Joint Committee on the Draft Communications Bill

SUBMISSION OF PROFESSOR PETER SOMMER

Summary

This submission concentrates on the technical feasibility and efficacy and value for money of the policies behind the draft Bill. The Bill's aim is to realise the ambitions of the Home Office's Communication Capability Development Programme (CCDP).

The role of retained communications data in investigations needs to be understood within the broader context of all the available potential strands of evidence available for consideration. The ever wider use of computers and telecommunications by individuals, businesses and governments has had a transformative effect on many types of criminal and intelligence investigation. Retained communications data is but one element and while over time some forms are becoming less available, this loss is more than balanced by the increased availability of other types of digital evidence.

The precise problems associated with communications data are best addressed by looking at the various types of Communications Service Provider and the classes of data they might retain. The globalised percentages approach of the Home Office misleads. Many forms of communications data will continue to be available for the foreseeable future without new legislation, while others are held by businesses outside the easy jurisdiction of the UK courts, raising the question of how UK laws, orders, and court decisions can in practice be enforced.

A key requirement of any law is that it is easy to interpret. It is now increasingly difficult to align and interpret the legal definitions of "communications data" and "content" with the complex ways in which data is transmitted over the Internet. Resort must be made to expensive hardware to apply a very large number of technical filters which are supposed to reflect the statutory definitions. These filters must be constantly updated and added to, to reflect the incredible dynamism of the Internet. Even then one can anticipate some of these will require testing in the courts. The complexity and difficulties also have an impact on the extent to which Parliament can be expected to scrutinise the Orders contemplated in Part 1 of the Bill, and to which the regime can be effectively overseen by the Interception of Communications Commissioner.

The penalties for incorrect separation of communications data from content fall chiefly on the police. The regimes for access are very different – interception of content requires a warrant

from the Secretary of State, communications data an authorisation from a senior designated officer. Communications Service Providers are *de facto* protected from mistakes, but police who have acquired material *ultra vires* will find themselves in difficulties, not the least at disclosure and the possibilities of arguments about abuse of process. The problem is significantly compounded by the UK's almost unique position in treating intercepted content as inadmissible and not referable to in legal proceedings.

The Request Filter proposals in cl 14-16 appear to be an attempt to overcome the twin problems of interpretation and the two entirely separate regimes for communications data and the interception of content. But making this a function, direct or delegated, of the same Secretary of State who also issues interception warrants and Orders under the Draft Bill is surely a mistake; if there is to be a credible and viable independent filtering agency much more needs to be said about its resources and governance.

The costs of the Home Office's proposals are impossible to calculate as there are too many unknowns but it is possible to identify criteria for likely value for money. Neither the Explanatory Notes nor the Impact Assessments discuss the source of funding but it seems reasonable to assume that in the current economic climate funding will have to come from existing resources. It is thus useful to seek to evaluate the role of the features of retained communications data that would be enhanced were the Home Office's proposals to be accepted against the loss of some funding to other existing forms of investigative activity and evidence.

Those who seek to avoid having their Internet activities being monitored will have a number of easy routes, even after significant public expenditure on the CCDP. There is a danger that CCDP will have ever-expanding technical ambitions as the Internet changes which, coupled with the need for secrecy, will lead to runaway costs.

I suggest that ways forward include:

- bringing interception evidence back into admissibility so as to simplify many of the technical interpretative problems the draft Bill creates
- continuing the current position that the requirements of domestic CSPs to retain communications data is limited to records they create as part of their regular business activities
- a substantially revised system for the issuing of warrants and authorisations coupled with more robust and credible forms of oversight, so as, among other things, to persuade critical non-UK-based Communications Service Providers to accede to the requests of the UK authorities.

This submission concentrates on the following questions in the Joint Committee's Call for Evidence: 1, 2, 5, 6, 11, 13, 17, 18, 19, 22, 24, 25, 26.

References to comments made in earlier oral evidence sessions are to the uncorrected versions published on the Joint Committee's website.

CV

1. I am currently a Visiting Professor at de Montfort University and a Visiting Reader at the Open University. For 17 years I was first a Visiting Research Fellow and then a Visiting Professor at the London School of Economics. My academic specialisations are cyber security, cybercrime, digital evidence and cyberwarfare.

2. I have acted as an expert witness , for both prosecution and defence, in many trials involving complex computer evidence since 1994. They include: global hacking, terrorism, "phishing", software piracy, murder, large scale illegal immigration, narcotics trafficking, art fraud, state corruption, money laundering and paedophilia. The computer evidence has included the examination of hard disks and other media, the interpretation of network traffic, Internet-related artefacts and communications data. I have also been instructed, in the UK and abroad, in cases involving intercept evidence, including to ETSI standards.

3. My practical work as an expert witness has brought me into frequent and direct contact with many specialist police units. I have provided advice for the UK's National High Tech Crime Training Centre, was the external evaluator and then external examiner for the MSc in Computer Forensics at the Defence Academy which is widely used for police training and while it existed I was the Joint Lead Assessor for the digital element in the Home Office-backed Council for the Registration of Forensic Practitioners.

4. Based both on my academic research and my practical experience, I hope to be able to assist the Committee. I make this submission in a personal capacity. A full CV is available at http://www.pmsommer.com/PMSCV012012_std.pdf

Digital Evidence Landscape

5. The requirement for and cost-justification for an enhanced regime for retained communications data needs to be tested in the context of the vastly increased range and extent of many types of digital evidence available to the UK authorities since the passing of the Regulation of Investigatory Powers Act 2000 (RIPA).

6. Over 75% of the UK population have access to the Internet from their home and each UK household on average owns three Internet-enabled devices[1]. Nearly 80% have at least one home computer[2]. Costs of hard disk storage fall by 50% every 18 months – a 1000GB (1 TB) hard disk now costs about £60 - so that in a typical police search warrant execution on domestic premises they can expect to find several PCs of various vintages, plus external data storage devices such as disks and USB memory sticks. There are 130 mobile phone contracts per 100 of the population, 39% of

[1] Ofcom, Q2012, http://media.ofcom.org.uk/facts/
[2] ONS, Selected Consumer Durables, http://www.ons.gov.uk/ons/rel/family-spending/family-spending/family-spending-2011-edition/sum-consumer-durables-nugget.html

them smartphones, in effect powerful ultra-portable computers[3]. Nearly all of these devices contain substantive files, copies of emails sent and received and histories of such Internet activity as websites visited, pre-occupations of and research carried out by the owner. PCs may also contain artefacts relating to other types of Internet services used, complete with user names and passwords. They may also provide strong evidence of persons with whom the computer owner has been in contact. All mobile phones will contain some records of calls made and received and copies of SMSs made and received – Ofcom says 200 SMSs are sent per person per month[4] . Smartphones will contain much more recoverable data.

