THE DATA RETETNION DIRECTIVE 2006/24/EC

This paper has been produced by France, Ireland and the United Kingdom for discussion at the Member States "Workshop to consider future options for data retention in the EU" on the 30 June. This follows the evaluation report from the Commission to the Council and European Parliament "Evaluation report on the Data Retention Directive (Directive 2006/24/EC) COM (2011)225".

1. Summary

The Commission's evaluation report confirms that data retention is a valuable instrument to maintain security in the EU. Communications data retained under the Directive plays a central role in the fight against serious crime. It has provided valuable leads and evidence which have resulted in convictions for criminal offences and in acquittals of innocent suspects in relation to crimes. Without data retention, some of these crimes might never have been solved. Despite these achievements, the report concludes that changes are required to the Directive to increase harmonisation and to set common rules for the storage, retrieval and use of traffic and location data.

This paper sets out why France, Ireland and the United Kingdom believe that the Data Retention Directive (2006/24/EC), (DRD), provides a valuable basis for data retention across the EU which is flexible and sensitive to the differences between Member States' criminal justice systems. The paper explains why the evaluation report has not made the case for changing the Directive and explains how the Commission's objectives could be achieved by guidance without reopening the directive.

The Data Retention Directive has provided greater consistency in relation to the retention of communications data across Europe. It provides sufficient flexibility to allow different Member States to regulate access to retained data in accordance with their different criminal justice systems, whilst ensuring that the necessary safeguards can be put in place to prevent improper access or disclosure in accordance with EU data protection rules. We believe that this enables Member States to implement the provisions effectively in ways that are compatible with their criminal justice systems. We are concerned that the proposed changes, intended to deliver greater harmonisation and more rigid controls, would result in reduced operational capability and no greater safeguards or reassurance to the public. While some additional guidance on data protection and clearer advice on what statistics Member States should submit to the Commission may be of benefit, we do not believe that changes are required to the Directive.

A number of operational examples have been included to provide a qualitative demonstration of the value of the communications data retained under the Directive.

2. Introduction

Since its adoption in 2006 the DRD has played a key role in maintaining public security throughout Europe by ensuring that communications data is available to police and law enforcement agencies. Communications data is vital to serious crime and terrorism investigations.

In the UK, communications data is used to provide important intelligence and evidence in around 95% of serious and organised crime investigations, and is used on a daily basis to

secure convictions, to confirm or disprove alibis, and to save lives. It has also been used in all major counter-terrorism investigations in the past decade.

The Irish Authorities consider retained communications data to be a very high-value operational tool for the investigation and prosecution of crime and the safeguarding of the security of the State. Retained data is particularly important with regard to combating the activities of terrorists and organised crime gangs as a tool in investigation or prosecution.

It is also important to emphasise the potential which retained communications data can have to prove or help to prove the innocence of an individual who may be suspected of an offence, or to help investigators to rule out persons who may otherwise become suspects in a criminal investigation.

The value of communications data was recognised by the Commission in its recent report COM(2011)225 "Evaluation of the Data Retention Directive (Directive 2006/24/EC)". The evaluation report questioned the extent to which the Directive has harmonised data retention across Europe and argued on this basis that the Directive should be amended. In section 8 it concludes that the EU should support and regulate data retention as a security measure but that there should be greater harmonisation and operators should be consistently reimbursed for costs. The Commission then identified some specific areas as meriting particular consideration namely:

- consistency in limitation of the purpose of data retention and types of crime for which retained data may be accessed and used;
- more harmonisation of, and possibly shortening, the periods of mandatory data retention;
- ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States;
- limiting the authorities authorised to access the data;
- reducing the data categories to be retained;
- guidance on the technical and organisational security measures for access to data including handover procedures;
- guidance on the use of data including the prevention of data mining; and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument.

