Response of the Criminal Bar Association to the Home Office Consultation on Changes to the Present Regime governing Communications Data under RIPA 2000

Introduction

1. On 27th April 2009 the Home Office published a Consultation document entitled "Protecting the Public in a Changing Communications Environment", inviting the views of interested persons on its proposals for significant changes to the type of Communications Data that Communication Service Providers would be required to hold and the extent to which those Service Providers would be required to process such data in anticipation of applications by Public Authorities for access.

2. The paper runs to some 41 pages in the course of which it poses 4 consultation questions. The closing date for responses is 20 July 2009.

3. The Criminal Bar Association represents 3,500 barristers, self-employed and employed, that specialise in criminal law acting for and advising prosecution agencies and defendants.

Executive Summary

1. Communications Data is information that discloses the "from whom", "to whom", "when", "where" and "how" of communications. It includes the technical information used by Communication Service Providers to enable them to meet the service users' aims of communicating via the particular medium adopted, whether postal, telephonic or e-based. It does not relate to the content of such communications and as such is to be distinguished from the regime for interception of communications.

2. However, information gained from communications data does have an important connection to the use of intercepts for investigative purposes. As recognised in the consultation, applications for intercepts are often based on the patterns of association revealed in the analysis of such data.

3. The overwhelming majority of users of communications services are of no interest to law enforcement, security, intelligence or emergency services.

4. The focus of the proposals in the current consultation is to bring about a system which ensures the retention of the existing categories of Communications Data (e.g. in the case of mobile telephones call data and cell site data) but also the retention by Service Providers of data which reflects the use by individuals of third party communication systems which are run "over" the basic lines of communication provided by the Service Provider to the user. This type of information is described in the consultation as "third party communication data".

5. The area the Consultation identifies as in need of a Governmental response might appear to be of an essentially technical nature. However, if enacted, the proposals will bring about a data retention regime which will be extremely broad and which will impose significant added burdens upon Communication Service Providers not only to retain more data but also to ensure that the data that they hold is pre-analysed. The aim of such pre-analysis is to

facilitate timely responses to applications for Communications Data from public authorities under RIPA 2000.

6. The Consultation includes a rejection by the Government of a solution based upon a single state-operated database.

7. The Criminal Bar Association is concerned that the proposals include the retention of a vast amount of information and seek to outsource the automatic analysis of all such information by Communication Service Providers.

8. Such automatic analysis of all such information will bring about highly detailed records of the use of communications services by every user. The proportion of such users that are ever likely to be of interest to public authorities is vanishingly small. The proposal that such analysis should occur automatically is a blanket solution that is objectionable even when not carried out by the State.

9. To put this in terms that are perhaps more easily understood, it as if the government were to ask the Royal Mail to keep a record, in respect of every letter ever posted, of the name and address of both sender and recipient and the date, time and place of posting. The technical ease with which such information can be recorded in respect of electronic data ought not to disguise the highly intrusive and disproportionate nature of what is now being sought.

10. In these circumstances and regardless of the potential for any system of safeguards to fail, it is better that such blanket analysis does not occur in anticipation of a RIPA request by a public authority but instead takes place after (or as a part of a response to) such a request.

Background to the Consultation

The Consultation describes the background in the following way at page 3:

"The Challenges

11. The communications industry is highly competitive and technologically driven. The UK is currently undergoing the most significant communications changes since the development of the telephone as a competitive market encourages companies to find new ways to offer more services and cut costs. BT, the largest network provider in the UK, is currently in the process of rolling out a nationwide network based on Internet Protocol.

12. As a result of these technical changes, companies will offer more communications services, for voice, data and media, and including TV, social networking, music, video messaging, games, text, email and internet browsing. Some new services will be offered by the companies that operate the existing communications networks. Others will be offered by companies, some based overseas, providing services without any physical networks of their own.

13. These changes will have a significant impact on the ability of public authorities to continue to access, and use, communications data as they have done in the past. The proportion of communications data that is retained by communications service providers in the UK, and therefore accessible to the authorities, will decline. That data will be more fragmented if it crosses the networks of several communications service providers."

The Governments Proposals are set out at pages 26 and 27:

"As a first step, the Government would legislate to ensure that all the data that public authorities might need, including the third party data, is collected and kept in the UK. Communications service providers based in the UK would therefore continue to collect and retain communications data relating to their own services but also collect and store the additional third party data crossing their networks. This would therefore include

communications data which does not come under the scope of the EU Data Retention Directive.

All the data retained by the communications service providers would continue to be accessible on a case-by-case basis to public authorities, subject to the same rigorous safeguards that are now in place.

This option would put additional demands on industry, especially around the collection and retention of third party communications data not required for the business purposes of communications service providers. The Government is therefore actively seeking the views of industry on these proposals through this consultation.

