All Party Parliamentary Internet Group

Communications Data: Report of an Inquiry by the All Party Internet Group

January 2003

APIG
ALL PARTY INTERNET GROUP

Communications Data

Report of an Inquiry by the All Party Internet Group

January 2003

Introduction

1. The All Party Internet Group (APIG) exists to provide a discussion forum between new media industries and Parliamentarians for the mutual benefit of both groups. Accordingly, the group considers Internet issues as they affect society, informing current parliamentary debate through meetings, informal receptions and reports. The group is open to all Parliamentarians from both the House of Commons and the House of Lords.

2. APIG issued a Press Release (*see Appendix A*) on 15th November 2002 to announce its intention to hold an inquiry:

> "into all aspects of communications data retention and the subsequent access to that data from a UK, European and global perspective. The inquiry will primarily focus on the enforcement of the powers contained in the Regulation of Investigatory Powers Act and the Anti-Terrorism, Crime & Security Act and their subsequent effect on communication service providers".

3. Written submissions were received from:

AOL (UK) Ltd
Mr Harry Cohen MP
European Information Society Group (EURIM)
Mr Peter Fairbrother
Foundation for Information Policy Research (FIPR)
ACC Jim Gamble, NCS
"on behalf of the UK Law Enforcement Community"
The Home Office
Internet Service Providers Association UK (ISPA)
Internet Society of England (ISOC England)
The JNT Association (trading as UKERNA)
Microsoft
The "Ad Hoc Operators ATCS Group"
Cable & Wireless, BT, T-Mobile, Telewest, ntl, Nortel Networks, Worldcom, O_2 (UK), O_2 Online, Colt, Hutchinson 3G, Orange, Vodafone, Kingston Communications, Thus, Energis and Your Communications
Orange UK
Dr Chris Pounder
T-Mobile(UK)
Prof. Clive Walker and Dr Yaman Akdeniz

4. The committee heard oral evidence in public from:

Internet Service Providers Association UK (ISPA)
Ms Camille de Stemple & Mr Clive Feather
Dr Ian Walden
Foundation for Information Policy Research (FIPR)
Dr Ian Brown
European Information Society Group (EURIM)
Mr Philip Virgo
UK Law Enforcement
ACC Jim Gamble & Mr John Donovan
The Home Office
Mr Bob Lack & Mr Simon Watkin
Mr Peter Fairbrother

and had private meetings with:

Representatives of the "Ad Hoc Operators ATCS Group"
BT, Cable & Wireless, T-Mobile(UK) & Thus
Bob Ainsworth
Parliamentary Under Secretary of State at the Home Office.

5. We are grateful for all the written and oral evidence that we received and also for the expert advice and assistance afforded by our specialist advisor, Richard Clayton of the Computer Laboratory, University of Cambridge.

6. Communications data retention and subsequent access to that data is a complex topic. These activities are subject to several different Acts of Parliament, which, we have learned, do not always join up properly at the edges. With the intention of making our report and conclusions easier to follow this report is split into a number of sections based loosely around the applicable legislation.

7. We first look at the general nature of communications data and how this might change in the future. We then examine the access provisions of Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA) and then discuss how it defines communications data. Since RIPA is not yet in force, we investigated the current data access regime that operates under the Data Protection Act 1998. We also consider the problems surrounding access to records by data subjects.

   We move on to consider the addition of further public authorities to RIPA and whether they should be using the "single point of contact" (SPOC) scheme. We also consider the question of "legacy legislation" that allows access to communications data and the problems of oversight and punishment that arise when considering abuses of data access systems.

   We examine in some detail the problems that surround the data retention regime set out in the Anti-Terrorism Crime and Security Act 2001 (ATCS), considering both the voluntary and compulsory regimes that are proposed by the legislation.

   Finally, we consider some issues relating to international co-operation that the Cybercrime Treaty has raised and look at a few of the more general suggestions made to us. A summary of our recommendations completes the main report.

   A glossary is provided *(in Appendix B*) for those unfamiliar with the technical terms and abbreviations that are used.

The Usage of Communications Data

8. There is considerable evidence that communications data relating to telephone usage (both fixed and mobile) is of great importance to Law Enforcement Agencies. Both the police and the Home Office put forward a number of "war stories" in their evidence to show how this data was being used in practice.

9. Every year an estimated million requests are being made to the telephone companies for information. The vast bulk of the requests are for subscriber data (who owns a particular phone number). Significant numbers of requests are also being made for billing data (which numbers were called) and for more specialist services such as the source of incoming calls or the geographical location where a mobile was used ("cell site data"). Telephone companies routinely bill the police for this data access, with the charges set at a level so that they can recover their costs.

10. Law Enforcement Agencies are also requesting communications data from Internet Service Providers (ISPs) but not in such large quantities. We were given fewer "war stories" about this type of request, but the Home Office did provide several examples of how Internet communications data was essential in tracking down wrongdoers. As with the telephone industry, the bulk of the requests are for subscriber data, but traffic data is also being sought occasionally. The lower volumes means that ISPs are often absorbing the costs, so charging is not universal but it does seem to be becoming more common.

11. There are very few statistics being collected as to how much money is being spent on accessing communications data, how effectively the results are being used, or even how many raw requests are being made, let alone of what type.

12. Since there is no raw information, there is no information either on whether the trend is towards more requests or fewer. The lack of information also makes it impossible to speculate on whether the introduction of RIPA will mark a significant change on the number of requests that the ISPs will receive.

13. The industry witnesses made it clear to us that the communications companies are expending considerable resources to service the requests they are receiving with whole departments doing no other tasks. The industry is also actively assisting, at their own expense, with the training of the Law Enforcement personnel who make the requests. Many of the telephone companies had developed special automated systems that allowed responses to be made in minutes (at very low cost), even for complex requests such as cell site data.

14. However, industry suggested to us that significant delays were occurring in some police forces because of an inadequate allocation of resources to the departments that make the requests. How police budgets should best be spent is, of course, a matter for Chief Constables and Police Authorities. However, if communications data is as important as many witnesses averred, we find it to be, at the very least, inconsistent that, in some areas, insufficient funds are being made available.

15. ACC Gamble explained that backlogs can also arise at particular service providers and this backlog can exceed the data retention time, so that when a request reached the front of the queue the data would no longer be available. For this reason, low priority requests might not be made at all to these particular

companies because they were expected to fail. Unfortunately, no record was currently being kept as to how often this occurred.

16. We were told that the existence of backlogs meant that some investigators were being tempted to avoid the proper systems and approach the communications companies directly. Since this avoids all of the controls built into the proper systems it is clearly in the public interest to ensure that the delays and backlogs in the access systems are minimised.

17. We find it remarkable that so little definite quantitative information is available about a system which is of such importance and that also appears to involve many millions of pounds of cost recovery payments. **We recommend that a formal statistics gathering process be put in place so as to determine the scope of access to communications data and its direct costs.**

18. The statistics collected must be detailed enough to distinguish between different types of communications data request (subscriber data, usage data, cell site analysis etc). Since requests may involve many individuals, it would be very desirable to collect sufficient information so as to be able to estimate the number of people whose privacy is being affected.

19. The process should also record sufficient information to allow an ongoing analysis of how effective communications data requests turn out to be in assisting Law Enforcement. This will ensure that those who set and spend Law Enforcement budgets can make proper value-for-money judgements.

The Future of Communications Data

20. It was suggested to us that individuals could reduce or eliminate the amount of communications data they created that was traceable to them. It was also suggested that steganographic techniques could make any data transfer appear to be innocent. We accept that, as time goes on, major criminals and terrorists, in particular, may find ways of reducing their vulnerabilities, much as burglars often wear gloves to avoid leaving fingerprints. However, at present it seems that analysis of communications data is an effective technique and we see no reason to believe this will change in the short term.

21. In the longer term, if communications data analysis ceases to be an effective tool when targeting well-informed wrongdoers then only the technologically naïve will be caught. Such a change would affect many of the trade-offs and "value-for-money" judgements of the matters that we consider in this report. Therefore, **we recommend that the Home Office supervise a regular, formal, technical assessment of the state of this technology 'war' and the overall effectiveness of the use of communications data in crime-fighting.**

22. There are already several forums that bring together Law Enforcement, Government and the Communications industry:

    - The ***ACPO Data Communications Strategy Group***, recently renamed from the ACPO Police and Telecommunications Industry Strategy Group, focuses on telephone service matters;
    - The ***Internet Crime Forum*** (originally called the ACPO, Internet Service Providers and Government Forum) focuses on Internet issues;
    - The ***Government/Industry Forum on Technology and Law Enforcement*** (originally named the "Government-Industry Forum on Encryption and Law Enforcement" and created on the recommendation of the 1999 Cabinet Office PIU Report "Encryption and Law Enforcement") originally concentrated on encryption issues. It has, despite its composition, lately considered the topic of communications data retention periods.

23. These forums have a mixed record in tapping expertise from academia and civil liberties groups. They have almost entirely failed to interact with the individuals, some of whom are UK-based, who have been the main developers, so far, of various "Privacy-Enhancing Technology" systems whose aim is often to prevent the tracing and identification of Internet users by anyone, including Law Enforcement. The risk in consulting only within Law Enforcement and with industry's "big players" (who are the main supporters of the existing forums) is that policy will be reactive, rather than anticipating trends.

24. This is an area of rapid change where "in house" and "big company" expertise may become outdated very quickly. **We recommend that the Home Office should ensure that they seek the views not only of Law Enforcement and the communications industry, but also independent views from academia and from the relevant technology developers themselves.**

25. Another topic that will become more important in the future was drawn to our attention by UKERNA. They pointed out how necessary it was that once communications data has been provided to Law Enforcement that it be held securely, with appropriate technical and procedural protection. The data archive could be useful to criminals and was likely to become a target for attack. They told us that public confidence would depend as much on the perception of secure storage as on the fact.

