APIG – Submission
On behalf of UK Law Enforcement

Communication Data

1.1 Communications data is crucial to the business of the law enforcement community. It is pivotal to reactive investigations into serious crime and the development of proactive intelligence. At the lower level, it provides considerable benefit to the detection of volume crime. It provides the only 'eyewitness account' for crimes on the Internet or exploiting telephone services. It can often be our only opportunity to trace the perpetrators. Short-term retention will have a disastrous impact on the ability of the law enforcement community to gather vital evidence and intelligence.

1.2 Communication data is currently accessed by Law Enforcement and others via the Data Protection Act (DPA). Sec 29 allows Communication Service Providers (CSP) to release data to requesting agencies if a sufficient case is made for its release. This system is not European Convention of Human Rights (ECHR) compliant as the law enforcement community does not access the data 'by law'.

1.3 This situation was recognised by Government and dealt with under the part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA). When enacted the section will allow Public Authorities to require CSP's to release relevant data providing a senior officer has considered the necessity, proportionality and collateral intrusion associated with the request. This brings the UK into compliance with ECHR and removes the exposure of CSP to civil tort for releasing data.

1.4 RIPA Part 1 Chapter 2 has not been enacted having been referred by the Home Secretary for further review over the issue of additional public authorities. These are mainly non – law enforcement agencies that sought to be listed under RIPA. A lack of visibility over the reasons these bodies required access to communications data led to a considerable amount of press criticism.

1.5 Thus despite a widespread public perception that 'the Police' already have unfettered access to telephone records no such power exists. Vital communications data is accessed by the good grace of the CSP's and the law enforcement community becomes increasingly concerned about the courts attitude to the legality of the access.

1.6 This is an unsustainable position. The law enforcement community urges Government to regularise it swiftly. This can best be achieved by enacting RIPA Part 1 Chapter 2 either with the non-law enforcement additional public authorities or, if that can't be achieved quickly, without them.

Data Retention

Purposes

2.0 Having established the necessity and requirement for Communications data for law enforcement purposes, it is essential to ensure that relevant data exists to be accessed.

2.1 CSPs rarely need to retain data for commercial reasons longer than 3 months. Existing UK and EU legislation requires CSPs to delete data once surplus to their business needs. It is the intention of most CSPs to begin deletion after 12 months. Most ISPs consider their data to be surplus within a matter of hours and some, therefore, begin deleting within 24 hours.

2.2 As current business models tend towards 'flat rate' schemes the necessity for and hence the availability of, billing data decreases. This will potentially destroy the investigative and evidential advantage Law Enforcement currently enjoys.

2.3 Additionally the Courts have an expectation that data will be equally available to both Prosecution and Defence. In the absence of retention legislation, early deletion could lead to miscarriages of justice. The Criminal Cases Review Commission has serious concerns about the absence of such data, should early deletion become the norm.

2.4 The Government recognised these concerns and attempted to rectify the omission of Data retention provisions within RIPA with the Anti Terrorism, Crime and Security Act 2001 (ATCS). Unfortunately this emergency legislation was based and presented as a response to the terrorist events of September the 11th. Insufficient emphasis was placed on the requirement of data for Crime purposes. Accordingly Parliament restricted the provisions of the act to terrorist related matters.

2.5 Then end result is legislation allowing the retention of data for terrorist related crime and access provisions to that data that do not take into account the reason for retention. This situation was highlighted by the law enforcement community prior to the bill and has subsequently been highlighted by the Information Commissioner as an area of grave concern.

2.6 This is untenable, leaving the industry exposed to civil action and law enforcement uncertain of their powers. The law enforcement community urges government to rectify the situation swiftly.

Mandatory retention

3.0 The other aspect of Data retention that has proved contentious is whether CSP's should be required by law to retain data or if a voluntary scheme would suffice. The service has always argued for a mandatory scheme as we fear that those CSP's that choose not volunteer may become 'data havens' attracting the business and customers that would prefer to avoid the notice of law enforcement.