7. All of these are key sources of digital evidence and none fall within the regime of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Draft Bill, which are solely concerned with data in the course of transmission. Significant types of evidence that can be obtained under RIPA powers can also be found on seized PCs and mobile phones; and the recovered data will have a considerable historic element because of the capacity of the associated storage devices. Computers and mobile phones are normally seized under powers within Part II of the Police and Criminal Evidence Act, 1984 (PACE) but there are also many additional powers in other legislation[5]. Whereas the RIPA route will exclude "content" for admissibility purposes[6], the same material if found on a hard disk is fully admissible.

8. Over the last 12 years, since RIPA came into force, the amount of information collected by commercial bodies about individuals has increased greatly, chiefly through "get to know your customer's interests better" Customer Relationship Management (CRM) software and the development of commercial credit and marketing databases.[7] Commercial marketing-type data can be bought by law enforcement agencies on commercial terms, privately-held data can be acquired via Production Orders under PACE, subject to the provision of a certificate under s 28 or 29 of the Data Protection Act 1998. [8] The same route can be used to obtain information about banking and credit card transactions – credit and debit card data may also contain information of the location at which a transaction took place.

9. At the same time the availability of Closed Circuit Television (cctv), both officially and privately owned, has expanded greatly, both in the quantity of cameras[9] and their locations and in the quality of images. [10] . The UK's National Policing Improvement Agency operates a national DNA database, which is one of the world's largest, with profiles on an estimated 5,570,284 individuals as of 31 March 2012. It also operates a national automated number plate recognition system, which by March 2011 was receiving 15 million sightings daily, with over 11 billion vehicle sightings stored. A

---

[3] Ofcom *Communications Market Report 2012*
http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_0.pdf
[4] http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_0.pdf
[5] Eg s 14 Computer Misuse Act 1990 and s 114 Finance Act, 2008
[6] S 17 RIPA 2000
[7] Eg DataHQ, Experian, Equifax. http://www.graydon.co.uk/, http://www.world-check.com/
[8] See also *Government Access to Private-Sector Data*, Brown, International Data Privacy Law, 2012 (in press)
[9] Cheshire Constabulary estimated in 2011 that there are 1.85m CCTV cameras in the UK, 1.7m of which are privately owned
[10] See BBC research in 2009 on the density of local authority-owned cctv cameras: http://news.bbc.co.uk/1/hi/uk/8159141.stm and a Channel 4 News assessment that in 2008 there was a cctv camera for every 14 citizens.
http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167.html

national fingerprint database contained 8.3m individual's prints in April 2010. [11]Another new-ish method for tracking the movements, at least of people in London, is via the Oyster card[12].

Types of Communications Service Provider

10. There are several distinct types of organisation and business subsumed under the phrase "Communications Service Provider". By identifying them we can more easily see what potential evidence they might produce, what role that evidence could have in investigations and what obstacles the authorities may encounter. Several important forms of communications data are not under threat of diminution in value as a result of technological developments.

11. Individual businesses may offer combinations of these roles and there may also be a limited amount of blurring of functionality.

12. **Telcos** These are the conventional telephone companies, offering either fixed or mobile services. In terms of communications data, they use and all telcos can provide: the identity of subscriber [13]and for each call: counter-party number, time and duration of call. Mobile phone companies can also provide location data (which is based on the technical requirement for the mobile phone system to know where each of its subscribers' phones is located so that they can be actuated to receive an incoming call). Mobile phone call data records also include the hardware identity of the handset (IMSI) and the SIM in use (IMEI).

13. All telco-related communications data is useful in building up patterns of calls between parties, perhaps to show some form of conspiracy; mobile phone location data additionally shows the movements of a cellphone owner by time over a landscape. Police routinely use special link analysis software to show the patterns of usage[14] and a number of companies also offer Cell Site Analysis to show patterns of movement. Although some fixed line calls may over time migrate to Internet-based telephony (VOIP, Skype), the use of mobile phones is unlikely to diminish and however these phones are used, so long as they are switched on, they will continue to deliver location data.

14. **Network Access Providers** This is what most people regard as Internet Service Providers. The core service is to give the subscriber some form of box (hub) through which the Internet may be accessed. The actual service may be superimposed on a conventional telephone line or entertainment tv cable, or may involve a dedicated line, perhaps fibre. A Network Access Provider (NAP) usually thinks of itself as a conduit. In addition to the basic facility there will usually be others, to handle conventional email, to improve the experience of using the world wide web (for example by

[11] www.npia.police.uk
[12] http://news.bbc.co.uk/1/hi/england/london/4800490.stm
[13] But not for PAYG customers; additional forms of matching are needed to identify them
[14] eg I2; http://www.i2group.com/uk

caching), and the same business may also offer its subscribers hosting facilities, for example to provide a base for a web-server from which the subscriber can publish their own information.

15. NAPs can provide: details about their subscribers[15] and also which of their subscribers held which IP addresses at particular points in time.[16] The latter is especially important as the originating IP address of a communication is routinely gathered in many types of Internet transaction such e-commerce, e-banking, use of file-sharing services, and it then becomes possible to associate the IP address with a subscriber or an individual. The NAP also provides a very convenient collection point at which to monitor the activities of their subscribers, subject to legal constraints. Nearly all large NAPs will have already have installed Lawful Intercept facilities (as required under s 12, RIPA, 2000) and they are also the logical place where any filtering to retain communications data might take place.

16. Under the Bill NAPs will bear the burden of carrying out the filtering functions; in effect their role will change from merely retaining data routinely generated as part of their business functions – for billing and quality of service purposes – into collecting data about their customers for which they have no business use but which may be required by the Secretary of State.

17. **Private Business Networks** As the name implies, these are networks run by businesses and organisations for their own benefit or to serve the requirements of a discrete industrial, professional, academic or other community. They are typically run on equipment owned or rented by the organisation. These days they nearly all use the same technical protocols as the Internet (TCP/IP). General admission to the public is not allowed; many private networks have gateways, some limited, to the public Internet. Private Business Networks still fall within the remit of the Draft Bill - (ss 1(3) and 2(1) RIPA, 2000) and more particularly if the private network is facilitating a communication onto a public telecommunications network.