This paper, drawing on the quantitative information provided to the Commission and qualitative examples, sets out why we believe that the changes proposed are to the Directive are unnecessary, would offer no greater benefits in terms of enhanced data security, and could adversely impact on the operational effectiveness of law enforcement agencies. We recognise the need for strong data protection and putting the right procedures in place to ensure that retained data is only accessed when it is necessary and proportionate to do so, in accordance with Member States national law and European law. But we do not believe it is necessary to change the Directive to achieve this. The existing Directive allows Member States the necessary flexibility to ensure the required safeguards can be put in place in ways that reflect the different criminal justice systems across Europe. We are concerned that moves towards greater harmonisation could result in greater bureaucracy, reduced operational capability, and no meaningful benefits in terms of safeguarding the privacy of individuals.

The eight areas identified by the Commission as meriting particular consideration are considered further below.

3. Consistency in limitation of the purpose of data retention and types of crime for which retained data may be accessed and used

The Data Retention Directive was necessary because another European Directive (2002/58/EC) – referred to as the "e-privacy Directive" – would otherwise have placed obligations on service providers to destroy certain types of communications data or make the data anonymous so the originator of the communication could not be identified. Article 15 of the e-privacy Directive does allow Member States to "derogate" from these obligations on a state by state basis but there was no consistency of approach. Crime and terrorism do not respect national boundaries, and the bombings in Madrid and London in 2004 and 2005 reinforced the need for a Europe-wide approach to the retention of communications data. The Data Retention Directive has delivered this and had made a major step forward in terms of delivering a common approach whilst allowing some flexibility to reflect the differences between Member States.

The Data Retention Directive specifies the types of data that can be retained, the retention periods, and requires Member States to ensure that the way in which the data is retained and accessed is consistent with national and European Law. Communications data usually constitutes personal data and as such the principles governing the protection of and access to communications data are essentially the same as those for other types of personal data.

The Data Retention Directive (Article 4) leaves the issue of access to retained data to Member States "who are obliged to ensure that data retained in accordance with the Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedure to be followed and the conditions to be fulfilled in accordance with necessity and proportionality requirements shall be defined by each member state in its national law, subject to the relevant provisions of European Union law or public international law , and in particular the ECHR as interpreted by the European Court of Human Rights." Once communications data has been retained (whether under the DRD or other instrument) it is for Member States to determine how that data can be accessed by competent national authorities in specific cases and in accordance with national law and European law – this includes proper consideration of necessity and proportionality.

We believe that it right is for Member States to determine how they comply with European law, taking into account national variations. This includes the purposes for which retained data can be accessed. The DRD in its current format achieves this.

The Data Retention Directive requires communications data to be retained for the prevention and detection of serious crime but once the data has been retained it can be accessed for other purposes providing that these are consistent with those set out in the Data Protection Directive. It would be unrealistic to expect service providers to distinguish between data that they would have lawfully retained for business purposes without the DRD (e.g. who owns a particular telephone number), data retained in reliance on the derogation in Article 15 of the E-Privacy Directive (Directive 2002/58/EC), or data retained as a direct consequence of the obligations placed on them by the DRD.

In the UK, access to retained communications data by public authorities is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). This allows communications data to be accessed for purposes other than serious crime, by specified public authorities, providing that the request satisfies the purposes set out in RIPA, meets the strict requirements for necessity and proportionality, and is in accordance with the principles and purposes set out in the Data Protection Directive and Article 8 of the European Convention on Human Rights, ECHR. So, for example, a coast guard responding to an emergency call may use location

data provided by the service provider to identify the whereabouts of the caller because in these circumstances there is a threat to life and it is clearly necessary and proportionate to do so.

A 14 year-old girl from the Fife area in the UK was reported missing in November 2009. She had a history of self-harm and suicide attempts, trying to hang herself, slashing her wrists and taking an overdose. She left a note for her parents saying she was 'hearing voices'.