3.1 The government chose to pursue a voluntary scheme and at the time industry backed this stance. Although consultation is ongoing it would appear that many large CSP's have been unable to volunteer for the scheme and it is therefore in danger of failing.

3.2 The potential for this to happen was envisaged by those drafting the ATCS and thus the Home Secretary has powers to impose a mandatory code should a voluntary one fail. The law enforcement community urges the use of these powers once it is clear that a voluntary scheme cannot work.

European & International Aspects

4.0 The law enforcement community has engaged with colleagues in European Law Enforcements agencies in a number of fora to agree a common data retention standard. This is a desirable outcome for reasons of mutual assistance and the investigation of cross border crime. It would also assist the larger, trans-national CSP's in providing a consistent framework to work to.

4.1 This work has proved difficult to the point of impossibility, foundering on the differing legal structures and access provisions in place in EU member states. In a recent meeting a member of the body representing European Internet Service providers (EuroISPA) suggested that a common EU data retention standard would not be possible until there was a common EU legal structure. Whilst the law enforcement community does not share that view we should point out that we could not wait that long.

4.2 The law enforcement community has been consulted on, and supports the generality of the work being undertaken by the Home Office to support the Belgian EU proposal. The work is at an early stage and is not assured of success. The law enforcement community would urge progress on domestic legislation whist this work evolves.

APPENDIX A

Attached, as appendix A is a document presented as evidence of the Law Enforcement requirement for Communications data. It was prepared for the debate over the data retention requirement as part of the consultation for the Anti Terrorism Crime and Security Act. It is therefore weighted with Terrorism examples and cases where data either was or could have been useful if retained for long periods. I apologise but your timescales prevented the preparation of a more bespoke evidence document.

Law Enforcement Agency business case for data retention under Anti-terrorism Crime & Security Act 2001

Communication is vital in the running of any organisation. This is as true of terrorist or organised criminal groups as it is of businesses. Given this, one of the key ways to disrupt terrorist and organised criminal activity related to terrorism is to investigate their communications. It is also true that communications data is considered by the law enforcement agencies an essential tool for the purposes of safeguarding of national security and the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security.

Access to communications data allows investigators to identify suspects, examine their contacts, establish relationships between conspirators, and place them in a specific location at a certain time. Analysis of this information can then be used to draw up a detailed profile of the suspect, either to inform prevention/disruption operations or for use as evidence in a prosecution, supported by witness statements. Equally, the information provided by analysis of communications data may clear an individual of any suspicions.

The terrorist attacks of September 11th highlighted the need for the retention of historic communications data in order to investigate threats against national security. Since that time one investigative agency has made over 4,000 request to the Industry for communications data specifically related to terrorist investigations.

The Anti-terrorism Crime & Security Act 2001 Act recognises that communications data is an essential investigative tool for the security, intelligence and law enforcement agencies in carrying out their work to safeguard United Kingdom national security.

The Agencies have provided the following examples to highlight the essential nature of data retention.

Case One (Elapse of 20 months before significant leads developed)

In July 1999 an assassination took place. Two witnesses described masked gunman bursting into the victim's house and firing two shots fatally wounding him. The victim made what was effectively a dying declaration, indicating why he believed he had been attacked

Initial enquiries revealed little of substance in terms either of linking the suspect to the offence, or identifying the other suspects, who in the interim fled the jurisdiction.

In early 2001, the investigation was rekindled as a result of contact with a former girlfriend of one of the suspects. She had significant, albeit circumstantial, evidence in relation to possible suspects.

Recovery of call data, relating to a series of calls she stated had been made on the day of the murder, was a means to corroborate her stated evidence. From this the cellphone number of another suspect was identified. However, due to the business practices of the service provider no call data remained relating to his number.

Significantly, though, the girlfriend knew the name of the other suspect and enquiries around the name led to the recovery of call data relating both to the latter's fixed line telephone at his home address and to his cellphone.

This indicated a significant call pattern both around the time of the purchase of the getaway vehicle (which had been identified earlier in the enquiry), and on the day of the murder. Cell site information was obtained, which effectively showed the route taken by the men, from early morning in North London, to the vicinity of the murder scene in Kent, the scene of the destruction of the getaway vehicle and the visit to the former girlfriend.