18. Because they have control over the network, owners and managers have complete technical access to all traversing traffic, though lawful surveillance may be limited.[17] There may also be extensive logging to record accesses by users, visits to websites and the activities of anti-virus software. If a RIPA approach does not prove effective, the same information could be obtained by Production Order or, *in extremis*, by a PACE or similar warrant to seize records and hardware,

19. The authorities might incur difficulties in getting access under RIPA or other means if the private network is managed from overseas and is uncooperative. RIPA covers all situations where the traffic crosses the UK, but enforcement would then require resort to a Mutual Legal Assistance Treaty, the outcome of which could be unsatisfactory.

20. **Social Network Service Providers** This rather awkward phrase (SNSP) encompasses businesses who offer communications and information services via a web-interface or phone/tablet app. The services are sometimes described as nomadic,

[15] The NAP/ISP can only provide information about their subscriber, the person with whom they have the contract, that may only indirectly point to who was actually using the equipment at the time

[16] An explanation of IP address appears from para 37 below. The availability of data is unlikely to be changed as a result of the migration from IPV4 to IPV6.

[17] Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

as they are available whereever there is an Internet connection. Examples include the web-based email facilities of Microsoft (Hotmail, Live, Outlook.com), Gmail, Yahoo and many others. It also includes businesses that offer social networking such as Facebook and LinkedIn and Internet indexing facilities such as Google and Bing. Many Voice-over-Internet-Protocol (VOIP) services, including Skype, fall into the same category.

21. Cloud-services are a variant: they offer remote storage and remote processing; examples are Google Apps/Drive, Microsoft SkyDrive, DropBox, Amazon Elastic Computing, Windows Azure and Apple iCloud. The same provider may offer more than one facility: Microsoft and Google both offer Internet-indexing, web-based email and "chat" (real-time conversation via keyboard); Google provides social networking as well Internet indexing and email, Facebook provides a messaging service, Skype, primarily a VOIP service also offers text messaging and so on.

22. A yet further variant are sites offering participation in online games; in some of them whole virtual worlds are created, participants can create avatars of themselves and chat to other participants; a leading example until recently was Second Life; a number are now delivered via games consoles such as Xbox. Concern is sometimes expressed that these services can be used for covert messaging between criminals and others, though I have been unable to identify any verified instance.

23. The headquarters of the legal entities behind the vast majority of SNSPs are based outside the United Kingdom, which means that non-cooperative enforcement of UK law is difficult. Most are based in the United States. The UK would have to rely on the operation of Mutual Legal Assistance Treaties (MLATs) and these can be slow in process because of the need to follow a variety of local protocols; they also rely on the enthusiasm of law enforcement agencies in the countries in which the SNSP is located. Many larger SNSPs have technical facilities – computer server farms – located in many jurisdictions all over the world, so that identifying where any particular communication or transaction is physically taking place may be almost if not entirely impossible.

24. SNSPs will have limited subscriber data as for many the enrolment process relies on the voluntary supply of information, which is often not verified; most do not impose a charge for their basic services, so that there is no linkage via the banking/credit card system. However IP address data may be collected so that an individual may traced that way (see above). However SNSPs often collect large quantities of *content*; for some the business model consists of giving desirable information or facilities to customers in order to collect information about them which in turn can be translated into opportunities for targeted advertising. In investigatory terms the content may be directly invaluable and may also help identify individuals even where those individuals have sought to obscure who they are. Cloud suppliers also store large quantities of their customers' data files; these presumably could be available to investigators, subject to the appropriate legal processes.

25. Many of these services use *https,* the secure encrypted form of the web, and which is also the foundation of web-based electronic commerce and banking. Encryption is used, not to thwart law enforcement but to protect customers from criminal eavesdropping. But the use of *https* also makes the type of NAP monitoring to obtain enhanced data retention contemplated in the draft Bill much more difficult to achieve.

26. In the US attempts are being made to bring SNSPs into the lawful intercept framework of CALEA (Communications Assistance for Law Enforcement Act, 1994, as amended) which would imply, in the US at least, an interception capability – although this could be provided using software on SNSP servers, rather than the interception of communications "on the wire".

27. The Joint Committee will undoubtedly be making its own enquiries of SNSPs but informal indications are that some US-based SNSPs are willing to respond informally in a positive and timely fashion to UK RIPA-type requests. However in so doing they have to consider, among other things, their obligations under US law, the impact that knowledge of their co-operation has on their customers and hence their business, and concern that authorities in other jurisdictions would want similar facilities. What is likely to be persuasive is the fairness and transparency of the ways in which requests (which would otherwise be warrants and authorisations) are made and by whom, how any material supplied is subsequently handled, and the quality and extent of oversight and audit.

28. **Small-scale informal private network service facilities** This equally awkward phrase covers the situation where communications and information facilities are set up on the Internet by individuals and small groups to service the need of small communities. Although the services are available on the Internet, access is restricted and may be only available by payment or specific invitation. Examples include bulletin board systems (which also have private messaging), private chat systems, file sharing systems, and secure email (which operates outside or in parallel with public email).

29. These services require only modest levels of technical skill to set up. Software to create the basic infrastructure is readily available, much of it at low or no cost. It is easy to run such services with cryptographic protection (*https* and its e-mail equivalent). Many ISPs offer hosting facilities, that is, the use of computers already connected to the Internet and to which the customer can upload his own software. It is also possible covertly to set up such services on large computer systems which are insecurely managed

30. Many of these services are non-sinister; for example bulletin board systems may serve people with particular professional or leisure interests. But the same technical infrastructure can facilitate illegal enterprises.

31. The opportunities for the authorities to detect such sinister services by routine as opposed to targeted Internet surveillance are very limited. The normal methods of detection are via traces left on the computer of one of the participants, confession or infiltration of the membership.

32. **Other forms of covert Internet communications** At this point we also ought to consider other forms of covert communications across the Internet, typically using existing Internet facilities and protocols in ways so that messages and data can be sent without easy detection. It can be a mistake to believe that covert Internet communication is only possible through the deployment of a sophisticated technology. Messages can be published via email, web sites, social networking sites where the words though innocent in appearance, have particular meaning to individuals; it is trivially easy to publish web-pages and files which are not directly

indexed on an otherwise innocent site and which could therefore only be found by those with specific instructions. More sophisticated methods of concealment are also available, but they require greater levels of skill in participants.

