a positive step. However, we recommend that more thought is given as to whether this can be reflected on the face of the Bill.

The data which would be most useful to criminals and terrorists, and which therefore is most sensitive, relates to the individual data retention notices. These must not be made public, since they would reveal which companies' services or applications can be used with the least risk of detection.

It is important for the Agencies that there is some means of accessing communications data from uncooperative overseas Communications Service Providers. The Government's proposed solution appears capable of performing this role.

Whilst we recognise the UK Communications Service Providers' concerns, we believe they would be willing to co-operate in deploying Deep Packet Inspection technology to obtain third-party data. We are however sympathetic to their argument that the Home Office should have to demonstrate due diligence before resorting to the use of Deep Packet Inspection to collect communications data from overseas Communications Service Providers, and we recommend that this should be reflected on the face of the Bill.

We believe the Government has adopted a pragmatic approach to the issue of encrypted material. In the first instance, agreement should be sought with the Communications Service Provider holding the communications data to provide it in an unencrypted form.

Where this is not possible, we accept the only prudent alternative is to attempt to collect residual, unencrypted communications data associated with a communication, which – although of lesser volume – may nevertheless still be of intelligence value.

The Committee considers that a filtering mechanism would offer considerable benefits to the Agencies. It would save many hours of analysis, and reduce the amount of collateral intrusion from complex communications data requests.

The technology seems to exist to provide this. It will be a significant challenge to integrate the numerous data sets from different Communications Service Providers to make the filter work, as well as manage the expectations of the various Departmental and Agency stakeholders. The record of government in managing such complex IT projects is mixed at best.

Authorisation procedures

The current arrangements within the intelligence Agencies for authorising communications data applications appear detailed and robust, and an appropriate safeguard on the use of these powers.

Any move to introduce judicial oversight of the authorisation process could have a significant impact on the intelligence Agencies' operational work. It would also carry a financial cost. We are not convinced that such a move is justified in relation to the Agencies, and believe that retrospective review by the Interception of Communications Commissioner, who provides quasi-judicial oversight, is a sufficient safeguard.

NOTES TO EDITORS:

1. The Intelligence and Security Committee (ISC) was established in 1994 to examine the policy, administration and expenditure of the Security Service, Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ). The Committee also examines the work of the Joint Intelligence Committee (JIC), the Assessments Staff and the National Security Secretariat in the Cabinet Office, and Defence Intelligence (DI) in the Ministry of Defence.

2. The ISC is a cross-party Committee of nine Parliamentarians from the Lords and the Commons. The Prime Minister appoints ISC Members after considering nominations from Parliament and consulting with the Leader of the Opposition. The Committee's membership is as follows:

The Rt. Hon. Sir Malcolm Rifkind, MP (Chairman)

The Rt. Hon. Hazel Blears, MP	*The Rt. Hon. Paul Goggins, MP*
The Rt. Hon. Lord Butler KG GCB CVO	*The Rt. Hon. George Howarth, MP*
The Rt. Hon. Sir Menzies Campbell CBE QC, MP	*Dr Julian Lewis, MP*
Mr Mark Field, MP	*Lord Lothian QC PC*

3. The ISC takes evidence in private, and its Members are subject to the terms of the Official Secrets Act 1989. This ensures they are able to scrutinise the most sensitive work of the intelligence Agencies that cannot be made public. However, when producing reports, the Committee aims to put as much material as possible in the public domain.

4. Communications data refers to the 'who, where and when' of a communication – but not the 'what'. Details that can currently be requested from a Communications Service Provider include subscriber details or calls made or received by a telephone number, and the location of a handset at a particular time. The content of a telephone conversation or email cannot be accessed in this way, and require a warrant signed by a Secretary of State. Requests for communications data are subject to strict processes of internal authorisation within public authorities, and are subject to external review by the independent Interception of Communications Commissioner.

5. The Government's draft Communications Data (CD) Bill was published on 14 June 2012. It covers revisions to be made to current powers of public bodies to access communications data (i.e. that information about a communication, but not the content). A Joint Committee of Parliament was established to conduct formal pre-legislative scrutiny of the draft Bill, and was charged to report to both Houses by the end of November 2012.