Not only was the girlfriend thus corroborated, but substantial evidence of conspiracy was provided by use of call data, which at the time all suspects were charged was approximately **thirty months** old. All defendants were convicted.

Case Two (Elapse of one year, before significant lead developed)

In May 2000, a drugs dealer was shot dead in the street. As with the former example, this was a carefully-planned assassination which had all the appearances of a contract killing related to terrorist activities.

Surveillance appeared to have been conducted on the victim throughout the early afternoon on the day of his murder, by men in two vehicles, as well as at a static observation point in a café.

The third vehicle followed the victim's car away from the scene where, whilst caught in heavy traffic, the victim was shot in his car. The suspects made good their escape.

After a year had passed with no significant leads, a witness came forward, requesting police assistance in relation to another matter. A named suspect was proffered in relation to this incident.

After several abortive attempts, a cellphone was identified for this suspect, the pattern of usage was such that it fitted his being the passenger in the third vehicle, that is to say the hit-man. The recovery of further call data, including the identification of other cellphones, used both by the suspect and by his co-conspirators resulted in enquiries, which established the identity of the latter and of the principal in the conspiracy offence. Much of the call data used in this case was **eighteen months old** at the conclusion of the investigation. These events took place against a backdrop of PKK/DHKPC activity, the 'hitman' being a Bosnian.

Case Three (Reseller data recovered after fifteen months)

A kidnap. These offences are characterised by illegal immigrants being held hostage in the UK, whilst ransom demands are made of family members in the home country. These are comparatively sophisticated offences, in that direct-dialled calls are seldom seen, suspects tending to rely on the service provided by means of pre-paid international calling cards.

After the successful recovery of the hostage in this instance, over a year passed before the suspects came to trial. It was noted that the hostage had been held at more than one premises.

Enquiries during the course of the trial, some **fifteen months** after the offence, resulted in the discovery of a previously overlooked pre-paid calling card. The relevant service provider was, fortunately, in a position to run a history of the card's usage, from which the use of the card by all three defendants was established, thereby providing evidence of association and common purpose. Furthermore, a fixed line number was identified, which in turn led to the hostage being able to identify the premises at which he was first held. Evidence relating to this location was crucial in bringing about the conviction of the defendant against whom the evidence was originally weakest, but who could now be shown to be the principal in the conspiracy offence.

This sector of the industry is normally not renowned for retention of records for long periods. The incident outlined was the exception not the rule. Whether this method of placing international calls is used simply because of the (substantial) cost savings or not is a moot point: it may be regarded as more than co-incidence several terrorist organisations, including Al-Qaeda have employed this method of placing calls.

Case Four

This operation was a significant long-term multi-jurisdictional enquiry, into offences involving money-laundering. The logistics of terrorist operations frequently require the movement of large quantities of money. Recent anti-terrorist activities have resulted in the freezing of substantial assets, controlled by such organisations, but *proof* of relevant offences can often be only as a result of protracted enquiries, often over a number of years.

By 1998, much relevant call data had been recovered. In many cases this resulted in the evidence of undercover officers being corroborated and the activities of the principals and co-conspirators being identified and substantiated.

The call data in question dated as far back as 1992. As **six years** had elapsed since the inception of the investigation (which is still ongoing), only one UK telecommunications network was able to provide significant data. This data, as in the last example, has been crucial to providing evidence of the association and common purpose of the conspirators.

Case Five.

Culminated in the arrest and charge of 5 RIRA members for acts of terrorism. Explosions had occurred in White City, Ealing and Central London. The parties involved where first shown as resident in England from May 2001, in all probability they had been resident for longer. They were arrested in early November 2001 and February 2002. The need for telecommunications information pre these times was essential. The investigation involved request for data for periods in excess of 18 months.

Case Six.