33. Almost none of these covert communications will be detected by routine Internet monitoring.

Communications Data and Content

34. Laws, in order to work, need to be capable of easy interpretation. One of the great weaknesses of the draft Bill is that the definitions of communications data do not align with the reality of the circumstances the Bill is supposed to be regulating and managing. At the heart of the Home Office's proposals is a belief that it is possible easily to separate content from communications data.

35. The penalties for incorrect separation of communications data from content fall chiefly on the police and other agencies. The legal regimes for access are very different – interception of content requires a warrant from the Secretary of State, communications data an authorisation from a designated senior officer. Communications Service Providers are *de facto* protected from mistakes[18], but police who have acquired material *ultra vires* will find themselves in difficulties, not the least at disclosure and the possibilities of arguments about abuse of process. [19] The problem is significantly compounded by the UK's almost unique position in treating intercepted content as inadmissible and not referable to in legal proceedings.[20]

Packet communications

36. In conventional analogue telephony, the distinction is easy to make.[21] "Communications data" consists of an enhanced telephone bill (traffic data, who called who, when, and for how long) and information about the subscriber. The content is the voice component, what would be captured if a tape recorder or similar were placed across the line. In mobile telephony, location data is also provided but is clearly separable from the voice element.

---

[18] They protected *de jure* under s 3(3), RIPA in that they are allowed to view intercept material for the purposes of separating it from content. In the event of inadvertent release they would argue absence of *mens rea* and also invite the CPS to apply a public interest test.

[19] See, for example the Codes of Practice on the *Disclosure and Acquisition of Communications Data* and *Interception of Communications* issued under s 71 RIPA and in particular Chapter 7 of the second Code. See also the *CPS Disclosure Manual* and in particular Chapter 27.

[20] See, among others, *Telephone Tap Evidence and Administrative Detention in the UK,* John R Spencer *in A War on Terror, ed Wade & Maljevic, Springer verlag 2010* and *Intercept Evidence: Lifting the ban,* Justice, 2010, Privy Council Review Chilcot, .Cm 7324,

[21] I am conscious how useful illustrations and demonstrations might be at this point but am also mindful of the restrictions in normal Parliamentary publishing. I would be happy to provide Committee members with a series of demonstrations if they feel it would aid their understanding

37. **Data packets** While in conventional telephony a permanent unique communications link exists between the parties for the duration of the call (a series of switches creating the link for as long as it is needed) , Internet traffic of all kind is transmitted as a series of packets. The system makes much more efficient use of available physical links; each link may convey large numbers of "conversations" or "transmissions". Data to be transmitted is broken down into a series of small chunks ("packets") each of which contains: the address ("IP address"[22]) of the originator, the IP address of the intended recipient, some supervisory information in case packets arrive at their destination out-of-order and need to be re-assembled correctly, and "payload".

38. **Packet payload** may include what RIPA regards as communications data and also what when captured becomes a RIPA interception. But there will also be a series of structures – commands, labels or values – which are the building blocks of the many protocols that make up the Internet – email, web-services, secure web-services, file transfer, file-sharing, Voice-over-Internet. These commands are not normally seen by the regular user; some of these commands and labels may themselves be either RIPA "communications data" or RIPA "content", or may help identify the subsequent sequences of text, etc. as either "communications data" or "content"."

39. **Contents of web pages** The complexity does not end here. A single web page may contain, at least in the terms hoped for in the draft Bill, both "communications data" and "content". A typical example would the "inbox" of a webmail service. The identity of the sender and the time of transmission is "communications data", but the subject matter is "content". On an individual basis visual inspection may easily spot the difference, but what is required is that the separation be carried out automatically at very high speed by software; each individual different design of a webmail web-page would need separate attention and whenever a specific webmail service has a changed design, the technical instructions for scraping the communications data from the content may need to be altered as well.

40. As if this is not enough, modern techniques for creating web-pages rely on taking material from multiple sources and using programming facilities loaded into the web-browser, the page is only finally assembled on the individual user's computer. (This technique relies on variants of JavaScript and HTML). In order to reconstruct from monitored packets the web page that the user sees – and hence be in a position to apply the legal definitions of "communications data" and "content" - several different packet streams may have to be assembled and reviewed. Some of the packets will contain fragments of the Javascript, etc. miniature programs.

41. **DPI** The basic tool for examining packets is called Deep Packet Inspection (DPI); it can operate in software in situations where traffic levels are low, but for high traffic levels (as when monitoring all communications by very many users), specialised hardware must be deployed. All DPI software and hardware arrives with an inbuilt-knowledge of the main Internet protocols of the time and can perform basic analyses on a per-packet basis. But any additional features require the writing of specific

[22] IP addresses are relatively unique to an individual computer; under the present system, IPV4, the ISP/NAP assigns IP addresses to their individual customers and maintains a record of such assignment, usually via the RADIUS log. Large organisations have permanent IP addresses which can be looked up via the Internet "whois" facility.

filters. Where the analysis requires several packets to be considered for their effect together, as in the complex web-page and JavaScript etc. facilities described above, the capabilities of DPI equipment to handle large amounts of data automatically and rapidly are unknown.

42. DPI equipment can usually only work where the web page instructions and components are sent unencrypted. But services from the likes of Google, Facebook, web-based email, are now delivered in encrypted form – using *https* – not deliberately to thwart the police and Agencies, but to protect their users for eavesdropping by criminals. For practical purposes in these circumstances, the only entities that can separate communications data and content are the Googles, Facebooks, and owners of webmail services, which I have referred to as Social Network Service Providers.

43. **Request Filters** As noted above at paragraph 39, an apparent individual communication may involve several different CSPs, a typical example being webmail or social networking. A subscriber's Network Access Provider would only be able to capture the identity of the machine to which the subscriber was connecting – cl 28 (2) and (3). The Social Network Service Provider might recognise that a customer/member was in communication with another customer/member but might lack detailed and authentic knowledge of who that customer/member is. The NAP does know, however, because the subscriber is identified when they pay – by direct debit or standing order – for the network access service.