26. UKERNA also pointed out the need for Law Enforcement to educate industry on forensic standards. Outside the major companies they said:

> "few if any staff of educational organisations, or indeed private companies, that operate communications networks have been trained in collecting computer evidence to forensic standards. If data retained and accessed under these provisions are not to be seriously doubted in court this will require a great deal of individual tuition of network operators by law enforcement officers, and a considerable amount of effort for both parties".

Access to Communications Data through RIPA

27. Part I Chapter II of the Regulation of Investigatory Powers Act 2000 (RIPA) sets out the regime for access to all types of communication data. The Act provides for access by the Police, Customs & Excise, the Security Services and the Inland Revenue. There is also a procedure for adding other public authorities to this list, to which we will return later in this report.

28. RIPA defines communications data in three broad categories, "traffic data" (where and when communications are occurring); "use of a service" (when and where it is accessed and for how long); and "subscriber data" (the information about the subscriber's identity).

29. The procedures on the face of the RIP Act for access to all three of these communications data categories is the same. An officer either serves an "s22 notice" on the communications service provider (CSP) who is holding the communications data or the officer receives an "authorisation" to access the data themselves.

30. A Code of Practice will prescribe when an authorisation is proper, for example when a hotel does not have the skills themselves to access call data held within their switchboard. The Code of Practice will also specify that a senior officer must approve notices and authorisations. It is expected that within the police service, requests for subscriber data will need to be approved by an Inspector and all other communications data requests will have to be signed off by a Superintendent.

31. There was widespread support for Law Enforcement to continue to have access to communications data. However, the reasons for which access should be allowed did differ markedly in the evidence we received. Industry generally thought the reasons should be national security, terrorism and serious crime. ISOC England though that national security was a suitable reason, but access should not be granted for general policing.

32. The law enforcement community and the Home Office believe that access should be available for the investigation and prevention of crime whenever it was necessary, reasonable and proportionate. They also drew attention to the growing use of communications data by defence lawyers and that the Criminal Cases Review Commission was concerned that deletion of data might lead to miscarriages of justice.

33. Some of the disagreement was clearly founded on different views as to the sensitivity of different types of communications data. The Home Office went to some effort to stress the difference between communications data and content. Access to content by "interception" is governed by a completely different legal regime involving warrants signed by the Secretary of State.

34. Those who were opposed to unfettered access to communications data made the point that some types of traffic data on the Internet, such as lists of visits to websites were almost as revealing as content, citing the former Information Commissioner's view that:

> "both sets of data provide insight into the private lives of individuals and should therefore be subject to equivalent controls and safeguards".

35. Dr Walden agreed with this proposition and then told us that he believed that the European Court of Human Rights has "somewhat lagged behind" in understanding the developments in communication. He felt that:

> "the onus is upon Government and policymakers to justify why the treatment of those two types of data is so different".

36. To meet the specific concern about the intrusiveness of "click-stream data" revealed by records of every web page that is visited, the original RIP Bill was amended during its passage through Parliament. Wording was added to restrict the amount of detail that can be obtained about website visits. In essence, the intent was to ensure that records of web accesses would only specify the site visited rather than exactly which page. As Mr Donovan helpfully put it, the police "are limited to the first slash" in the URL. Although this limits intrusion, some of the witnesses clearly still felt that reporting the mere names of the websites being visited was very intrusive.

37. FIPR proposed a three level authorisation scheme, with Law Enforcement providing internal authorisations for access to "subject identification" data and judicial approval being required for other types of communications data (much as it is required for search warrants at present). The existing Secretary of State signed warrants would continue to be needed for access to content. FIPR argued that the low levels of requests for anything other than subscriber data would mean that the judiciary would not be overwhelmed.

The Definition of Communications Data

38. EURIM told us they were very strongly of the opinion that laws should be technology neutral and the same law should apply on-line as off-line. They believed that the meaning of communications data was a "moveable feast" and that:

> "The moment you try and do definitions which rely on some kind of implicit technology model, then you know that those definitions are doomed, certainly within ten years and probably within five. It is better [..] going for genuinely technology neutral definitions as opposed to trying to draft the definitions which look as though they are technology neutral but really depend on a model of thinking of how, at the moment, the Internet works or rather the packets on which a sub-set of the Internet works".

39. Several witnesses averred that RIPA had turned out not to be entirely neutral between telephones and the Internet, since they believed that the definitions encouraged spurious analogies between phone billing data and website visits. ISOC England went further and made the point that the technology comparison

was far too narrow. They observed that detailed records are kept about email but not recorded for postal mail. They also asked us to consider the rather different amounts of logging data that would be generated if one went shopping online rather than taking a trip to the local High Street.

40. Several witnesses noted the complexity of the definitions within RIPA for the different types of communications data. They observed that this would make it hard to implement different levels of authorisation, whether this was along the FIPR lines, or the Home Office proposals to require more senior officials to sign the internal authorisations for some types of data.

41. EURIM noted that the definitions in the legislation are "difficult to reconcile" with the real world things they describe and that this would be compounded by rapid change. FIPR asked what actual purpose some of the distinctions served and Ian Walden suggested that it would sensible to request data by description, rather than to risk error when creating formal paperwork by attempting to categorise it into the exact (a), (b), (c) definitions of s21(4).

42. The Home Office told us that they were intending to build up "common understandings" of the meanings of the particular types of communications data.

43. The Home Office drew attention to the consultation that they are about to commence on the addition of further public authorities to the list in RIPA s25(1). We think that it is very likely that this consultation will conclude that some of these public authorities should have "internally authorised" access only to some specific types of communications data. Therefore, since this specificity is likely to be based on the formal definitions in RIPA, the exact differences between s21(4) (a) (b) and (c) will become very significant.

44. The evidence we have heard has led us to conclude that the existing definitions of communications data are inadequate, especially when attempts are being made to draw parallels between data generated in making a telephone call and that generated by accessing the Internet. **We strongly recommend that, as a part of their forthcoming consultation, the Home Office should seek to establish better definitions for the different types of communications data.**

45. The imminence of the Home Office consultation makes it undesirable for us to make recommendations in the areas it will cover, because the Home Office should be giving significant weight to the responses it receives. However, **we do recommend that if the Home Office consultation shows that it is desirable to amend the definitions within RIPA s21(4) then appropriate legislation should be brought forward as soon as is practicable.**

46. Dr Pounder proposed that a specific prohibition should be put into RIPA to prevent access to communications traffic data for "predictive use". If particular patterns of behaviour were highly correlated to criminal behaviour then it might become possible for "fishing expeditions" to detect these patterns to be seen a proportionate action. We agree that this type of access to traffic data raises considerable concern and do not believe it should be permitted under an "internal authorisation" regime. **We recommend that the Home Office ensure that their forthcoming consultation seeks to determine whether the public agrees that access to communications data for "predictive" purposes should be subject to special controls.**

Use of the Data Protection Act 1998

47. Communications data that refers to individuals is defined to be "personal data" by the Data Protection Act 1998 (DPA) and by its predecessor the Data Protection Act 1984. This means that the data controller – the Communications Service Provider (CSP) – has some legal obligations that prevent this data being handed out, willy-nilly, to anyone who asks for it.

48. Although, RIPA Part I Chapter II provides a legal framework for access to communications data that will override the DPA provisions, it has not yet been brought into force.

49. In October 2000 the Home Office intended this to happen "during the second half of 2001", but various delays then occurred. By June 2002 a firm date of August 1st 2002 was being widely promulgated, but this was scrapped as a result of the furore surrounding the Home Office proposals to add further public authorities to the list in s25(1).

50. Many of the original delays appear to have been caused by difficulties in creating an appropriate Code of Practice. A draft of this Code of Practice was subject to a public consultation between August and November 2001, but the Home Office has yet to publish the results of this exercise, their intent having been to do this when they laid the Code of Practice before Parliament.

51. At present, communications data continues to be accessed by Law Enforcement Agencies by using some specific exemptions within the DPA. In particular s29 (s28 in the 1984 legislation) permits CSPs to release data if a sufficient case is made for its release. The specific tests are:

> s29(1) Personal data processed for any of the following purposes-
> (a) the prevention or detection of crime,
> (b) the apprehension or prosecution of offenders, or
> (c) the assessment or collection of any tax or duty or of any imposition of a similar nature,
> are exempt from the first data protection principle […] to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.
>
> s29(3) Personal data are exempt from the non-disclosure provisions in any case in which –
> (a) the disclosure is for any of the purposes mentioned in subsection (1), and
> (b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

52. Requests are made using a standard "29(3) form". There is some, albeit limited, information on this form to allow the communications service provider to assess whether it would be correct to release the requested information. One of the mobile operators told us in private that the volume of requests was such that "it is not possible for a CSP to form its own considered view on whether each individual request is 'appropriate'". This is clearly unsatisfactory for a CSP because it is they, and not the requesting officer, who would be committing an offence if the request were flawed in some way.

53. We were told that there was significant trust in police procedures because of the way that requests were funnelled through specialist departments. This trust did not extend to public authorities in general and therefore 29(3) forms, acting upon which is entirely optional, were not usually accepted from other bodies.

54. The evidence from the Internet and telephone industry was that they wished to see Part I Chapter II of RIPA in force as soon as possible, once a Code of Practice was approved. Some felt that it should be implemented "immediately".

55. The evidence from Law Enforcement was that they also wished to see Part I Chapter II of RIPA brought into force "swiftly". In particular, they expressed concern that the permissive nature of the DPA provisions (which permits release of communications data, rather than requiring it) is not compliant with the European Convention on Human Rights. This lack of compliance arises, they said, because it is not access "by law", and hence their current procedures might be open to challenge under the Human Rights Act 1998.

56. However, Law Enforcement also explained to us that they had very recently revamped their procedures to make them identical to those that would be used when Part I Chapter II of RIPA does eventually come into force. Even the forms now being used were essentially the same as the RIPA versions, except that they referred to the DPA rather than to RIPA.