A trace to find the current location of the girl's phone was carried out but it was switched off so could not be found. Historic call data was looked at to ascertain who she had been in contact with prior to going missing. The call data identified a mobile phone subscribed to an individual who was unknown to the girl's parents. Checks at the registered address of the mobile phone revealed that the missing girl was in the company of a 36 year-old man whom she had met in an internet chat room. He was reported to the Procurator Fiscal for sexual offences and offences in respect of the Communications Act 2003 for sending offensive, indecent and obscene messages.

In this case retained communications data was instrumental in identifying the man and ultimately finding the missing girl. Without this data, this lead might not have been identified.

A similar approach is adopted in France in relation to data retained under the DRD. The two examples provided below show how communications data was used to locate individuals who had were fugitives from justice.

In November 2005, the National Fugitive Search Brigade (Brigade Nationale de Recherche des Fugitifs - BNRF) was charged with investigating and locating an individual, known as "M GB", who was wanted following convictions by various courts on serious charges. The BNRF investigations in 2006 and early 2007, centred on the family circle and close relations of the M GB, and relied mainly on telephony. Interception of telephone communication did not provide any evidence of a connection between the fugitive and his family.
In February 2007, the fugitive's sister, "MB", was arrested on charges of organised fraud. The BNRF obtained some information about the fugitive's sister, in particular her aliases and her immediate circle of friends/acquaintances. One of the aliases, "LA", attracted the attention of the investigators. By cross-checking call records, it was shown that LA was in fact M GB.
A detailed invoice for the telephone line of M GB, (registered under an assumed name) provided call data over a one year period. This enabled calls to Senegal in March 2006 to be highlighted and associated with the telephone number assigned to LA. As a result the investigation relating to the fugitive focused on calls to and from Senegal, thus enabling phone numbers, obtained under assumed identities, to be identified as those of M GB's family. Then, thanks to new judicial interceptions and the help of the in-country liaison officer in the country where he was hiding, MGB was formally identified, located, and arrested by local police on 22 March 2007 in possession of false French documents under the alias "LA".

In April 2007, the TGI D charged the National Fugitive Search Brigade (Brigade Nationale de Recherche des Fugitifs - BNRF) with investigating M GJ-P who had been

on the run since his conviction in absentia in December 1997 when he was sentenced to 20 years' imprisonment for acts of rape of a minor aged 15 years or over. The BNRF took a keen interest in the fugitive's family circle and in particular his mother, Mme GJ. Detailed call records for the number of Mme GJ for the previous 12 months were requested from her telephone service provider. Examination of the call records enabled the identification of a telephone number in another country "P".
Investigations also showed that Mme. GJ was sending cash through Western Union to a person who was resident in P. This reinforced the evidence trail to a "P" as the country where her son was hiding.
The interception of the telephone line of Mme. GJ confirmed that she was making regular calls to her son who was living in P.
With the help of the liaison officer and local authorities in "P", M GJ-P was arrested in September 2007 pending extradition to France.

In Ireland, the power to access retained communications data is governed by the Communications (Retention of Data) Act 2011 which, in addition to allowing data to be accessed for the prevention, detection, investigation or prosecution of a serious offences and for safeguarding the security of the State, also allows the police access to data for the purposes of the saving of human life. It can readily be envisaged that in a kidnapping or missing person investigation location data could be a critical operational tool in locating a person who may be at risk of imminent, serious harm.

In summary, where data has been retained under the DRD it should be capable of being accessed for a wider range of purposes than serious crime providing they are consistent with EU law. The correct approach is to ensure that any data that is retained by service providers can only be accessed for a legitimate aim and when it is necessary and proportionate to do so. We would not support proposals to legislate on access to, rather than retention of, communications data.

4. More harmonisation of, and possibly shortening, the periods of mandatory data retention

The Data Retention Directive allows Member States to choose retention periods of between six and twenty four (6-24) months.