44. The Bill, cl 14-16 and ENs 73-93, envisages an entity separate from both the CSP(s) and the requesting law enforcement agency which analyses a specific problem, requests material from the respective CSPs which will probably include "content" along with "communications data" and then combines them so that there is a resulting clearer identification of who is communicating. The process, so it is hoped, will prevent the requesting investigating agency from seeing anything other than communications data. In terms of webmail it will enable the requesting agency to see that their person of interest, who is now clearly identified from data supplied by the NAP accessed the webmail service and via it exchanged emails (or other messages) with a number of individuals at particular times. But the requesting investigating agency would at no stage see the subject matter of the messages. This is also the explanation offered by Peter Hill at Q94.

45. Cl 14-16 have a number of safeguards in that necessity and proportionality tests must be applied throughout, there must be rigorous security, after the delivery of the filtered material any remaining material obtained by the Request Filtering Entity in the course of their work must be destroyed, and audit records kept for scrutiny by the Interception of Communications Commissioner. However if these safeguards are not rigorously applied and fully examined by the Interception of Communications Commissioner there is a risk that that what is described as "request filtering" becomes large-scale data mining; the necessity and proportionality tests need to be applied not to just the individual data streams as supplied by CSPs but to the likely effect when they are assembled together.

46. The main purpose of this complex arrangement seems to be to protect CSPs and law enforcement agencies from the situation where the requesting investigating agency inadvertently receives "content" with the consequences indicated at paragraph 35 above.

47. Doubt must also be expressed about the credibility and viability of the entity that performs the Request Filter. Could it really be the same Secretary of State who also issues interception warrants under RIPA Chapter 1 and who also issues the Orders under cl 1 of the Draft Bill? If it is to be a separate "designated public authority" as suggested in cl 20(1) it will need resources, among them highly skilled staff who are familiar with the law, the applicable technologies and police investigative procedure – and who can also act independently. They will almost certainly need high levels of security clearance. In the private sector such people are likely to earn fairly high income; moreover they will want some form of career structure and stability. But there may not be a sufficiently consistent flow of work to make this possible.

Practicalities and Interpretations

48. The process of separating communications data from content is thus theoretically as follows:

    - In the first place the communication must be viewed as the participants would normally see it and the legal definitions in clause 28 (2-5) applied.

    - This must then be converted into instructions which the DPI interception equipment can implement; this in turn implies a full understanding of the various protocols in use for the main Internet services as well as the construction of certain web pages which contain both communications data and content.

49. Some aspects may be easier than others, for example cl 28(2)(b)(iii): "comprises signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of the communication". This sub-clause more-or-less reflects something that can be recognised at a technical level. But others do not.

50. The Bill has a number of clauses in this area that look as though they are capable of several interpretations. For example cl 28(3):

    Data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication is not "traffic data" except to the extent that the file or program is identified by reference to the apparatus in which it is stored.

51. This is borrowed from s 21(6) RIPA, 2000. One particular problem is the status of web pages within a website – the identity of the website is communications data, the web pages within it are content, but what happens if the filename of the web page gives an indication of its content? An example: "http://www.independent.co.uk/news/uk/crime/rebekah-brooks-and-andy-coulson-conspired-to-hack-milly-dowler-and-600-others-7966265.html"

52. Or cl 28(4):

    "Use data" means information—(a) which is about the use made by a person—(i) of a telecommunications service, or (ii) in connection with the provision to or use by any person of a telecommunications service, of any part of a telecommunication system, but (b) which does not (apart from any information falling within paragraph (a) which is traffic data) include any of the contents of a communication."

53. What would be the position of a website which builds up a profile of its customers' activities in order to make them future offers based on previous sales – like Amazon? Or a social networking site that similarly collects information about its user so that *inter alia* it can make recommendations? Both Facebook and LinkedIn frequently suggest "People You May Know" as suitable to add as "friends" – based on previous activity.

54. Simple interpretation of web pages generated by social networking sites such as Facebook may also be surprisingly difficult; here there can be significant problems in identifying which elements on a web page are communications data as opposed to content even before we attempt to turn these into technical instructions. Do we take it that the identities of posters are "communications data" and what they say (or pictures they put up) is "content"? What is the effect if some postings are only available to selected viewers – "Friends" - as opposed to being published to the world at large? What is the position of one-to-many communications but which still fall short of general public publication?

Implications for clause 1 Orders

55. The structure of the Bill is that it is provides a framework, with the detail to be covered by Orders to be issued by the Secretary of State. EN22 sets out the intentions:

> In practice, it is likely that an order under clause 1 may, amongst other things, impose requirements on operators to: generate all necessary communications data for the services or systems they provide; collect necessary communications data, where such data is available but not retained; retain the data safely and securely; process the retained data to facilitate the efficient and effective obtaining of the data by public authorities; undertake testing of their internal systems; and co-operate with the Secretary of State or other specified persons to ensure the availability of communications data.

56. Clause 2 sets out the requirements that Ofcom, the Technical Advisory Board (TAB) set up under s 13 RIPA (and which I understand has until now hardly ever met), and relevant stakeholders must be consulted. But the main democratic safeguard is supposed to be that Orders are subject to affirmative resolution by Parliament - cl 29 (2).

57. Given the pressures on Parliamentary time and material that will be technically complex and outside the normal experience of most Parliamentarians, it seems highly doubtful that detailed consideration will take place. Any such discussion would require information about the precise nature of the threats and, based on what ACC Gary Beautridge said to the Committee in oral evidence (Q 152), the police will want to discourage public debate as they fear that might inform criminals and others of gaps in law enforcement capability. In effect, Parliamentary affirmative resolution will not be a safeguard.

Costs, Value for Money

58. The Impact Assessment accompanying the draft Bill estimates costs to be £1.8bn for the 10 years from 2011/12 without allowing for inflation, VAT and depreciation. The main assumptions are: the total volume of internet traffic increases tenfold over 10 years, CSPs retain data for 12 months, data storage costs decrease by 25% per annum. Of the £1.8bn, £859m is the estimated cost to the private sector – CSPs of all kinds – and which will be paid for by the Home Office. The balance is made up of costs likely to be incurred in management and facilities by law enforcement and the agencies and in oversight by the Interception of Communications and Information Commissioners[23].

59. One of the unfortunate features of the Impact Assessment is that the only bodies listed as formally consulted were the users of communications data, as opposed to the CSPs who are expected to provide it[24]. It is puzzling how costs could be calculated without their input.