57. Dr Walden told us that he found it "hard to believe" that the DPA arrangements would fall foul of Human Rights legislation. He went on:

> "The legislative provisions clearly make it foreseeable to an individual that their data could be accessed for the purpose of a criminal investigation. The certificates which have been agreed between the industry and law enforcement agencies, I think, probably give greater credence to this process rather than rendering it less compliant with Human Rights legislation. I understand that certain authorities do believe that there is a question there, but my personal view is that I do not think it is, by any means, clear that the 29(3) approach is unlawful."

58. The Home Office also did not share Law Enforcement's concerns. They agreed that access to communications data is an interference with an individual's right to privacy. However, they believe that this right is already being performed "by law", either under PACE, other Statutes or by requesting a CSP to make a disclosure within the meaning of s29(3) of the DPA. They stressed that it is of course essential that public authorities comply with the principles of the Human Rights Act and ensure that their actions are lawful, necessary and proportionate.

59. The Home Office also argued that the use of Part I Chapter II of RIPA was not a requirement to make access to communications data become Human Rights compliant – as the Law Enforcement evidence had suggested. What RIPA will do, they said:

> "is to place the duty to respect Convention rights firmly and more expressly with the public authority at the same time as removing the CSP from the decision to disclose personal data, and as ACPO rightly note, removing from CSPs potential liability to any civil action arising from 29(3) decisions to disclose personal data. However public authorities must respect Convention rights whether seeking disclosure under DPA now, or under RIPA in the future".

60. Besides this dispute over whether the current regime is lawful, we have noted all of the other concerns expressed by Law Enforcement and by industry. We agree that there can only be improvement by bringing RIPA Part I Chapter II into force and we are minded to recommend that this should be done as soon as possible.

61. However, we are also conscious that the existing regime has operated successfully for the 27 months since the Human Rights Act (and contemporaneously RIPA) came into force. We note that the recent work to enhance the process under 29(3) provides a RIPA regime in all but name. This leads us to the view that though changing to a RIPA regime is highly desirable, it is not extremely urgent.

62. We are also very conscious that the Home Office is about to consult widely on the specific matter of adding further public authorities and on the wider issue of how RIPA should be operated for the authorities that are on the face of the Act. We believe that activating this part of RIPA whilst this consultation is taking place would be to risk bringing the consultation into disrepute.

63. Accordingly, **we recommend that implementation of Part I Chapter II should be delayed until the responses to the Home Office's public consultation has been evaluated. It should then be brought into force as soon as possible thereafter, consistent with addressing the other issues that we highlight in this report – and that we expect the public consultation to demonstrate are of wide concern.**

Access to Data Subject Records

64. Several witnesses addressed the issue of data subject access and whether a data subject could or should learn that communications data relating to them had been passed to law enforcement.

65. The basic concern was that a customer could ask their CSP for a copy of the information held about them, which is a fundamental right under s7 of the Data Protection Act. If this information included the fact that, for example, the police had been asking for data, then there would be an obvious risk of compromising an ongoing investigation. If the investigation was complete then this risk would not arise, but of course the CSP would not be in a position to know when this had happened.

66. Industry did not have a uniform approach to what they recorded. Some did not keep records of the data flow any longer than would be needed for cost recovery. Others kept the record for a long period so that in the event of a dispute they would be able to show that their actions were justified.

67. Law Enforcement's view was that they would wish to be consulted before the subject was told any information about an investigator's access to their communications data so that they could act accordingly.

68. We were told that it would not be necessary, at least once RIPA Part I Chapter II is operating, to report the generic information that data may be passed to Law Enforcement. This is because s70 of the DPA excludes reporting upon recipients to whom data is provided because of a power conferred by law.

69. However, if a note is made on the individual's record about the circumstances of the data being passed then the situation becomes rather less clear, though there are relevant exemptions from the subject access provision under DPA s31.

70. **We recommend that clear guidance be sought by the Home Office, in conjunction with the CSP industry, from the Information Commissioner to clarify what should happen when a subject access request is made.** The guidance should make it clear to what extent the CSP can suppress information about Law Enforcement's interest in a customer's communications data.

71. The guidance should also cover the situation where the CSP has made further annotations to an individual's record. Because this data could be extremely sensitive, it would be of assistance to seek recommendations on how long this type of information should be retained.

72. When the guidance is given, it may be to the effect that subject access requests *should* disclose recorded information about Law Enforcement investigations. **We recommend that if the guidance means that responding to subject access requests could prejudice ongoing investigations then the Home Office should act expeditiously to address this issue, perhaps under DPA s38.**

73. Approaching the issue of subject access from a completely different direction, FIPR suggested that it should be compulsory to inform the data subject that their communications data had been accessed. They argued that this was an important safeguard that would trigger investigations within the supervisory regime when improper activity was occurring and would therefore bolster public confidence.

74. We shall have more to say about oversight below, but we do not agree with FIPR's suggestion. We believe that this approach would cause needless anxiety to considerable numbers of people who became marginally involved in investigations and are rapidly eliminated from enquiries. We do not accept that it would have the effect desired.

Adding Public Authorities to RIPA

75. In June 2002 the Home Office published a Statutory Instrument (SI) that would have added a large number of further public authorities to the current list in RIPA s25(1) of the organisations that can request communications data. In the face of considerable adverse comment they withdrew the SI a few days later. The Home Secretary undertook to consult widely on the issue before returning with new proposals. This consultation, which has already been referred to above, is expected to commence in the very near future.

76. The SI that was published only identified the public authorities to be added in a general manner. A second SI, that was never published, was to set out which specific senior officials would be entitled to issue requests. This would have had the effect of removing some smaller organisations from the list (because they did not have such senior ranks) and would have made it more clear which particular sub-sections of Whitehall departments or Local Government were intended to be given these new powers.

77. A number of witnesses referred to this issue of extra authorities. It was clear from the evidence we received that some organisations are still under the

impression that parish councils were to be allowed to access communications data, whereas we do not believe that was the Government's intention. We hope that the forthcoming consultation will be based upon detailed information and a clear enough explanation of what the Home Office is actually considering, so that meaningful responses will be received.

78. This clarity must continue if, as a result of the consultation, the Government brings forward fresh proposals. We believe that the Government significantly undermined public confidence by their initial failure to spell out the detail of their proposals and that the perception of blanket access to communications data was very damaging to public acceptance of what was proposed then and what might be proposed in the future.

79. **We recommend that the drafting of any future Statutory Instrument should have clarity as an important goal. We recommend that the authorisation levels be published at the same time as the list of authorities. We also strongly recommend that when the SI is published it should be accompanied by further explanatory documentation that has been written for the benefit of the general public.** There should be clear explanations not only of exactly what is being proposed, but also how the proposals reflect underlying policy decisions as to the appropriate balance between privacy and effective enforcement of laws.

80. We note that, although the Home Office would bring any future SI forward, there are significant inter-departmental issues involved. Careful attention must be given to "joined-up government" in ensuring that consistent standards of clarity and transparency are applied by all concerned.

81. As already indicated above, we do not consider it appropriate in this report to provide many recommendations on matters that will be addressed by the Home Office's public consultation. So we will not comment on whether particular public authorities should be granted powers under RIPA or what types of communication data they should be permitted to access. However, we do feel that it is entirely proper to comment upon the, essentially orthogonal, issues of SPOCs and the continued existence of "legacy" legislation that allows access outside the RIPA framework.

Single Points of Contact (SPOCs)

82. For reasons of efficiency and to prevent abuses, the CSPs have for several years insisted upon the use of a "single point of contact" (SPOC) scheme. The intention is that all requests for communications data from a particular police force will be channelled through a single office. The people in this office will be graduates of an in-depth training course and will be fully aware of the legal background and practical issues such as what information particular CSPs can provide and indeed, for a particular enquiry, which CSP should be contacted.

83. Several witnesses made the point that without the training involved in becoming a SPOC it was rather unlikely that requestors would be able to correctly judge what was "proportional" or indeed what was "reasonably practical".

84. Several witnesses were concerned about the potential for a large expansion in officials who would have powers under RIPA. Without a SPOC scheme it would be hard to maintain a list of the people who were authorised to serve notices and hence allow impersonators to be detected. UKERNA made this point in particular, because their constituency comprises a diverse group of universities and colleges that would not generally expect to receive large numbers of notices and hence would not develop sufficient practical experience to spot impostors.

85. SPOCs are currently used by the police, although some forces such as the Metropolitan Police have more than one SPOC! Gloucester Trading Standards has also been running what was effectively a SPOC for Trading Standards departments throughout the UK. However, this latter arrangement is currently being dismantled, partly for reasons of cost and partly because it will not be able to operate if (when) Trading Standards start to operate under a RIPA regime.

86. We accept the view of the CSPs that the existence of well-trained SPOCs is an essential part of the RIPA process. **We recommend that all authorities using RIPA to access communications data must be required to do this through a Single Point of Contact (SPOC).**

87. **We further recommend that arrangements be made to ensure that SPOCs will always be trained people ("graduates of SPOC school") and that their technical, legal and organisational training is maintained at the highest standards.**

88. Under RIPA there is a requirement that requests should only be made, and information returned to, a single public authority. It is not lawful for requests to be made on behalf of another agency. This means, for example, that adding all Trading Standards departments to s25(1) of RIPA would alone mean an increase in the number of SPOCs from the current count of 62 to about 500.

89. We were not told of any plans to train the large number of people involved in the expansion of RIPA, which would of course be essential, albeit expensive and time consuming. We also share the concerns expressed to us by several witnesses that the low volumes of requests passing through many of these new SPOCs would mean that they would not remain the centres of excellence that helps to justify their current existence within the police forces.

90. We recognise that data protection issues may arise when communications data is fetched by one organisation on behalf of another and that this was why RIPA is worded as it is at present. However, we consider it artificial to treat a large police force as a single unit whilst treating all the Trading Standards organisations in the same region as being a disparate set of authorities which must each interact separately with the CSPs.