The evaluation report considers the statistical returns provided by Member States. The analysis showed that most requests for CD are for data less than 6 months old. However, this only shows part of the picture and it is often the more serious crime and terrorist investigations that are most likely to request data older than 6 months. This is particularly true for cross border investigations and certain types of crime.

Operation Overt was an extensive investigation in 2006 into a group of individuals influenced by Al Qaeda who planned to detonate home-made explosive devices aboard planes bound for the United States of America. This ultimately led to the change in rules concerning the transport of liquids in hand-luggage on planes leaving the UK.
In this investigation, communications data:

- provided evidence of the use of operational phones and attempts by the suspects to conceal communication through the use of telephone kiosks and calling card platforms

- indicated suspects' presence at survival training camps in the UK
- provided evidence of contact with further UK and overseas suspects
- provided evidence of calls from the suspects to Hydrogen Peroxide suppliers and follow-on enquiries provided evidence of actual purchases made
- indicated travel to the vicinity of a 'hide' in woods outside London where component bomb parts were buried.

The planning for this attack had been at an advanced stage, with the purchase of component parts and design and testing of the devices well underway. Expert evidence indicated that these devices were credible and would have resulted in catastrophic structural failure of the planes. Had the conspiracy gone undetected, the loss of life would have been considerable.

Operation Vivace was the investigation into four attempted bombings in the London area on 21st July 2005, mirroring those carried out a fortnight earlier on 7th July 2005. In this investigation, historic communications data:

- identified regular contact between the main five offenders and assisted in identifying further offenders who were arrested and charged with offences relating to the attacks
- placed some the offenders close to the attack scenes prior to and after the attempted attacks on 21st July 2005
- routinely placed four of the offenders in the vicinity of the bomb factory, including placing three of the defendants there the night prior to the attacks
- was crucial in evidencing two subjects who provided material assistance to offenders during their escape from London to the south of England, and then abroad, after the attacks.

These investigations were protracted investigations, lasting, at a minimum, several months, and up to several years, and with new information coming to light right up until the end. As more information was gathered, so further fresh target communications were identified. However, as each day passed, historic communications data was lost as it was deleted from Communication Service Providers' storage databases in line with data retention policy. Lost with it were potentially valuable leads.

Although most Member States have opted for retention period of between 6 – 12 months, Italy, Ireland and Poland have all opted for 24 month retention period.

The United Kingdom opted for a 12 month retention period. This was based on an analysis of the requests for communications data made by all police forces within the UK over a two week period in 2005. This exercise was repeated in 2010 and the picture was very similar to the earlier study, although in the later study almost a third of data used in crime investigations were between 7 and 12 months old. There are also some types of offences where the data is more likely to be over six moths old. For example, rape and child abuse cases may often not be reported to law enforcement until 6 months or more after the event. The 2010 study also showed that over 55% of CD used in sexual offence investigations was 6 months old or older.

The UK, France, and Ireland would find anything less than a 12 month retention period unacceptable, and would prefer to leave the retention periods as they are at present and allow Member States to choose the period that best suits them.

Wiltshire Police in May 2010 used retained communications data in a stranger rape investigation where the arrested offender had committed various offences all over the country spanning two years. Communications data plotting the suspect's movements going back one year helped identify linked offences in other forces' areas.

In section 4.5 of the evaluation report the Commission suggests "applying different periods of retention to different categories of data, different categories of serious crime or a combination of both". It is unclear what is intended in relation to "different categories of serious crime" because at the point of retention the purpose for which data may be accessed will not be known. It is also unclear if what is intended is to apply different retention periods for internet data and telephony data. When the Directive was introduced, Member States were allowed to postpone transposition of the internet access, internet telephony, and internet e-mail until March 2009. This was because of concerns about the some of the practicalities of implementing the Directive and in particular the availability of systems for storing the internet data. Some Member States have opted for different retention periods for internet communications data but it is not clear the extent to which technology and economics has influenced Member States' decisions.