60. Forecasting anything to do with the Internet is fraught with uncertainty. Looking back over the last 10 years one must point out that the earliest manifestation of Facebook, one of the key concerns behind this Bill, dates from 2004 and was only opened to the public-at-large in 2006. MySpace, its predecessor in popularity, was founded in 2003 and in June 2006 was more-visited, at least in the US, than Google[25] but it was overtaken by Facebook by April 2008 and by August 2012 had declined to being the 166th "most visited" Internet site[26]. Twitter dates from March 2006, Google Apps, its consumer orientated cloud service of email, online calendar and remotely-stored and editable documents was fully launched in July 2009[27]. Skype, often cited as a particular problem for investigators, was founded in 2003 and has been through a number of versions.

Cost and Benefit Estimates

61. The Home Office Impact Assessment seems solely based on increases in the total volume of Internet traffic, not on its increasing complexity and level of change, which is what any form of separating of communications data from content will have to be concerned with. Even forecasts of traffic volumes over 10 years are problematic; looking simply over the next three years much will depend on the rate of roll-out of high-speed fibre-based links (which by themselves would encourage greater usage) and also to take-up of video-on-demand services, in which customers see films not over the air (terrestrial, satellite, conventional cable) or by renting DVDs, but by receiving video over the Internet. [28]

62. Similar doubts must exist of the estimate of benefits, which are suggested as being between £5 and £6.2bn. The Impact Assessment says:

> These benefits are assessed by operational stakeholders and, using a model validated by HM Treasury, translated into economic values. The assessment takes into account an analysis of criminal behaviours by the Serious and Organised Crime Agency and an analysis of the future communications market

[23] See also Charles Farr's reply at Q73.
[24] Paragraph A3 of the Impact Assessment.
[25] http://news.cnet.com/Googles-antisocial-downside/2100-1038_3-6093532.html
[26] http://www.alexa.com/siteinfo/myspace.com
[27] http://googleblog.blogspot.co.uk/2009/07/google-apps-is-out-of-beta-yes-really.html
[28] See the House of Lords Communications Committee Report: http://www.publications.parliament.uk/pa/ld201213/ldselect/ldcomuni/41/4102.htm

based on OFCOM and other market sources. The largest categories of benefits are direct financial benefits arising mainly from preventing revenue loss through tax fraud and facilitating the seizure of criminal assets. Values for benefits for example from lives saved and children safeguarded are derived from standard estimates by Home Office economists.

63. But if we turn to the main Home Office Research document cited[29] many caveats are made:

> Whilst information on the total and average costs of crime is extremely useful, average cost of crime estimates in this study need to be treated with some caution, for a number of reasons.
>
> _ *Different crimes within the same offence category are likely to have vastly different costs*.
>
> _ *Particular crime reduction initiatives may impact on different types of crime within the same offence category*.
>
> _ *Average cost estimates given…. are best estimates of costs given the information available. However, due to lack of good information in a number of areas, the estimates are inevitably imprecise*.
>
> _ *The costs of an identical crime may fall differentially on different social, economic or geographic groups –*
>
> _ *Some crimes are inevitably costed less accurately than others, and unquantified costs exist which may differ between crimes.* A *comparison* of average costs between different crimes could therefore be misleading. A higher average cost for one crime than for another could reflect the size of quantified, rather than unquantified costs, rather than a real difference in the costs of the crimes to society, although to some extent this is unavoidable in an exercise of this nature.

64. The Impact Assessment's "benefits" have a further problem: they are claims about what would result from the increase in access to communications data over what is currently already available.

65. Whatever the size of the costs and benefits, the Impact Assessment makes a further assertion: "The proposed *10 year* investment in communications data capabilities of £1.8bn compares with an annual cost for policing alone of £14 billion." But this is for every aspect of policing; it may be more realistic to look at the front-line organisations dealing with serious crime. SOCA's resource expenditure in 2011/12 was £427.9m, with a further £34m in capital expenditure[30]. A further basis for comparison is the UK's Cyber Security Strategy from November 2011.[31] The National Cyber Security Programme has a budget of real new money of £650m for the four years 2011-2015, of which only 10%, £65m, will go to the Home Office for "tackling cyber crime". Out of this comes a specific budget for the police: the new National Crime Agency will include the existing Police Central E-Crime Unit, the existing SOCA e-crime and CEOP, the child online protection group. On this basis the estimated costs for the proposed Communication Capability Development Programme begin to look rather large.

Source of Funding for CCDP

66. Even if costs are difficult to calculate it is possible to identify criteria for value for money. One of the great weaknesses of the Bill and the policies behind it is that nowhere has there been any explanation of the source of the required funding. The

[29] http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs/hors217.pdf
[30] http://www.soca.gov.uk/about-soca/library/doc_download/392-soca-annual-report-and-accounts-201112.pdf
[31] http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

government is currently seeking reductions across the whole of public spending costs of 20%, including the police. It seems a reasonable assumption that similar cuts will be expected from the Security and Intelligence Agencies. Only unambiguous evidence of new and growing threats would overcome this. But overall crime is down[32] and the last deaths in the UK from terrorism were in 7 July 2005, although of course this cannot be the sole indicator of level of threat.

67. If we assume that the CCDP will have to be funded from existing resources, the question then arises: which current areas of expenditure will have to be further curtailed beyond the 20% across-the-board savings already demanded? There seem to be two broad choices, either from every form of government expenditure – education, health, defence, transport, social services, etc. – or more specifically from the police and Agencies. One suspects that the police in particular will have reduced enthusiasm for CCDP if they have to partially fund its infrastructure costs.

Essential Criteria for Success

68. If CCDP is to be successful, or value for money, it must have a number of features, not all of which are explicitly referred to either in the Explanatory Notes or the Impact Assessment:

69. DPI equipment must not slow down the Internet experience At present CSPs are simply required to retain business records which fall into the definitions of "communications data". The Bill requires them to process it (see paragraphs 37 ff) and as we have seen these processes can be quite complex; without very high-speed equipment – which implies expense – the user's experience of Internet browsing will be slowed. This outcome would directly conflict with other aspects of Government policy, including that for superfast broadband.[33] DPI equipment installed now would need to be upgraded as fibre-based delivery services are rolled out

70. Monitoring must be near-complete The avowed aim of data retention is that once an individual, hitherto thought innocent, comes under suspicion, investigators are able to discover their past online activities. Although 100% availability of retained communications data seems infeasible, each 1% per cent drop surely significantly weakens the benefits as one must expect that those who wish to conceal their activities will take evasive action. A 90% coverage would incur significant costs but might only capture the activities of the wholly innocent. Thus, every UK ISP, no matter how small, would need to be covered, unless that ISP was only able to function by being a client of a larger, UK-based ISP.