91. **We recommend that the law should be amended to permit the creation of multi-agency SPOCs and that the low volume users of communications data should use these multi-agency institutions.** This amendment should maintain as far as possible the general data protection principles of limiting distribution that were behind the original RIPA approach. **We believe that this change can be made using the relatively new procedure of a Regulatory Reform Order and recommend that this "lightweight" approach to amendment should be used if possible.**

92. It was suggested to us that instead of having a single SPOC per police force it might be desirable to have a single SPOC per CSP. However, since CSPs differ significantly in size this would in practice mean considerable centralisation and so we do not accept this suggestion. We also note that when we asked the CSPs for their views, they could see little merit in the idea.

93. Although we believe that SPOCs should not become too small, we also believe that they should not become too large either. We believe that there is some value in diversity and significant merit in fragmenting the SPOC apparatus so as to build in barriers to the type of institutional corruption whereby unacceptable practices become the norm. **We therefore do NOT recommend the creation of a single SPOC to handle all non-police activity, but that an upper limit should be placed on the number of inquiries each multi-agency SPOC should handle, of perhaps 50,000 per year.**

Legacy Legislation

94. Some of the public agencies which the Home Office proposed to add to s25(1) already operate under existing legislation, as indeed do others that the Home Office were not intending to add. EURIM suggested that some authorities claimed access to stored computer data under powers that date back to World War II emergency legislation, before computers databases even existed.

95. A mobile company told us that they'd recently dealt with requests from the following list of authorities, citing legislation as given:

Charities Commission	Charities Act 1993
Environment Agency	Environmental Protection Act 1990
Health & Safety Executive	Health & Safety at Work etc Act 1974
Inland Revenue	Taxes Management Act 1970
Radiocommunications Agency	Wireless Telegraphy Act 1974 Telecommunications Act 1974
Serious Fraud Office	Criminal Justice Act 1987
Social Security Investigators	Social Security Administration Act 1992
Trading Standards Officials	Consumer Protection Act 1987

96. Although the Human Rights Act should restrict how legacy legislation is operated, legacy legislation does not contain the safeguards, accountability or robust Codes of Practice that are expected of a RIPA regime. We were told that some of these other agencies deliberately choose to use powers granted under their own legislation so as to avoid the cost recovery schemes that currently operate for the police and, as volumes are growing, this is clearly becoming a significant issue for the CSPs.

97. It was suggested to us that some organisations were hoping to get more powers under RIPA than were available under their existing legacy legislation, though perhaps "legacy" is an inappropriate term when some of this legislation post-dates RIPA. In particular, Social Security investigators, who received some new, but relatively circumscribed, powers very recently – in the Social Security Fraud Act 2001 – are said to welcome the further powers that RIPA could give them to access billing records.

98. We do not see this extension of powers as automatic or inevitable and believe that existing arrangements should not be changed without open debate and prudent consideration of whether a carefully judged existing balance should be disturbed. We draw particular attention to the possibility of restricting the types of communications data available to specific authorities.

99. We accept the argument made to us, by almost every witness, that there are significant merits to applying the RIPA regime to all of the organisations that request communications data from CSPs. Using RIPA will provide a formal framework for ensuring Human Rights observance. It will also ensure that the CSPs are properly reimbursed for their costs.

100. This does not seem to be contentious. The Home Office told us in their oral evidence; "our objective is that RIPA should establish a single regulatory regime for access to communications data for those authorities which are tasked with the investigation of crime".

101. As already indicated, we are deferring to the Home Office public consultation process as to which organisations should be included within RIPA directly. We also leave to this consultation what types of communications data should be available under particular authorisation schemes.

102. However, where the public consultation leads on to the decision that a particular public body should *not* be given access under RIPA then we consider it unacceptable that they should continue to have access under their own legacy legislation. For these bodies, we envisage a scheme whereby they would either work alongside another public authority, such as the police, or they would need to seek the approval of the courts for their actions.

103. Where access via RIPA *is* made available to a public authority, we do not believe that there is any benefit from using legacy powers from existing legislation, so this should be prohibited.

104. The net effect of the previous two paragraphs is that the only access to communications data should be via the RIPA Part I Chapter II regime. **We recommend the bringing forward of legislation to "ring fence" access to communications data so that it can ONLY be accessed by public authorities through the use of RIPA Part I Chapter II and hence use of other legislation would be ineffective.**

105. We note the large amount of "legacy legislation" that is involved and so we suspect that arranging to amend or override all of it might take some time to arrange, even if fast-track schemes such as Regulatory Reform Orders are appropriate. Therefore, as a practical way forward in the short and medium term, **we endorse the recommendation made to us by ISPA UK that a Memorandum of Understanding be developed whereby those public authorities who currently access communications data would renounce use of their legacy powers.**

106. When data is collected by one agency, we consider that it would be inappropriate to share this data with other agencies unless the RIPA compliant conditions under which it was accessed continue to be met. There are a number of statutory "gateways" in existence through which data could flow and of course Part III of the Anti-Terrorism Crime and Security Act 2001 created a whole series of

further gateways through which data could flow for the purposes, *inter alia*, of any criminal proceeding. **We recommend that the Home Office bring forward legislation to prevent agencies from deliberately avoiding RIPA controls by accessing communications data through a "statutory gateway".**

107. The Home Office policy is currently to add extra authorities to the list in s25(1) before bringing Part I Chapter II into force for all authorities at the same time. Although this approach has the virtue of simplicity, there must be expected to be further delays in setting up a suitable SPOC regime and addressing the matter of legacy powers. Therefore, **we recommend a separation between the issues affecting implementation of Part I Chapter II. The complications that will undoubtedly arise in adding further public authorities should not be allowed to delay addressing our previous recommendation regarding implementation for those authorities already on the face of the Act.**

Oversight and Punishment

108. It was common ground amongst the witnesses that it was necessary for the access to communications data to be regulated in such a way as to provide robust safeguards for Internet and telephone system users.

109. As already discussed the industry witnesses all took the view that SPOCs were an essential part of preventing fraudulent access to data. As this aspect of oversight has already been discussed, it will not be considered further here.

110. Part I Chapter II of RIPA will be overseen by the Interception of Communications Commissioner, currently the Rt Hon Sir Swinton Thomas. He is currently responsible for overseeing Part I Chapter I (the interception provisions). His latest annual report (for 2001) indicates that he envisages a "very substantial" increase in duties and "a very considerable extension" of his work. He states that "the extent and nature of the assistance that I will require is being considered by the Home Office in consultation with me and my staff".

111. In order to bolster public confidence in the oversight regime, **we recommend that the Home Office make an early statement on the assistance that the Interception of Communications Commissioner will receive.**

112. In his evidence Dr Pounder pointed out that the Interception of Communications Act Tribunal, which was the predecessor of the Tribunal set up under RIPA s65 had considered 400 cases between 1996 and 2000. None had been adjudicated in favour of the complainant. He observed that, "this 100% "perfection, like 100% support for Saddam Hussein in the recent 'presidential election' in Iraq, is simply not credible". Others have observed that the lack of knowledge about who actually has been intercepted may be contributing to these figures.

113. Dr Pounder also observed that the complaints system is fragmented and is riddled with overlapping and competing bodies. A hypothetical case, based in London and Northern Ireland that touched on personal data, national security and RIPA could require investigation by: the Information Commissioner, the Information Tribunal, the Information (National Security) Tribunal, the Security Service Commissioner, the Security Service Tribunal, the Secret Intelligence Service Commissioner, the Secret Intelligence Service Tribunal, the Interception of Communications Commissioner, the Interception of Communications

Tribunal, the Surveillance Commissioner, the Surveillance Tribunal, the Investigatory Powers Commissioner for Northern Ireland, and possibly the Police Complaints Authority.

114. Although we note that there is already some overlap in personnel between these posts and tribunals, we accept Dr Pounder's basic premise that this is a very confusing arrangement and that consideration should be given to simplifying these arrangements.

115. We note that some, but not all, of these bodies already operate websites describing their role and providing appropriate contact details. **We recommend that they all acquire a web presence as soon as practicable. We further recommend that the Home Office should host a general "one-stop-shop" website for the public (a "SPOC for Commissioners") providing links to the specialist websites, along with an indication as to their remit.**

116. EURIM told us that

> "those responsible for security in major international and financial services users are well aware of incidents in recent years where those in national security, law enforcement and other public sector agencies in the US and UK have abused positions of trust for personal gain. Some agencies are known to have internal processes that would not be tolerated by any private sector regulator, let alone a financial services regulator. There are similar issues with regard to some suppliers of security software (including encryption) and services."

117. EURIM also told us that one of their members "with branches in most high streets" passed requests for subscriber data to a central point for validation. When this central point interacted with the law enforcement agency SPOC to validate details of the request they found that many enquires "lapsed". EURIM said that, "there is no time or resource to check whether lapsed enquiries were attempts to gain data for the purposes of fraud or impersonation."

118. EURIM pointed out that publicity about wrongdoing was coming from the organisations with "better governance because they have processes for detecting the abuse". They said that, "the bigger issue is those where there is no publicity for abuse because there is no process for actually detecting abuse".

119. UKERNA were concerned that adding authorities to the s25(1) list would lead to a considerable risk of increased fraudulent demands for data. They stated that, "effective oversight and punishment of those who abuse the system are essential to maintaining public and jury confidence".

120. EURIM suggested the way forward was a well-publicised Code of Practice and greater transparency to allow reaction to potential as well as actual breaches. Effective processes were needed at all levels, combined with the taking of effective action against those in breach.

121. There are no specific offences in Part I Chapter II for unlawful access to communications data, and the only option for a CSP who suspects abuse appears to be that they should ask the Interception of Communications Commissioner to take note of what is occurring.

122. In oral evidence the Home Office stated that the approach to wrongdoing would be to see why the abuse was occurring and then prosecute that offence. If access were being abused to commit a fraud then the person would be charged with the fraud offence. Where there was no other offence then there would still have been an offence committed under the Data Protection Act.