The UK has a 12 month retention period for all communications data retained under the Directive. Although the statistics for IP communications data are based on a smaller number of requests, the recent survey reinforced the need for the same retention period for both fixed line/mobile telephony and internet communications data.

It is unclear from the Commission's evaluation report whether the proposal for different retention periods for different types of data was looking for some alternative split – for instance seeking to differentiate between subscriber data and traffic data. From a law enforcement perspective it would make no sense for an investigation to be able to access some types of data but not others because an arbitrary time period had passed. Such proposals would have very serious implications for criminal and terrorist investigations. For example, in the course of a single recent operation in the UK, 17 applications were made for traffic data, 45 applications for service-use data, and 58 for subscriber data. This makes a total of 120 applications overall for this specific investigation, which led to 9 convictions. This approach would also increase the administrative burden for all involved whether as service providers, law enforcement, data protection authorities and other oversight bodies.

On the 17th September 2009 the body of a taxi driver, Stuart Ludlam, was discovered shot dead in the boot of his taxi outside the train station in Cromford, Derbyshire in the UK.

Police carried out checks on the mobile phones the victim had with him at the time of his murder in order to try to help identify his killer but checks only showed numbers diverted from the taxi office's main phone number. Police then applied for call data for the taxi landline number to identify the last number to contact the victim and any other numbers that might be of interest to the investigation.

One number was identified from the call data to be the last to contact the victim just prior to the murder and could potentially be the call that lured him to the murder scene. However, the mobile phone was pre-pay with no subscriber details so the place of purchase for the phone and top up details were requested which showed a £5 top up being purchased at a supermarket petrol station a few days before the murder. The time of this transaction was known so CCTV footage was used to identify a man and showed him purchasing the phone at the supermarket earlier that day. This man was identified as Colin Cheetham.

Colin Cheetham was convicted of the murder of Stuart Ludlam and jailed for 30 years. Without the mobile and fixed line telephone data which identified the number that last contacted the taxi company, the information about the £5 top up and the purchase of the mobile phone in question, this suspect might not have been identified.

If it is necessary and proportionate to retain communications data then it is difficult to understand the rationale for mandating the retention of different parts of that data for different periods. There may be a separate issue about the extent to which all public authorities are entitled to access that data to fulfil their statutory duties. It is then the responsibility of Member States to put the correct controls in place to ensure that requests to access that data are only granted if they have satisfied the criteria of necessity and proportionality based on the specific requirements of the case. In other words the filter should be placed in relation to **access** not retention, and access is a matter rightly left to Member States to determine according to their national and European law.

5. Ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States

Article 4 of the Directive deals with access to data. It requires Member States to ensure that data retained in accordance with the Directive are provided only to the competent national authorities in specific cases in accordance with national law. It also puts the onus on Member States to ensure that the right processes and procedures are in place to ensure proper consideration of necessity and proportionality, subject to national and European law.

Law enforcement's use of data must be in accordance with the data protection principles. It is not a case of balancing public safety and data protection: we need both. The police also need to ensure accountability at all stages as this is key to achieving successful prosecution. This goes hand in hand with good data security.

Leaving aside the question of whether these proposals are within the current legal base of the Data Retention Directive, the concerns expressed by the Commission could be addressed by issuing guidance to Member States on the general principles and the need to comply with national and European law.

There are a number of different ways of ensuring independent supervision. For example:

In Ireland, the retained data is subject to the provisions of the Data Protection Acts (which give effect in Irish law to European data protection law) and the service providers are therefore, subject to supervision by Ireland's national data protection supervisor. The Communications (Retention of Data) Act 2011, which transposes the 2006 Directive, provides for additional specific, independent oversight mechanisms to ensure that access to retained data for the purposes of law enforcement is carried out

in accordance with law.

Any person who believes that data relating to them which are in the possession of a service provider and have been accessed in response to a disclosure request, may apply to the 'Complaints Referee' for an investigation. The office of the Complaints Referee is established in law and the holder of the office a Judge of the Circuit Court.