71. The Home Office's position here appears confusing. At Q9 Charles Farr speaks of hoping to get, by deploying CCDP, up to 85% of "coverage" which presumably refers to 85% of communications data being transmitted in and through the UK. Richard Alcock at Q77, says the same but at Q82 says:

> In terms of the general number of CSPs, just in the United Kingdom, I think it is in the order of 250 to 300 communications service providers. We certainly do not envisage working with that many within the piece. Clearly, it depends how communications services change over time and whether groups

[32] http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-march-2012/stb-crime-stats-end-march-2012.html
[33] http://www.culture.gov.uk/publications/7829.aspx

gravitate to a certain service or not. But we certainly do not envisage working with everyone, and I estimate it will be **a relatively small proportion of those**. (emphasis added)

72. This lack of clarity about intended scope of coverage looks odd against the suspiciously precise projected cost of payments to CSPs of £859m.

73. Evasive measures In addition, the proponents of CCDP will need to explain how they would address the obvious easy routes to evading attention:

- Bought-for-cash pay-as-you-go-SIM, giving anonymity
- Use of Internet cafes and other public access services (unless it is assumed that the owners of these services will keep elaborate verified records of the identities of all their customers)
- Hi-jacking of unencrypted domestic Internet access points (with the result that the Internet activity is attributed to the registered subscriber)
- Use of encrypted webmail and other services from providers outside the UK and with whose law enforcement agencies the UK does not have close working relationship
- Use of small NAP/ISPs, thought unlikely to be asked install the DPI monitoring equipment

There are other methods of evasion but the above require no skill on the part of the user, other than to know that the route exists

74. How will encrypted services be handled? As we have seen, an increasing number of large important services are now encrypted, using *https* – see paragraphs 25 and following above. There does not appear to be a *routine* means of decrypting and hence getting access to anything that might be communications data. *HTTPS* is fundamental to Internet-based e-commerce and e-banking. In the course of a targeted investigation it may well be possible to obtain the co-operation of the encrypted service as there will then be evidence upon which judgements of necessity and proportionality can be made[34]. But CCDP is about the routine retention/collection of data from the whole population and in the absence of specific suspicions.

75. A possible solution would be for the CSP to retain all data that appeared to be encrypted and to make no attempt at separating communications data and content until there was a specific request. However, given the quantities of encrypted transmissions, CSP storage costs would soar. But Richard Alcock, Q47, seems to say that RIPA would not allow this, presumably as content, even if encrypted, cannot be retained.[35] And most versions of https can only be intercepted at the time encrypted messages are sent, using a "man-in-the-middle" attack.

76. **How will overseas CSPs be dealt with?** The UK appears to have two routes to dealing with CSPs outside the jurisdiction. The first is to seek their co-operation, a

[34] There are also other technical routes which are available in a targeted investigation in the event of non-cooperation from the service provider

[35] It is possible that the uncorrected transcription on which I am relying is not wholly accurate at this point.

view reflected in Charles Farr's response at Q52: "The central plank of this programme is a collaborative relationship with service providers in this country and overseas. DPI, black boxes, or whatever other metaphor or language we choose, only come into play in certain circumstances when an overseas provider or the state from which an overseas provider comes, or both together, tell us that they are not prepared to provide data regarding a service which is being offered in this country and which we knew and know is being used by criminal elements of whatever kind." This incurs relatively low financial costs but may involve persuading the CSPs that the legal and regulatory framework for issuing requests is fair and rigorous. See my remarks at paragraph 27 above and 92 below.

77. The second route appears in the same answer: "The legislation therefore creates the option, in those circumstances, of putting a black box, using your language, on a UK network across which the data from the overseas provider must move, with the purpose of sucking off that data, under our guidance—"control" is too strong a word—and storing it through that network provider." In other words a form of filtering based on that service. At Q54: he says: "The network provider would take off the network the data particular to the service of concern to us and store all that data. We would then apply to the network provider for specific bits of the data that has been so stored, in accordance with usual practice." This would incur expense and the Joint Committee should make further enquiries as to its likely level.

78. Many of the big overseas services with which we assume there is the greatest concern, like Google, Live/Hotmail, Twitter, Facebook, etc. use encrypted links, in which case this second route would have very limited effect.

Benefit Elements

79. The Home Office express the benefits in terms of globalised percentages, saying that they hope to move from a 75% availability to 85% (Q9). At Q22, Charles Farr produces a percentage breakdown of applications for communications data, presumably based on existing law.

> 27% of data for which applications are made and obtained is for drugs-related offences, 15% is for property offences, arson, armed robbery, theft, 12% is for financial offences, 10% is for sexual offences, 6% is for homicide, 5% is for missing persons, 5% is for harassment, 4% is for offences against the persons, and 4% to 5% is for explosives.

80. But what is really required, if there is to be a proper value for money assessment, is the ability to identify particular types of communications data originating from particular classes of communications service provider. Many existing highly useful forms of communications will continue to be available for the reasonably foreseeable future – including mobile phone location (which is not Internet dependent) and, from Network Access Providers, the ability to link IP addresses obtained by a variety of means to the identities of their subscribers. What is needed is a way of identifying the specific forms of further communications data that CCDP will deliver – so that it can be related to the costs of acquiring it.

81. One purpose of setting out the various types of CSP and the classes of data they might produce in paragraphs 10 to 31 above was to assist the Joint Committee in gaining a

better ability to assess these separate elements. I note the remarks of ACC Gary Beautridge to the Committee in oral evidence (Q 152) and have some sympathy with his concern not to expose current law enforcement weaknesses. But I hope the Joint Committee will pursue with vigour and carefully test any confidential information supplied to it by ACPO and others.

Cost Elements

82. DPI Boxes The first cost element, to be paid for by the Home Office, is the installation of the DPI boxes at NAP/ISPs. Because one must anticipate attempts at evasion by those of greatest interest to the authorities, this investment will have to be front-loaded. That is to say, near 100% coverage of UK NAP/ISPs will be required not too long after the intended start-up. Although the Home Office speak of wishing to run pilot studies, usually an important means of testing a policy, the pilots could not show how well CCDP was meeting the threats of evasion. This significantly increases the risk to the taxpayer.