123. We are deeply unimpressed by this approach. The specific abuse should be punished along with any other crime that has been committed. Resorting to the Data Protection Act is an unconvincing approach. Prosecutions under this Act are notoriously rare and the only sanction available to the court is a fine. **We recommend that the Home Office amend RIPA to provide for explicit criminal penalties for those who use s22 notices without proper authorisation or who deliberately abuse the system to obtain information to which they are not entitled.**

124. Dr Pounder drew our attention to the recommendation of the Lindop Committee on Data Protection that Codes of Practice should be created by (we would now say) the Information Commissioner rather than by the Home Office. This would remove the in-built bias that the Home Office, quite naturally, brings to the table of understanding the case for privacy invasion better than the case for privacy protection. Given that the Home Office has still not published their proposed Code of Practice for Part I Chapter II it is hard to believe that this procedure would have slowed anything down.

125. We see the merit in the Lindop Committee recommendation. However, RIPA requires the current arrangements. Therefore, as a practical way of improving public confidence, **we recommend that the Home Office formally consult with the Information Commissioner on the Part I Chapter II Code of Practice and publish the response.**

Anti-Terrorism Crime and Security Act 2001 (ATCS)

126. The Anti-Terrorism Crime and Security Bill passed through Parliament in the late autumn of 2001 in the aftermath of the "9/11" attacks. It received Royal Assent on the 14th December 2001. Part 11 of the Act is concerned with the retention of communications data by CSPs and s102 envisages the creation of a Code of Practice to which CSPs will voluntarily adhere. Further to this, the Secretary of State can enter into formal agreements with particular CSPs.

127. The provisions of the Data Protection Act 1998 and the Telecommunications (Data Protection and Privacy) Regulations 1999 (SI 2093) mean that communications data may not be retained by CSPs when they no longer have a business need to do so. For certain data, such as call records, this business need is specifically constrained by the legislation to be matters such as billing. Companies differ considerably in their arrangements, but in general records of telephone calls are kept for a year or so, but logs of usage of Internet services tend to be kept for very much shorter periods.

128. The Home Office is concerned that less data will be retained as business models change. If a phone company moved to flat-rate services then billing individual calls will no longer be necessary and so it can be expected that their records will only be retained for relatively short periods.

129. The intent of the ATCS legislation was to ensure that communications data would be available for Law Enforcement to access for a substantial period. In practice this would mean maintaining the status quo for some companies, but significantly extending retention periods for others, and in particular for most Internet Service Providers.

130. The Bill was originally worded so that data retention could be for the purposes of the prevention and investigation of crime in its generality. However, during the passage of the Bill through the House of Lords it was amended, by a large majority, to change the purpose of retention in s103(3) to:

> (a) for the purpose of safeguarding national security; or
>
> (b) for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security

131. Law Enforcement told us that they believed that this change had occurred because "insufficient emphasis was placed on the requirement of data for Crime purposes".

132. The Government accepted the Lords amendment, apparently because they believed that pretty much of all of the data would be kept for these national security reasons. This would mean that it would still be available as well for the more general crime related reasons. At the time, the Home Secretary David Blunkett told the Commons:

> "The amendment, in relation to part 11 therefore suggests that we should try to separate out those parts of data. As I tried to explain on a number of occasions, including last night, it is not possible to do that, but paradoxically, because it is not possible to do it, it is not reasonable to suggest that we should not do it. I am therefore prepared to accept the amendments that have been tabled. In order to be able to implement what they want, we will have to retain the data, so that it can be accessed to test out whether the intelligence services are right in believing that it is relevant in tackling terrorists. That is how stupid the Liberal Democrats are."

Voluntary Data Retention under ATCS

133. One of the other amendments made by the House of Lords was to require that the Information Commissioner should be formally consulted on the voluntary Code of Practice. In the Spring of 2002 the Information Commissioner sought legal advice on her response. The advice she received was that the provisions of ATCS made the retention of data lawful, because Parliament had made their own judgement that it was proportionate to do so for national security reasons.

134. In some people's view, Parliament was mistaken and the retention of communications data, even for reasons of national security, is not proportionate and therefore not "human rights compliant". Professor Walker and Dr Akdeniz provided us with a detailed analysis of the issues that needed to be considered, without coming to a definitive conclusion either way.

135. Leaving aside the issue of data retention *per se*, the Information Commissioner was advised that there was a further significant problem with ATCS, which arose whether the scheme was voluntary or compulsory. The communications data was being retained for a national security related purpose. However, RIPA s22 notices and indeed, as we have discussed at length, other legislative means, could be used to access it for other purposes as well. The Information Commissioner was advised that this access would be disproportionate and would therefore infringe the rights of data subjects under Article 8 of the European Convention on Human Rights.

136. Yet another Human Rights related issue then arose. The CSPs are fearful that should a data retention scheme be adopted, the courts would treat them as "public authorities" and so they – as well as any requesting authorities – would be laid open to action under the Human Rights Act. In his evidence, Dr Walden said that he thought this risk was small, but this was partly because of the legal position that if the ATCS Act itself was indeed not human rights compliant, then it would not be unlawful for the CSPs to comply with it.

137. Since these issues came to light, the Home Office has considered various options that might reconcile the ATCS framework with the Data Protection Act and Human Rights legislation. These other approaches have yet to be successful. In the Home Office's evidence they state that they will not proceed with a voluntary code if CSPs cannot operate it lawfully. They appear to be entirely alone in being confident that this can be achieved.

138. It might be thought that the solution would lie in proscribing access to the retained data via RIPA perhaps using s25(3)(b). However, this would not prevent access via other legislation or indeed through the civil law. Dr Walden told us:

> "You could not re-write RIPA to say 'This data is not accessible to a civil litigant who has a perfectly legitimate right'. I think the courts would find such provision in breach of Human Rights in the sense of a right to a fair trial, because that data exists and it could be accessed to be used in my defence against a legal action. Legislation preventing me to gain access to that data, I think, would be a breach of the Human Rights Act. They cannot close the gap. So there is a problem both ways. Because civil litigants have the right to access it, I believe the provisions are in breach of the European Convention on Human Rights. To try and plug that gap would, essentially, give rise to another breach of the Human Rights Convention, so it is the data retention provision per se which again cause the problems.

139. The CSPs told us, very frankly, that in their view the voluntary scheme was not going to be adopted by any part of industry. Although the Home Office acknowledged the problems that had arisen of proportionality, the risk of being treated as a public authority and the disparity of purpose with RIPA, no actual solutions were emerging.

140. The CSPs were also concerned about the financial impact upon the industry and were unimpressed by the continued uncertainty as to exactly what periods of retention would be required because the agencies could not agree what to ask for. The net effect was to create a situation where no one we talked to from industry could envisage recommending their boards of management to take the significant risks, legal and financial, of entering into a voluntary scheme.

141. In view of the clear evidence presented to us of its inevitable failure, we can see nothing to be gained from the spectacle of seeing a voluntary scheme proposed, approved by Parliament and then being ignored by the communications service providers. **We can reach no other conclusion than to recommend that the Home Office immediately drop their plans to introduce a voluntary scheme for data retention under ATCS.**

142. The structure of ATCS Part 11 means that it is necessary to take the formal steps of consultation and the assessment of the success of a voluntary scheme before the Secretary of State can consider whether or not to introduce a compulsory scheme. We leave the Home Office to determine the best way of meeting these statutory requirements in the light of our recommendation above and the further recommendations that follow.

The Cost of Data Retention

143. A very significant difficulty with the proposals for data retention has been the issue of costs. The legislation provides in s106 for CSPs to be reimbursed for the costs that they incur in complying with a voluntary Code of Practice or a compulsory direction. The Home Office has been allocated just over 20 million pounds for implementation of the data retention regime.

144. Orange pointed out that there was no explicit commitment to payment, the legislation leaves it to the Secretary of State to do what he “thinks appropriate”. The Home Office did however appear to be committed to spending the money that they had available. It was unclear if more money would be approved for new entrants to the market or if they would have to see this as the “price of doing business”. If the latter, then this would become a barrier to market entry.

145. Unfortunately, the Home Office funds appear to be entirely inadequate for the industry that currently exists. Many of the CSPs were waiting for firm proposals before attempting to quantify their likely expenditure. However, AOL told us that they processed 392 million user sessions a day, sending 597 million emails and estimated they would spend $40 million setting up a system and $14 million per annum in running it. THUS plc told us that within their business they could, at the upper end of what might be required, be looking at a five or six million pound project. When one considers the size of the rest of the ISP industry, let alone the fixed line and mobile telephone companies, it is entirely clear that the money available to the Home Office is totally insufficient. Sums well in excess of £100 million might well turn out to be necessary.

146. The Home Office does not accept these figures, suggesting that far lower sums will be needed. The disparity appears to arise because one side is calculating the cost of the raw disk storage, whereas the other is estimating on the basis of the need to build systems that can not only process the raw data but also provide

highly reliable and secure storage and retrieval. Some confusion clearly also arises because of doubt about exactly what must be stored, for how long, and how quickly retrieval should be managed. Though the figures we were presented with were clearly very rough estimates rather than anything exact, we have to accept that the CSPs do understand their systems and so we believe that the figures they propose are likely to be of the correct order of magnitude.

147. ISPA told us that although a considerable number of meetings had taken place over an eleven-month period, the legal issues had dominated these and as a result, "little time" had been spent so far upon technical and cost issues. From the disparity of the evidence we were presented with, this lack of discussion between the parties was quite apparent to us.

148. The projects that the CSPs say will be necessary to implement data retention and to allow prompt access to the data are of a significant size. The cost is not just in purchasing equipment, but in personnel costs as well. These projects will tie up staff resources and so they will not be available for other projects.

149. When businesses normally run projects of this size then there is an expectation that there will be a large "return on investment" in a relatively short time frame. However it is argued that the Act only permits cost recovery and no profit may be made. Therefore if, as is clearly envisaged, the Home Office does not provide money over and above the direct costs then the industry will under-perform financially as a result of implementing data retention.