Enquiries since 11th September 2001. The case against a person detained in USA has involved the investigation of telephone records that identify links between the individuals involved showing association. These links are now being traced back to a date 18 months before 11th September 2001. The enquiry is now a year old, needless to say there are numerous suspects involved which increase on a daily basis. Subscribers and billings is an important tool in the investigation to show links between certain Nominals.
One person is at present detained and awaiting trial in the United States charged with being the 20th Highjacker.
The U.S Attorney General is bringing in Telephone evidence not only obtained over the period since September 11th, but a long period before, to show association.
Historical billing on a previous UK case called is also being introduced. This case, involved the suicide bombings on two US Embassies in Dar Es Salaam and Nairobi in August 1998. Records show a direct connection between the two Operations, proving an Al-Queda connection over three years ago. At present three suspects in this case are detained in the UK, awaiting extradition to the US.

Case Seven.

A person was detained and arrested trying to detonate a bomb hidden in one of his shoes. There was no intelligence to indicate his involvement in the Islamic Fundamentalist movement other than his indoctrination whilst detained in a Youth custody establishment back in 1996. Records show this was the only period he owned a mobile. Telephone records on this mobile and his various places of residence would have been invaluable in showing association with other members, over the past six years. Phone records would not only have shown who he rang, who rang him and from where, but would have shown his period out of the country whilst under terrorist training.

Case Eight.

Involved the arrest and charge of six members of the IRA indirectly linked to numerous acts of Terrorism in England over a long period. Including Hammersmith Bridge, Manchester and Birmingham bombings of 1996. All the members of the active service

unit had been living in England for many years in various locations, so telephone records would have been very useful during the investigation. This investigation was pursued for much longer than a year.

Case Nine.

Involved the arrest and charge of three members of RIRA, the same group that was responsible for the Omagh bombing. They continuously travelled backwards and forwards from Ireland and purchased three mobile phones on the mainland. They were kept under surveillance and eventually arrested in July 1998. Places of residence in the UK were searched and phone records helped to establish links with other groups in Northern Ireland and England.

Case 10.

Operation Heron was the lorry-bomb that exploded in Canary Wharf on February 1996. Initially no one was arrested for the incident. In April 1997 a James McArdle was arrested as a result of a positive identification on fingerprints. Once again all telephone data requested were already over 14 months old.
If telephone data retention were reduced in time cases five to ten would not have produced positive lines of enquiry.

Case 11.

Operation Excel was the mortar attack on Heathrow Airport in March 1994. In October 1996 a member of the IRA living for several years in London was arrested for being the Quartermaster to the active service unit based in the UK, responsible for the attack. He not only had a home phone but a mobile. His biggest ploy was to use the Public Call Box outside his home. He was charged and convicted in February 1998. The attack to the time of arrest was 2 and a half years.

Current Day.

The arrest of Kerim Chatty in Sweden has provoked requests for information on communications data almost 12 months after the September 11th incident. The possibility of linking calls made to fundamentalist in the UK and other linking calls to al-Qaeda groups, or the lack thereof will become major issues in proof or disproof of the case against the person concerned.

Homebred and International Terrorism is very different from any other form of Police Criminal Investigations. Investigators are not aware of suspects until their time of arrest. They may have been resident in the UK for many years, had various mobiles during that period and had different hardlines. Mobiles need not be registered any more so by the time a mobile is identified as being associated with a specific Terrorist the records under the present system may have been deleted.
September 11th atrocities in the US were planned over many years, resulting in the death of over 3000 people. Connection between the various highjackers must have been made during the previous years but the records are no longer available.

It is generally understood that all records cannot be kept but the longer the better, for existing and future Operations.

Reviewing the level of request for data from the communications service providers since September 11th 2001 indicates that in excess of 10,000 request related to terrorist activities have been made. Not all these requests have actually provided results as the companies, although keen to assist, have set limits of data retention that mean that information has been deleted and is therefore no longer available.

The agencies that have been involved in the investigation of terrorist incidents identify the need for retention periods that exceed those outlined in the Anti-terrorism Crime & Security Act code of practice. However they see the retention periods proposed as an opportunity for enabling those companies that have a business practice of retaining data for shorter periods to assist future investigations by aligning their retention periods with those of the code.