The Complaints Referee shall investigate whether the alleged disclosure request was made and, if so, whether any of the provisions governing access to retained data set out in law were contravened. If a complaint is upheld, the Complaints Referee has the power to direct the destruction of the data and compensation for the applicant. If the Complaints Referee finds no contravention he must so notify the applicant.

There is an additional independent judicial oversight mechanism. A serving Judge of the High Court is designated to keep the operation of the provisions under review, to ascertain whether those authorised by law to seek access to retained data are complying with its provisions of the data retention law and to report on such matters as he considers appropriate.

The Act also provides that the powers of the designated Judge in relation to data retention are without prejudice to the independent data protection enforcement functions of the Data Protection Commissioner under the Data Protection Acts.

It is important to note that in accordance with the Irish Constitution members of the judiciary are independent in the performance of their functions. It should also be noted that both the Complaints Referee and the Designated Judge report to the Taoiseach (Prime Minister).

In the UK, public authorities who use communications data all have individuals who are trained to fulfil the following roles to ensure that data is lawfully acquired and is subject to proper oversight:

- A **Designated Person** is a senior officer to whom all requests for data are made. The Designated Person must consider the necessity and proportionality for any intrusion into a person's privacy arising from the acquisition of communications data in every case. The Designated Person is generally expected to not be connected to the investigation in question unless "need to know" requirements mean this is not possible. The public authorities and the ranks of these authorising officers are specified in law.

- The **Single Point of Contact (SPoC)** is a specially trained expert in the use of communications data and the privacy impacts of using this data. All requests for communications data must go through the SPoC who provides advice to the designated person and processes the request from the public authority to the communications service provider.

- The **Applicant** is the officer in the public authority who makes the request for the data, for example a police officer investigating a crime.

- The **Senior Responsible Officer** is the person responsible within the public authority for their use of communications data and compliance with the law.

The process is generally as follows: the Applicant works with the SPoC to establish

what data is required, on what grounds, and then to draw up the request for acquiring it. The request then goes to the Designated Person who considers its necessity and proportionality. The Designated Person, if content, will approve the request and return the authorisation to the SPoC who will then acquire the data on behalf of the Applicant. Steps are taken to ensure that data is transferred by secure means such as a dedicated secure portal or encrypted email.

Over and above the safeguards and accountability procedures built in to the acquisitions process, there is also independent oversight from the **Interception of Communications Commissioner**. He operates independently of Government to scrutinise public authorities' use of communications data and the systems in place for this data. The Commissioner inspects public authorities and visits communications service providers in the course his duties. He reports to the Prime Minister specifically on this and publishes a public report on his findings annually. The Commissioner must hold or have previously held high judicial office.

In addition to this, if an individual believes that their communications data has been acquired unlawfully, they have the right to complain to the independent **Investigatory Powers Tribunal** who can investigate the claim. The Tribunal can impose sanctions if wrongdoing is found, including ordering the destruction of unlawfully obtained data and financial compensation to the individual making the complaint.

The European Data Protection Supervisor (EDPS) has expressed concerns about the way in which some Member States have implemented the directive and questioned the extent to which they have adhered to the requirements of national law and the Data *Protection* Directive. It is unfortunate that this has detracted form the very real value of the Data Retention Directive, but we believe that the solution is to enforce the adherence to the existing national and European law rather than trying to create further legislation through the Data Retention Directive.

The Data Retention Directive puts the requirement on Member States to implement the Directive in ways that are compliant with data protection requirements and it is flexible enough to enable Member States to do this. We believe that this is the correct approach and it is not appropriate within the terms of the Data Retention Directive to seek to regulate matters relating to law enforcement's access to data.