150. At the beginning of 2002 the CSPs requested a "business case" from Law Enforcement in order that the industry might justify, at board level, their decision to commit to these substantial projects. They also wished to know what it was, in their current practices, that prejudiced national security. Human error appears to have delayed this request reaching Law Enforcement for six months, and it wasn't until September 2002 that a document was received and this did not really tackle these two requests. ISPA told us that it "failed to present a compelling case".

151. There appears to be a cultural difference here, because the CSPs clearly expected a document that set out a cost/benefit analysis giving projected figures for enquiries and indicating how various retention strategies would affect investigation success rates. What they received documented some specific cases (much along the lines of the information Law Enforcement provided to this inquiry) to demonstrate how telephone company communications data could be used to solve crimes. The document contained no figures or projections. It also concentrated on circumstances where data had been accessed after many months, far longer in fact than the retention periods that are being discussed under the ATCS regime.

152. The CSPs were generally unimpressed at the level of effort being expended by the Home Office in addressing ATCS implementation, describing it as "under-resourced and under-skilled". A single official had been responsible in the first part of the year and there were still only three involved. Whilst the RIP Bill was being created various Law Enforcement agencies had seconded staff to the Home Office so that their expertise had been available. This had not been the case with ATCS. The CSPs suggested that this was a contributory factor in the

failure to determine if it was necessary, whether it was proportionate and what the likelihood was of it delivering value for money.

153. We agree with the CSPs that at the current time, no quantitative case has been made for spending large sums of money on data retention. We also agree with them that given the huge impact this will have, any such case would have to be very compelling indeed.

154. There are a very large number of CSPs in the UK, of vastly varying sizes. There are no firm figures, but there are well over a thousand companies (and of course academic institutions) involved. Law Enforcement wishes all of them to adhere to similar data retention policies. However, the evidence given to us was that for many of these companies meeting the data retention requirements would involve them in the installation of entirely new systems.

155. Because many components of these systems would be almost independent of the company size, this would make the expense fall disproportionately upon the smaller players. Failure to reimburse all companies equally would affect the market competition, yet exempting the smallest companies with a view to improving the value for money aspect would not meet Law Enforcement's objectives because it could create "data havens" where much less data was available on wrong-doers.

156. The Home Office faced a similar dilemma of applying requirements (and funds) in a targeted way when implementing the interception ("tapping") requirements in RIPA s12. They achieved this by constructing a secret regime whereby it is an offence to discuss interception warrants and only the general s12 order is public. There is no similar secrecy scheme in ATCS, nor does it seem likely that with the huge number of communications data requests and the large number of public bodies involved that any such scheme could be kept secret for long.

157. In the past it has been suggested that if costs were too high then it might be desirable to save money by constructing "data warehouses" to hold the data from all CSPs in a single place. Industry did not believe that this would be lawful or desirable, FIPR went as far as to claim that these were exactly the tools needed to create a totalitarian state. Having heard these witnesses, we do not think this warehouse scheme is an avenue worth exploring.

Multi-national Aspects of Data Retention

158. Many of the CSPs that operate in the UK, particularly the mobile companies, are now multi-national organisations, often under foreign ownership. The economics of scale mean that there is an increasing trend to cross-border transfers of communications data to centralised systems.

159. If the regulatory cost of setting up these systems within the UK became higher than elsewhere then this would inevitably mean that less data was stored in the UK as systems migrated "off-shore". This was particularly relevant where new technologies were being deployed and the architecture was unlikely to heed national borders. For example, one mobile company told use they were considering a European wide billing system for 3G traffic. The cost, including of course the cost imposed by local regulations, would be a key part of the decision as to where this system would be sited.

160. Data held in "off-shore" systems is expected to still remain accessible to Law Enforcement but only through more complex, cross-border, procedures. Therefore the result of imposing a data retention regime under ATCS might be to make less data available to investigators rather than more.

161. ISOC England made the point that criminal elements were likely to use systems that were inherently "off-shore" such as satellite phones and foreign web-based email services.

162. Should it become known, perhaps as a side effect of a "subject access request", that communications data for a particular system was held off-shore in a different regulatory regime then criminals might use such a system in preference to domestic equivalents. This would further disadvantage Law Enforcement.

163. ISOC England observed that the definition of public communications service provider is very wide and could catch interactive gaming networks, club based wireless networks and even writers' circles. It seems to us that the Home Office does not propose to impose burdens on what are essentially private organisations, but their plans are certainly not expressed precisely enough to be absolutely sure of this.

164. However, in making a similar point EURIM suggested ATCS could embrace the Information Communications and Technology (ICT) operations of "almost any organisation, however modest, as well as data in transit through the UK or held overseas". This shows that there are policy issues on jurisdiction that should have been more clearly addressed by now.

165. Microsoft also thought it should be made clear to what extent ATCS sought to have an extraterritorial effect. They believed that such an aim would be unworkable because of the likelihood that different legal regimes would apply. They also worried that CSPs who were providing services beyond mere connectivity could well be unaware which country their users lived within. They felt the sensible approach was to have laws apply only to the CSPs physically located in a particular country.

166. CSPs owned by German companies already face internal difficulties in justifying existing "business needs" retention policies because German law is far more restrictive than the UK and therefore requires far more rapid deletion of communications data. German managers, we were told, are "horrified" at current UK practice.

167. Microsoft, whose software might be amongst the products which would have to be enhanced to meet regulatory requirements for data retention, was very concerned that ATCS should not mandate features that had to be available in UK systems. Such an approach, they told us, would freeze innovation and consumers would lose out on improved, less expensive, products and services.

168. Microsoft also noted that consumers were beginning to express significant privacy concerns with regard to what data is stored and for what purposes. They warned us

> "if these concerns are not adequately addressed, they will undermine consumer confidence in the Internet and impair the growth of electronic markets".

Compulsory Data Retention under ATCS

169. ATCS s104 provides that

> If, after reviewing the operation of any requirements contained in the code of practice and any agreements under section 102, it appears to the Secretary of State that it is necessary to do so, he may by order made by statutory instrument authorise the giving of directions under this section for purposes prescribed in section 102(3).

viz: if the voluntary scheme fails altogether, or as S A Mathieson suggested in the Guardian, the CSPs "don't volunteer enough", then the scheme can be made compulsory.

170. Not surprisingly, Law Enforcement told us that if a voluntary scheme did not work then a mandatory scheme should be put into place.

171. UKERNA told us that creating directions would be complex because of the different types of service provider and pointed out that whilst they hold some data, albeit not much, the customer identities are recorded by the academic institutions to which they provide service. In the Internet industry as a whole, 'vertical dis-integration' is leading to similar scenarios with "virtual ISPs" holding some records, the services they brand keeping other data and perhaps a bulk dialup connectivity service holding yet more information.

172. Microsoft pointed out to us that if *everyone* who was engaged in providing a telecommunications service was required to retain data then there would be considerable overlap in what was recorded and considerable unnecessary expense. They proposed that on the Internet it would only be appropriate to apply compulsion to ISPs because they would be the ones who captured the bulk of the information.

173. Looking to the future, ISOC England pointed out that the trend was to ever greater volumes of ever more ephemeral data. We are concerned about how a compulsory scheme will work in such a future. We believe that compulsion will destroy the existing collaboration we can discern between Government, Industry and Law Enforcement. Without assistance from industry, which they may not be motivated to provide, mandatory rules will fail to track technology change.

174. Exactly as the Information Commissioner had been advised in Spring 2002, Dr Walden told us that making data retention compulsory would not address the Human Rights issues:

> "I think the question of whether compliance with a voluntary or directed scheme is compliance with the Human Rights legislation is much of a muchness. I think the failure of the legislation is, again, not whether it is voluntary or mandatory but the interaction with the data access provisions under RIPA. The concern about voluntary is whether that exposes them to greater liability. I do not believe it does expose them to greater liability. The liability exists under a voluntary or a mandatory regime".

175. It is often said that modern communications, the telephone, mobiles and the Internet are so unlike anything else that constructing analogies is useless. Nevertheless, we consider it useful to consider the way in which larger

businesses may keep a record at reception of who has visited their premises and perhaps have some CCTV cameras to provide security. The ATCS mandatory retention provisions are just like insisting that every office in the country ensure that they have a 'visitors book' and a camera in every room. Furthermore, the book and the videotapes must be safely retained on the off chance that an investigator turns up to ask for the records from twelve months earlier. Of course we can appreciate that such a scheme would occasionally be useful to the police in solving an ancient crime, but we don't believe this usefulness would be so great that the imposition on businesses would be reasonable.

176. To recap, we have been told that a data retention regime will be immensely expensive and even with Government assistance on costs will consume engineering resources that the CSPs wish to devote to other, profitable, projects. We believe that it will be very hard to disburse money to the industry without significant market distortion and the creation of financial barriers to market entry. We are also convinced that the financial pressures will drive some data processing systems abroad and that mandatory policies will fail to track technology change. Finally, we note that there is significant doubt that the whole scheme is lawful.

177. Having considered all the evidence presented to us, we have come to the conclusion that a mandatory data retention scheme will do immense harm to the CSP industry and will not actually achieve the results wished for by Law Enforcement. Fundamentally, we do not believe that it is ***practical*** to retain all communications data on the off chance that it will be useful one day. We further believe that existing retention policies, driven by and funded by business needs, are currently proving to be adequate resources for the majority of investigations.

178. **We recommend very strongly that the Government do not invoke their powers under s104 of ATCS and impose a mandatory data retention scheme.** We note that under s105 these powers will lapse automatically on 14th December 2003, so no specific action will be required for this recommendation to be adopted.

Data Preservation

179. Data Preservation is the jargon term for obeying a request from Law Enforcement to keep certain communications data beyond the time when it would normally be destroyed or anonymised. It differs from data retention in being targeted at a specific type of data, a specific person or persons, or a specific time period. Access is still through the usual channels, but may not be immediate or indeed may turn out eventually not to be necessary at all.

180. The Council of Europe 'Cybercrime Treaty' requires that signatories set up a data preservation regime because cross-border requests for communications data under "Mutual Legal Assistance" provisions can take a long time. The data being sought may no longer assist if it has not been specially preserved until the disclosure notice has been authorised and served.