This option would resolve the problem that some communications data which may be important to public authorities will not otherwise be retained in this country. However, it would not address the problem of fragmentation: as data is increasingly held by a wider range of communications service providers, it might take longer than it does at present to piece together data from different companies relating to one person or communications device. The current capability would therefore diminish.

To mitigate this problem the Government would require communications service providers not only to collect and store data but to organise it, matching third party data to their own data where it had features in common (for example, where it relates to the same person or to the same communications device). This would require additional legislation.

Organising data together would help to ensure that communications service providers would be better able to respond to a request from public authorities for all the data relevant to a specific communications device or subscriber. It would significantly decrease the turnaround time for requests and in life-threatening situations greatly help public authorities. In particular, where all the data that a public authority needed for an investigation was held by one communications service provider, this option would mean it was available quickly in a readily understandable form.

To maintain the capability set out in this document, the Government recommends taking the steps outlined above, specifically: that it legislates to ensure that all data that public authorities might need,

including third party data, is collected and retained by communications service providers; and that the retained data is further processed by communications service providers enabling specific requests by public authorities to be processed quickly and comprehensively."

Responses to the Consultation Questions

Question 1

"On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public? "

1. This the type of leading multiple –part question to which on one level the answer self-evidently is "yes" but which begs many other questions: are all the data as "vital" to (e.g.) the emergency services as they are to law enforcement or intelligence services? What is the definition of serious crime and how will the collection of data differentiate it from less serious crime? What does a phrase like "protecting the public" connote beyond tackling serious crime and terrorism? Where is the proportionality of the measure considered?

Question 2

"Is it right for Government to maintain this capability by responding to the new communications environment? "

2. Again, the form and language of this question superficially admits of only one answer: "Yes". Such a question and answer gives no assistance in assessing the appropriateness of particular means to this end.

Question 3

"Do you support the Government's approach to maintaining our capabilities?"

3. We are concerned that the Government, having stated that it recognises the privacy objections that there would be to a single state-run system based upon a centralised database of all the expanded definition communications data, is intent upon bringing about a system in which the collection and analysis of exactly the

same degree and quantity of communication data is outsourced to Communication Service Providers.

4. It seems to us that, if there are acknowledged privacy concerns involved in the collection and collation of this degree of information, those concerns do not disappear if they have been carried out by Communication Service Providers. It is envisaged in the consultation that such collection and collation will take place automatically and for all users of a particular Communications Service in anticipation of the statistically extremely unlikely possibility that a request for such information is subsequently made by a public authority under RIPA.

5. The proposed retention and pre-analysis by Communication Service Providers would put them in possession of data that extends far beyond that required for their business purposes and which would represent a level of intrusion into the legitimate and private communications of the overwhelming majority of their customers. Additionally, there is no reason to suppose that the employees of such Communication Service Providers are less likely than anyone else to misplace copies of sensitive data or to offer them to organs of the media.

Question 3 (supplemental) "*Which of the solutions should it adopt?*"

6. On a close reading of the consultation, it seems that there is really only one proposal: that Communication Service Providers retain <u>all</u> existing communication data and third party communication data <u>and</u> that they automatically subject all the data stored to pre-analysis.

7. In our view the automatic retention and analysis of <u>all</u> communications data is objectionable on privacy grounds whether it is carried out by the State in a single database or piecemeal by individual Communication Service Providers.

8. If the extra step of pre-analysis were to be omitted from current proposals then it seems to us that a scheme which only requires the retention of data <u>might</u> be a more measured response to the identified need to ensure that the Communications Data retained matches technological developments.

9. The Government's concern that the fragmented nature of the expanded range of communications data could delay timely

responses in critical situations could be met by targeted "de-fragmentation" at the point of a request under RIPA. This would be a less intrusive approach than the blanket pre-analysis of all data.

Question 4

"Do you believe that the safeguards outlined are sufficient for communications data in the future?"

10. We consider that safe-guards discussed in the consultation at pages 27 to 29 represent the very minimum that is required.

11. We consider that if the Communication Service Providers are required to pre-analyse all communications data legitimate questions will arise as to the extent to which they are assuming public duties. Even without such pre-analysis, the simple act of retaining such a broad range of otherwise private data should be seen as involving heavy responsibilities.

12. Given the gravity of the responsibilities likely to be imposed upon Communication Service Providers, we are concerned whether reliance upon Data Protection Act 1998 and Computer Misuse Act 1990 offences is sufficient. There are no criminal offences created under RIPA 2000 in relation to the unauthorised disclosure of communications data. This is in contrast to the position in relation to unauthorised interceptions of the content communications. We would welcome an opportunity to contribute to any future consultation on creating specific offences relating to the unauthorised disclosure of communications data.

Paul Mendelle QC

Adrian Chaplin

July 2009.