83. As noted above, given the growth speed, and difficult-to-predict nature of the Internet DPI boxes would need constantly to be upgraded

84. Filtering Software As explained at paragraphs 37 to 40 above, the provision of filters to be run on the DPI hardware is likely to be an extensive and on-going project. It is not clear who will do the necessary research and produce final products – GCHQ might be a candidate. This will still be a cost which has to be met from some budget or other ultimately funded by the tax payer.

85. CSP additional costs In addition to the costs identified in the ENs and Impact Assessment, the Joint Committee should ask CSPs about the costs of producing material from their archives of retained data at speed to meet likely emergency requirements from law enforcement. It is not enough that required communications data is simply kept, it must also be available; and that implies some near online capability. Mobile phone companies, on whom there are frequent demands but where the normal requests are very standardised – calling number, receiving number, date/time, call duration, IMEI, IMSI, location – have automated or semi-automated systems. Will something similar be required of other types of CSP, and what will be the cost implications?

Open-ended nature of CCDP

86. The following elements are highly difficult to forecast: the growth in Internet traffic volumes, the levels of complexity of future Internet services, the numbers of CSPs, and the extent of attempts at evasion. If allowed to proceed in in anything like its current form CCDP will have all the pre-conditions for an uncontrolled government computing project or MoD defence contract. Its details will be shrouded in secrecy in order not to give criminals and others an advantage, any associated contracts will be hidden from scrutiny as "commercially confidential" and the precise specification will be subject to constant change. This is the classic formula for runaway costs and hence a significant risk to the taxpayer.

Possible Alternative Legislative and Policy Routes

87. I hope it will help if I sketch out some alternatives to the proposals in the draft Bill.

88. **Intrusive Data Monitoring Warrant** A more radical form of legislation would almost certainly have *to abandon the attempt to separate communications data from content*, so that an intrusive data monitoring warrant would cover both. This would mean that the peculiar UK position of making intercept evidence inadmissible[36] would also have to be abandoned. RIPA already features directed and intrusive surveillance regimes – s28 and s 32 respectively. The test for granting would depend on the levels of intrusion rather than a technical assessment of whether data was "communications data" rather than "content".

89. Any new power along these lines would almost certainly have to be subject to judicial scrutiny as opposed to the current position where warrants are issued, for historic reasons, by a Secretary of State acting on behalf the Crown. I am aware the arguments for and against of warrants issued by a Secretary of State and of the similar arguments about self-authorisation by designated senior officer in relation to communications data.

90. **Data Retention of Business Records** This would be very similar to the current position where CSPs retain records that they create in the normal course of their business and which would include "communications data" as currently defined in RIPA or EUDRD but would not require them to do any further processing.

91. I would favour passing power this over to judicial scrutiny as well, not the least for the reasons now explored below.

92. **Position of Overseas CSPs, including SNSPs** As we have seen, much of the material which the authorities hope CCDP would make more available is held by CSPs based outside the UK. It seems much more sensible to seek their co-operation rather than relying either on Mutual Legal Assistance Treaties, which can be cumbersome and too slow to be effective, or to hope that the data can be monitored while in transit in the UK. But to do this may require convincing SNSPs that UK legal procedures are fair and transparent. As noted above, SNSPs will need to consider their position under the laws of their home jurisdiction, usually the United States, and also the perceptions of their world-wide customer base.

93. Judicial supervision is far more common and understood worldwide than then UK practices of a politician to grant warrants for the most intrusive activities and self-authorisation by senior law enforcement officer for the rest. For that reason alone, judicial supervision is likely to be more credible and persuasive.

94. There is a further element: companies like Google, Facebook hold large amounts of personal data about their customers and do so with their consent. Cloud providers hold files created by their customers. In these circumstances the assessment of proportionality becomes especially important. Should a warrant automatically give

[36] S 17 RIPA

access to *all* the material the cloud provider holds? To my knowledge this issue has not be examined in any detail anywhere in the world.

95. **Enhanced role of Commissioners** Also as part of a policy of convincing SNSPs and others of the rigour and fairness of UK procedures, there surely needs to be a more visibly robust regime of Interception of Communications and Information Commissioners. Information Commissioners have always had a public profile, appearing on television, engaging in debate and making public demands for law changes and increased resources. Interception Commissioners have until recently been almost invisible. The most recent report[37], for 2011 provides more detail and candour than hitherto, but the Commissioner held just one meeting outside a wholly official environment, with the specialist Data Protection Forum.

96. Although his Report describes how he audits the activities of the police, Agencies and other bodies, it is unclear how far he questions the reasoning and evidence of the "necessity and proportionality" tests that are the starting point for each warrant/authorisation. If he doesn't he should do so – and identify situations where matters went awry. Obviously any review of such tests would have to be on the basis of information available at the time. The Commissioner could also usefully describe in more detail the resources and skills of his inspectors. Consideration should be given to moving this role into the Information Commissioner's Office, where it might be less easily perceived as "captured" by the law enforcement and intelligence agencies it is supposed to be overseeing.

97. The Investigatory Powers Tribunal is even less visible, and hence less credible, than the Interception of Communications Commissioner. It would have much greater perceived independence and credibility if reconstituted directly under the control of the Supreme Court (as is the US Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Appeal), with more transparency.

98. **A new type of retention warrant?** One can also envisage a new type of warrant, also issued by a judge, on the basis that although an individual who is not currently presenting sufficient of a threat to justify full scale monitoring there was the possibility by virtue of people whom they knew or views they were thought to hold, it might be useful if the ISP were to **retain** their communications and content for a period of year against the future possibility that the police or other investigators produced a full warrant to view the material. This would address a problem identified by investigators that on occasion they identify a substantial conspiracy in an advanced stage and wish to know something of the previous actions and thoughts and associates of those thought to be involved. However this last proposal has many difficulties associated with it – what would be the actual criteria for the issuing of such a warrant and how would it be supervised? But it would have the further advantage of being targeted – effort and expenditure would be directed against those who might in the future be of interest, as opposed to the 99.5% of the population who never will be.

I would be happy to answer any questions the Joint Committee may have.

2 August 2012

[37] http://www.intelligencecommissioners.com/docs/0496.pdf