181. Data preservation does of course impose a cost on the CSP, but because it is specific, this is considerably less than a blanket data retention requirement.

182. We were told that data preservation had already been tried in the UK. Shortly after the 11th September 2001, UK CSPs were asked to voluntarily preserve data from the period around the attacks on the USA. The Information Commissioner was entirely satisfied that the request was lawful. The request to preserve the September data was eventually extended until the middle of February 2002. When writing to CSPs to say that the retention should lapse Detective Inspector Mike Ford of the National Hi-Tech Crime Unit said:

> "I thank you all, on behalf of the National Hi-Tech Crime Unit and the whole of the international law enforcement community, for your excellent co-operation with this enquiry. Whilst you will understand that I cannot give any information about the use made of the retained communications data, I can assure you that the existence of the data has been of significant benefit and value".

183. AOL has experience of data preservation schemes in the USA (where the PATRIOT Act passed after "9/11" did not include either voluntary or mandatory data retention). They told us that the system was less burdensome and less costly to business and consumers as well as being less harmful to public confidence. They proposed a study to determine how it would work in the UK.

184. Microsoft, another US based company, also endorsed data preservation saying that it "protects the privacy of innocent users while at the same time enabling law enforcement to fight crime effectively".

185. We recognise the concerns of Law Enforcement that as business needs for communications data change they cannot continue to rely on the data that they seek continuing to be available for long periods. However, we note the success of data preservation in the USA, the recommendations made to us by USA based companies, and how it worked successfully in the UK, even on a voluntary basis, in the aftermath of "9/11".

186. **We recommend that the Home Office enter into a dialogue with the CSP industry to develop an appropriate data preservation scheme to meet the needs of Law Enforcement.**

187. We have already touched upon the requests by many of the witnesses for international agreement upon a uniform approach to communications data policy and we have observed that the United States has chosen not to adopt a data retention policy, being content with their data preservation regime. However, there are various moves in Europe towards creating a consistent policy of data retention throughout the European Union (EU).

188. However, Law Enforcement told us that it had "proved difficult to the point of impossibility" to achieve a consistent policy because of the differing legal systems and access provisions in EU member states. The Home Office agreed, albeit more diplomatically, referring to "issues about the cultural approaches they have [..] and the legal traditions which they have, which means they all come at it in slightly different ways".

189. We believe that exactly the same considerations that we have already identified as ruling out the ATCS data retention regime are applicable elsewhere in Europe. We therefore believe that moves in other EU states towards a data retention policy are entirely mistaken. In particular, we believe that saddling the entire European CSP industry with costs that do not have to be incurred by their American competitors will cause immense damage. **We recommend the Government urgently enter into Europe-wide discussions to dismantle data retention regimes and to ensure that data preservation becomes EU policy.**

190. We are conscious that our recommendations for ATCS mean a significant change in policy, moving from Data Retention to Data Preservation. We are sure that it is the right and practical thing to do, but we recognise that it will require some realignment by the Law Enforcement agencies. **We recommend that a body such as the Intelligence and Security Committee should look into the ramifications of this policy change** and accordingly, we have sent a copy of our report to Ms Ann Taylor, its chair.

International Co-operation

191. In their evidence, EURIM stated that:

> "the UK subsidiaries of major US financial institutions have expressed concerns that a combination of UK law and loose statements on 'mutual assistance' may be used by their own Federal or State Governments, let alone other national Governments, to gain accesses which would not be permissible under US domestic law".

192. Several witnesses made the related point that questions of jurisdiction might arise. Some concept of "country of origin" for communications data might be of assistance in clarifying access provisions.

193. FIPR noted that the Government signed the Council of Europe's Cybercrime Treaty in November 2001, though it has yet to be ratified by the UK. As already discussed above, the treaty prescribes a data preservation regime and for foreign law enforcement agencies to access this data under "Mutual Legal Assistance" provisions. As presently operated, Mutual Legal Assistance relies upon its extended time-scale to ensure that we do not assist foreign governments whose policy objectives we disagree with. For example, the UK may not recognise the offence, the UK may be supporting opposition groups, or the evidence gathered might be used to secure a conviction leading to capital punishment.

194. The Cybercrime Treaty goes further than the existing Mutual Legal Assistance regime, in also providing for "expedited" preservation and disclosure. This could mean that data was shipped abroad only a few minutes after it was collected. FIPR believes that this raises considerable practical difficulties in ensuring that UK public policy objectives continue to be maintained. ISOC England raised a related point, that there was the potential for UK companies to have to subsidise the costs of preservation and disclosure, to the benefit of foreign law enforcement agencies.

195. We recognise the concerns raised with regard to the Cybercrime Treaty and the EU "Council Framework Decision on Attacks Against Information Systems" and note with approval that the Home Office is already beginning to study this topic internally. **We recommend that the Home Office study specifically addresses the public policy and internationalisation issues that arise in the context of communications data.**

General

196. As is inevitable, some of the issues on which we received evidence, and which we agree are important, do not fit into tidy categories, nor are they specifically concerned with particular pieces of legislation. This final section of our report covers these topics.

197. EURIM drew attention to the problems caused by the way in which the civil service personnel policies for career development meant that staff were rotated through a series of posts. With deeply technical issues such as those surrounding communications data, it took considerable time for officials to understand the technicalities and what measures might be practical. By the time a policy had reached the implementation stage they would have been replaced by someone who was entirely unaware of the reasoning behind particular arrangements. EURIM believed that RIPA would make a particularly good case study where the problems are particularly acute. **We agree with EURIM's recommendation that the Select Committee on Public Administration be asked to consider this topic as one aspect of the general problems with policy formation.**

198. ISPA considered that it was important for the Government and Law Enforcement to work in partnership with industry because "invaluable expertise" could be provided on technical feasibility, practicality and cost. EURIM noted the US scheme whereby individuals from industry were regularly seconded to Law Enforcement Agencies as reservists, deputies or specials to provide specialist expertise for particular investigations. We have already noted the Government/Industry forums and that there appears to be considerable assistance being provided by industry to Law Enforcement training. ACC Gamble told us that Law Enforcement sought specialist assistance where they could, "either through the provision of specialists in the Armed Services and other specialist bodies [..] or through our relationship with industry itself". **We have no hesitation in recommending that the existing links between Law Enforcement and industry are continued, broadened and deepened.**

199. Many of the issues addressed by this report are affected by rapid technological change, which may in time affect the balance to be struck between the powers we give to Law Enforcement and the privacy which the public can expect. It would be very desirable for these issues to be revisited on a regular basis. **We recommend that the Government hold an annual debate, in both Houses of Parliament, on privacy matters.** It might be appropriate to tie this in to the data protection aspects of the annual report from the Information Commissioner.

Summary of Recommendations

#17 **We recommend that a formal statistics gathering process be put in place so as to determine the scope of access to communications data and its direct costs.**

#21 **We recommend that the Home Office supervise a regular, formal, technical assessment of the state of this technology 'war' and the overall effectiveness of the use of communications data in crime-fighting.**

#24 **We recommend that the Home Office should ensure that they seek the views not only of Law Enforcement and the communications industry, but also independent views from academia and from the relevant technology developers themselves.**

#44 **We strongly recommend that, as a part of their forthcoming consultation, the Home Office should seek to establish better definitions for the different types of communications data.**

#45 **We recommend that if the Home Office consultation shows that it is desirable to amend the definitions within RIPA s21(4) then appropriate legislation should be brought forward as soon as is practicable.**

#46 **We recommend that the Home Office ensure that their forthcoming consultation seeks to determine whether the public agrees that access to communications data for "predictive" purposes should be subject to special controls.**

#63 **We recommend that implementation of Part I Chapter II should be delayed until the responses to the Home Office's public consultation has been evaluated. It should then be brought into force as soon as possible thereafter, consistent with addressing the other issues that we highlight in this report – and that we expect the public consultation to demonstrate are of wide concern.**

#70 **We recommend that clear guidance be sought by the Home Office, in conjunction with the CSP industry, from the Information Commissioner to clarify what should happen when a subject access request is made.**

#72 **We recommend that if the guidance means that responding to subject access requests could prejudice ongoing investigations then the Home Office should act expeditiously to address this issue, perhaps under DPA s38.**

#79 **We recommend that the drafting of any future Statutory Instrument should have clarity as an important goal. We recommend that the authorisation levels be published at the same time as the list of authorities. We also strongly recommend that when it is published it should be accompanied by further explanatory documentation that has been written for the benefit of the general public.**

#86 **We recommend that all authorities using RIPA to access communications data must be required to do this through a Single Point of Contact (SPOC).**

#87 We further recommend that arrangements be made to ensure that SPOCs will always be trained people ("graduates of SPOC school") and that their technical, legal and organisational training is maintained at the highest standards.

#91 We recommend that the law should be amended to permit the creation of multi-agency SPOCs and that the low volume users of communications data should use these multi-agency institutions. We believe that this change can be made using the relatively new procedure of a Regulatory Reform Order and recommend that this "lightweight" approach to amendment should be used if possible.

#93 We therefore do NOT recommend the creation of a single SPOC to handle all non-police activity, but that an upper limit should be placed on the number of inquiries each multi-agency SPOC should handle, of perhaps 50,000 per year.

#104 We recommend the bringing forward of legislation to "ring fence" access to communications data so that it can ONLY be accessed by public authorities through the use of RIPA Part I Chapter II and hence use of other legislation would be ineffective.

#105 We endorse the recommendation made to us by ISPA UK that a Memorandum of Understanding be developed whereby those public authorities who currently access communications data would renounce use of their legacy powers.

#106 We recommend that the Home Office bring forward legislation to prevent agencies from deliberately avoiding RIPA controls by accessing communications data through a "statutory gateway".

#107 We recommend a separation between the issues affecting implementation of Part I Chapter II. The complications that will undoubtedly arise in adding further public authorities should not be allowed to delay addressing our previous recommendation regarding implementation for those authorities already on the face of the Act.