6. Limiting the authorities authorised to access the data

The same arguments apply as set out in section 5 above. It is for Member States to determine which "competent national authorities" should be entitled to access retained data based on the statutory duties of the public authority. Criminal justice systems vary between different Member States. For example some Member States use investigating magistrates in addition to the police, so it would be hard to devise a scheme on the face of the Directive that would be appropriate in all Member States.

7. Reducing the categories of data to be retained

The evaluation report provided no justification for seeking to reduce the categories of data retained.

The Commission's report shows that mobile telephony data is generally the most commonly accessed data type, followed by fixed network telephony, and internet data accessed the least. However, internet data is extremely valuable and will play an increasing role in future as more and more communications take place over the internet.

The statistical information available shows that more use is made of fixed line and mobile telephony communications data than is currently made for internet communications data. This is unsurprising given that law enforcement's understanding of IP communications data is less mature than traditional telephony. If we were discussing the Directive in the late 90's the same arguments could be made about fixed line and mobile telephony.

The apparent lack of evidence in the form of statistics on the use of internet data should not be taken as a sign that it is not valuable, particularly since most Member States chose to defer transposition of the internet provisions of the DRD to 2009, wishing to allow adequate time to ensure that technology and systems for retention of internet data could be put in place. This means that there is less experience and a smaller statistical base.

The rapid increase in the use of the internet for communications and the rise in online crime have reinforced the need for law enforcement to be able to access internet data and improve their analytical skills to obtain full benefit from the data. The UK is currently undertaking a programme of work to train its law enforcement agencies in the use of internet data to ensure that valuable retained internet data is employed to best effect now and in the future.

In the United Kingdom fixed line and mobile telephony still accounts for around 90% of requests for communications data but where internet data is required it is just as critical to an investigation. There are certain types of crime which exist solely online, such as hacking, online fraud, cyber harassment, and the sharing of child abuse images, where retained internet data is crucial and sometimes the only way of progressing an investigation.

> Internet data was used in the UK in an investigation into the grooming of a 13 year-old girl via the Internet. Examination of the victim's computer by the E-Crime Unit revealed an email address of a person having sexual chat on a MSN chat room with the victim. The girl had also been coerced into sending naked photographs of herself via email and had exposed herself during web cam chat. Police officers made enquiries about the e-mail address which revealed the IP address subscribed to a man from Wales, giving his name and address. Further investigation resulted in the man being cautioned and charged.
>
> It was assessed that without the acquisition of the communications data, this incident might have led to crimes of a more serious sexual nature.

Technology is moving forward and increasing use is made of internet communications, whether through computers/lap tops or smart phones which combine both mobile telephony and internet communications (voice and data). If law enforcement is to maintain its current capability in future, it is crucial that internet data continues to be retained beyond 6 months.

Because our knowledge and experience of internet data was less mature when the DRD was negotiated, the provisions for internet access, internet e-mail, and internet telephony are perhaps less suited for purpose than the provisions around telephony. For example, data necessary to identify the date, time and duration of a communication is dealt with better in the telephony provisions (which specify the start and end of the communication) than those

for internet email which only specify the log in and log off times for someone accessing the email service (and not the timestamps on the email communications themselves).

There may in future be scope to improve the provisions around internet data but we believe that there has not yet been adequate time to evaluate the effectiveness of the existing provisions. We should be seeking to ensure that the directive remains technology neutral so it can cope with the changes that technology will bring, rather than seeking to limit the categories of data retained within the existing Directive.

Some arguments have been raised suggesting that rather than limiting the categories of data we should be seeking to expand them (e.g. to include Information Society Services ISS). While there may be merit in this argument, the DRD is a mandatory derogation from the E-privacy Directive 2002/58/EC which is in turn part of the Regulatory Framework for electronic communications and ISS are specifically excluded from the framework.

8. Guidance on use of data including the prevention of data mining

It is unclear what the Commission envisage here but we have no objection in principle to guidance reminding Member States of what is or is not permitted under EU law – but this should be guidance and would not require a change to the Directive.

9. Developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument

Article 10 of the Directive requires Member States to provide the Commission with statistics on a yearly basis which shall include:

- the cases in which information was provided to the competent authorities in accordance with national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
- the cases where requests for data could not be met.

There has been some criticism of the quality of statistical returns to the Commission. While this has been caused in part by genuine confusion about what was required, there is some justification for this criticism. Part of the scope for confusion is caused by the interrelation between the e-privacy Directive and DRD, for example some Member States were not including subscriber checks. The template issued by Commission added to the confusion.

Under "the cases in which information was provided" and "cases where requests for data could not be met " it was unclear what "cases" meant and different Member States have interpreted this differently. It could mean each and every item of data that was or was not provided, or each investigation in which there might be multiple requests for multiple items of data. Similarly, where the request to a service provider is for more than one item of data, the data may be of different ages. Recording the age of individual data records can increase the costs to service providers and/or consume valuable LEA investigative resource. Increasing use of automated interfaces and handover interfaces could help with the gathering of statistics but only once it is clear what is required.

"Cases where requests for data could not be met" is also ambiguous for another reason– does it mean cases where i) the service provider was unable to provide data that should

have been retained under the directive but wasn't; ii) data that is wanted but does not fall within the scope of the Directive, or iii) data that had been retained but was then deleted because it was after the specified retention period? Despite these problems a number of Member States have provided detailed quantitative information and qualitative examples to demonstrate usage and value of CD. However, clearer guidance from the Commission could address this issue and result in more meaningful statistical returns without the need for changes to the Directive.

There is another area where the recorded statistics do not give a full picture and that is the exchange of communications data between Member States. The evaluation report relies on recorded Mutual Legal Assistance Treaty requests (MLAT). Mutual Legal Assistance Treaty, and Commission Rogotoire, can be slow, adding to delays in identifying communications and the loss of associated data so law enforcement are keen to establish more effective ways of obtaining communications data. The MLAT figures do not reflect all of the requests or the joint investigations whether through INTERPOL or bilateral arrangements between police forces in different Member States.

10. Alternatives to Data Retention

The Commission's evaluation report recognises that data preservation or "quick freeze" is not an adequate replacement for data retention. Though considered by some to be less intrusive than data retention, there are problems with its implementation for security and law enforcement purposes which undermine its value. It does not guard against vital historical data being deleted and provides no consistency in what types of data will be available between different providers and for how long, instead leaving it to individual differences in the business models of service providers to determine this. If data preservation was used instead of retention, the unpredictability of the amount, type, and age of data available would create a very worrying lack of certainty for law enforcement. Data preservation also has very limited value in terms of the prevention of crime.

> In March 2011 UK police used mobile phone communications data to dismantle a cocaine trafficking ring that stretched from London to South Wales. Officers used the communications data from thousands of calls made over the previous 12 months between more than a dozen mobile phones to link foot soldiers at the bottom of the gang to those at the top who 'didn't want to get their hands dirty'.
>
> Two members of the gang were arrested with 3.58kg of cocaine (worth £143,000) and their mobile phones were seized. Detectives then spent months piecing together the jigsaw of phone calls to prove links between the other members of the group. This resulted in the six gang members being jailed for a total of 53 years and the investigation also involved confiscating £53,000 in cash which is being used to fund police operations targeting other drug dealers.

11. Conclusion

France, Ireland and the United Kingdom believe that the Data Retention Directive (2006/24/EC), (DRD), in its current form provides a valuable basis for data retention across the EU which is flexible and sensitive to the differences between Member States' criminal justice systems. The issue of access to data retained under the Directive is an issue for Member States and the responsibility lies with them to determine that effective safeguards are in place to ensure that retained data is only accessed in accordance with national and

European law. We believe that the Commission's objectives could be achieved through guidance to Member States, and that there is no case for making changes to the Directive.