#111 We recommend that the Home Office make an early statement on the assistance that the Interception of Communications Commissioner will receive.

#115 We recommend that [the Commissioners] all acquire a web presence as soon as practicable. We further recommend that the Home Office should host a general "one-stop-shop" website for the public (a "SPOC for Commissioners") providing links to the specialist websites, along with an indication as to their remit.

#123 We recommend that the Home Office amend RIPA to provide for explicit criminal penalties for those who use s22 notices without proper authorisation or who deliberately abuse the system to obtain information to which they are not entitled.

#125 We recommend that the Home Office formally consult with the Information Commissioner on the Part I Chapter II Code of Practice and publish the response.

#141 We can reach no other conclusion than to recommend that the Home Office immediately drop their plans to introduce a voluntary scheme for data retention under ATCS.

#178 We recommend very strongly that the Government do not invoke their powers under s104 of ATCS and impose a mandatory data retention scheme.

#186 We recommend that the Home Office enter into a dialogue with the CSP industry to develop an appropriate data preservation scheme to meet the needs of Law Enforcement.

#189 We recommend the Government urgently enter into Europe-wide discussions to dismantle data retention regimes and to ensure that data preservation becomes EU policy.

#190 We recommend that a body such as the Intelligence and Security Committee should look into the ramifications of this policy change.

#195 We recommend that the Home Office study specifically addresses the public policy and internationalisation issues that arise in the context of communications data.

#197 We agree with EURIM's recommendation that the Select Committee on Public Administration be asked to consider this topic [the effect of civil service career rotation] as one aspect of the general problems with policy formation.

#198 We have no hesitation in recommending that the existing links between Law Enforcement and industry are continued, broadened and deepened.

#199 We recommend that the Government hold an annual debate, in both Houses of Parliament on privacy matters.

Appendix A: Press Notice & Guidelines for Witnesses

15th November 2002
For immediate release

Press Release

All Party Internet Group to hold public inquiry into the retention of and access to communications data for law enforcement purposes

The All Party Internet Group (APIG) is to hold a public inquiry into all aspects of communications data retention and the subsequent access to that data from a UK, European and global perspective. The inquiry will primarily focus on the enforcement of the powers contained in the Regulation of Investigatory Powers Act and the Anti-Terrorism, Crime & Security Act and their subsequent effect on communication service providers.

APIG calls on communication service providers to present written evidence to the inquiry before December 6th 2002. Public hearings will be held in the House of Commons on the 11th & 18th December when MPs will hold oral evidence sessions with industry, Government and other interested bodies. The group will publish a report on their findings early next year, likely to contain a number of recommendations to Government.

Joint Chair of the All Party Internet Group, Richard Allan MP, said: "The raft of legislation and associated issues which communication service providers now face are daunting. What data should be retained, how it is accessed and retained, the cost of retention and conforming with multiple legal commitments are just some of the serious issues facing law enforcement agencies, industry and legislators alike."

Brian White MP, Treasurer of APIG, said: "This inquiry will cut across traditional departmental remits to examine in detail a multifarious but hugely important issue that has connotations for the whole of society"

He added: "I am very much looking forward to what will I know will be a interesting and beneficial inquiry to all parties involved."

Specifically the inquiry will examine:

- The powers incorporated in the Regulation of Investigatory Powers (RIP) Act 2000, Part I Chapter II;
- The voluntary and compulsory data retention regimes found in Part 11 of the Anti-terrorism, Crime and Security Act 2001;
- Other relevant legislation and European Directives such as:
    - The Data Protection Act 1998,
    - The Telecommunications Privacy Directive EU 97/66/EC,
    - The Data Retention provisions of the EU 2002/58/EC, the recently adopted "Electronic Privacy" Directive;

    - The Data Retention, Preservation and Partial Disclosure regimes in the Council of Europe Convention on Cybercrime;
- The extent to which communications data is held outside the direct control of Communications Service Providers (CSPs) and how this should be addressed;
- The value of communication data access to Law Enforcement Agencies, the types of data that are of importance and the periods for which it should be retained;
- The value of access to retained data by further authorities beyond those currently authorized by the RIP Act;
- The difficulties faced by Law Enforcement Agencies in conforming with existing legislation;
- The mechanisms that should be put in place to allow expedited data preservation and partial disclosure of traffic data to Law Enforcement Agencies in foreign countries;
- The costs to the CSPs of retaining communications data and in providing access to retained data;
- Competition issues for CSPs;
- Privacy Issues.

Written evidence should be submitted to inquiry@apig.org.uk by 6th December 2002. APIG may, at their discretion, as for oral evidence from witnesses on the mornings of 11th and 18th December 2002 at the House of Commons. The inquiry's report is expected to be published in late January 2003.

Note to Editors:

Richard Allan MP is the Liberal Democrat IT spokesman and represents Sheffield Hallam.

Brian White MP is a leading Labour backbencher on technology issues representing Milton Keynes.

The All Party Internet Group exists to provide a discussion forum between new media industries and parliamentarians. Accordingly, the group considers Internet issues as they affect society informing Parliamentary debate through meetings, informal receptions, inquiries and reports. The group is open to all members of the Houses of Parliament.

The Members of the inquiry are yet to be confirmed but will include Richard Allan MP & Brian White MP.

Enquiries about the work of the Committee:
Telephone: 020 7233 7322
Fax: 020 7233 7294
e-mail: inquiry@apig.org.uk

APIG Inquiry: Guidelines for Witnesses

The All Party Internet Group announced an inquiry into "Communications Data: Retention and Access" on 15th November 2002. The inquiry is anxious to receive as wide a range of submissions as possible.

1. More information about APIG can be found at http://www.apig.org.uk

2. Recent documents of relevance to the inquiry include:

    - Regulation of Investigatory Powers Act 2000
      http://www.hmso.gov.uk/acts/acts2000/20000023.htm

    - Anti-terrorism, Crime and Security Act 2001
      http://www.hmso.gov.uk/acts/acts2001/20010024.htm

    - Data Protection Act 1998
      http://www.hmso.gov.uk/acts/acts1998/19980029.htm

    - Human Rights Act 1998
      http://www.hmso.gov.uk/acts/acts1998/19980042.htm

    - Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
      http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html

    - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
      http://www.oftel.gov.uk/ind_info/eu_directives/data0702.pdf

    - Council of Europe Convention on Cybercrime
      http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185

3. Members of Parliament daily receive a mass of papers. If a memorandum is to command their attention, it should be brief and to the point. In particular, it should address the matters raised by the inquiry and concentrate on the issues with which the witness has a special interest. A typical length would be about 1,000 words. Essential statistics or further details can be added as appendices.

4. It would be greatly appreciated if memoranda could be submitted electronically either in plain ASCII, Adobe PDF format or in Microsoft Word .DOC or .RTF format. Ideally, pages and paragraphs should be numbered. Memoranda should be dated, with the name, address and telephone number of the person in the organization who is responsible for submission given at the end. Memoranda should be submitted to the address at the end of this notice.

5. It is at the inquiry's discretion to print any evidence it receives. Any information that a witness would not wish to be considered for publication should be clearly marked.

6. The inquiry has asked for all written evidence to be submitted by 6 December, although extensions to that deadline will be considered. The inquiry may decide, having read a memorandum, to invite a witness to give oral evidence.

Evidence may be submitted to:

APIG Secretariat,
23 Palace Street,
London, SW1E 5HW.

inquiry@apig.org.uk

Electronic submissions (in plain ASCII, Adobe PDF or Microsoft Word .DOC or .RTF formats) are preferred and can be emailed to inquiry@apig.org.uk

Appendix B: Glossary of Terms

ACC
Assistant Chief Constable

ACPO
Association of Chief Police Officers

AOL
A large ISP operating at a global level (originally "America Online")

APIG
The All Party Internet Group
a discussion forum for Parliamentarians and the new media industries.

ATCS
Anti-Terrorism Crime and Security Act 2001

CCTV
Closed Circuit Television, a surveillance technology.

Cell site data
Information that indicates the geographical location (cell) where a mobile telephone has been used.

CSP
Communications Service Provider
generic term for telephone companies and also Internet Service Providers

Cybercrime Treaty
An international treaty that is intended to provide a consistency in approach to crime on the Internet and assist in its investigation.

DPA
Data Protection Act 1998

EU
European Union

EURIM
European Information Society Group
an all-party pan-industry “lobby” for the Information Society and E-Commerce.

FIPR
Foundation for Information Policy Research
a “think tank” studying the interaction of Information Technology and society.

ISOC England
Internet Society of England
“representing a cross-section of the Internet community”

ISP
Internet Service Provider

ISPA
Internet Service Providers Association UK
a “trade body” for the UK ISP industry.

Law Enforcement Agency
Generic term usually reserved in this document for the Police, Customs & Excise and the Security Services.

Legacy legislation
Term used in this document for Acts of Parliament that give powers to access communications data outside the RIPA framework.

Mutual Legal Assistance
Procedures for providing evidence to foreign Law Enforcement Agencies.

NCS
National Crime Squad

PACE
Police and Criminal Evidence Act 1984

Part I Chapter II
Sections 21-25 of the Regulation of Investigatory Powers Act dealing with the acquisition and disclosure of communications data.

PIU
The Cabinet Office Performance & Innovation Unit now merged into the Cabinet Office Strategy Unit.

RIPA
Regulation of Investigatory Powers Act 2000

SI
Statutory Instrument

SPOC
Single Point of Contact
a department that deals with communications data requests made by a public body, such as the police, to a communications service provider.

Steganography
A technique for hiding data within an otherwise innocuous transmission, document or picture.

UKERNA
Trading name of the JNT Association, which operates the JANET network connecting UK academic institutions together and to the public Internet.

URL
Uniform Resource Locator, such as a web address in the form
http://www.example.com/

3G
"Third Generation" mobile telephone standards.


APIG
ALL PARTY INTERNET GROUP