COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 21.9.2005
SEC(2005) 1131

COMMISSION STAFF WORKING DOCUMENT

Annex to the:

Proposal for a Directive of the European Parliament and of the Council

on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC

EXTENDED IMPACT ASSESSMENT

{COM(2005) 438 final}

1. WHAT PROBLEM IS THE PROPOSAL EXPECTED TO TACKLE?

1.1. Introduction

Citizens increasingly perform daily activities and transactions using electronic communications networks and services. Electronic communications are considered by EU Heads of States and Governments as a *powerful engine for growth, competitiveness and jobs in the European Union* on its way to the knowledge economy.

Each and every move over electronic communications networks generates so-called 'traffic data' i.e. *data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof.*[1] Traffic data include details about time, place and numbers used for fixed and mobile voice services, faxes, e-mails, SMS, and other use of the internet. Subscriber (and sometimes user) data, such as the name and address of the subscriber, are also processed by providers or subscription-based electronic communications services.

To protect citizen's fundamental rights and freedoms, and in particular their privacy and personal data, Community law provides for the deletion of traffic data once it is no longer needed for the purpose of the transmission of the communication. Some may however be kept and further processed by service and network providers for their own business purposes such as billing or with the consent of the consumers.

Beyond these business purposes, 'public order' purposes can also be invoked to justify the further processing of traffic data.[2] There is no doubt that the availability of traffic data can indeed be important for certain 'public order' purposes such as specific national security threats or specific investigations into criminal offences.

This is why public authorities in the Member States are in principle, if necessary and in accordance with applicable law, able to request access to traffic data stored by electronic communications operators for their own business purposes. Legitimate requests for the retention of specific data – otherwise called data preservation – are also allowed when necessary for specific purposes, such as investigations and prosecutions. Data preservation ensures the onward storage of specific data on specific users as from the date of the request.

However, with changes in business models and service offerings, such as the growth of flat rate tariffs, pre-paid and free electronic communications services, traffic data may not always be stored by all operators to the same extent as they were in recent years, depending on the services they offer. This trend is reinforced by recent offerings of Voice over IP communication services, or even flat rate services for fixed telephone communications. Under such arrangements, the operators would no

---

1 Article 2a of Directive 2002/58/EC on Privacy and electronic Communications (OJ L 201, 31 July 2002)

2 "Public order' purposes are understood in the present document as referring to the public order interests mentioned in Article 15 of Directive 2002/58: national security (i.e. State Security), defense, public security, the prevention, detection and prosecution of criminal offences or of unauthorized use of the electronic communications system. For the sake of this document, law enforcement purposes are understood as restricted to the prevention, investigation, detection and prosecution of criminal offences.

longer have the need to store traffic data for billing purposes. If traffic data are not stored for billing or other business purposes, they will not be available for public authorities whenever there is a legitimate case to access the data. In other words, these developments are making it much harder for public authorities to fulfil their duties in preventing and combating (organised) crime and terrorism, and easier for criminals to communicate with each other without the fear that their communications data can be used by law enforcement authorities to thwart them.

To respond to this concern, a number of Member States have adopted, or planned to adopt, national general data retention measures. Compared to data preservation measures, which are targeted at specific users and for specific data, general data retention measures aim at requiring (some or all) operators to retain traffic data on all users so that they can be used for 'public order' purposes when necessary and allowed.

The need to take legislative action in this area at the European level has most recently been confirmed by the European Council in its Declaration on Combating Terrorism of 25 March 2004, adopted shortly after the horrific events in Madrid on 11 March. In that Declaration the European Council explicitly recognises the importance of legislative measures on traffic data retention, through its instruction to the Council to examine measures in the area of "proposals for establishing rules on the retention of communications traffic data by service providers". The European Council Declaration continues to state that "Priority should be given to proposals under the retention of communication traffic data (…) with a view to adoption by June 2005". The priority attached to adopting an appropriate legal instrument on this subject was recently confirmed in the Conclusions of the European Council of 16 and 17 June, as well as at the special JHA Council meeting of 13 July 2005 following the London terrorist bombings.

1.2. The importance of traffic data for law enforcement

To provide some perspective on why the European Council and a significant number of Member States call for data retention measures, it is important to realise the importance of traffic data to serious criminal and terrorist investigations. In this context it should be recalled that traffic data includes both data on contacts made through the use of 'standard' mobile and fixed telephony and data related to internet usage. As law enforcement authorities have indicated during the consultation process on this issue, traffic data is therefore not only important for preventing and combating serious offences and terrorism, including serious forms of cybercrime. According to recent research, the results of which were presented by one Member State in discussions in Council on the issue of data retention, the large majority of traffic data requested by law enforcement relate to mobile and fixed telephony, and only around 15% to internet-related data.

In terms of the importance of traffic data for serious criminal offences and terrorism numerous examples were provided to the Commission in the consultation process, ranging from the investigation in the Madrid bombing, where telephone data up to six months old was investigated, to the Omagh bombing, the murder of French Prefect Erignac, of famous Irish journalist Veronica Guerin, other murder cases,

extortion attempts etc. Examples were also given where traffic data was used to exculpate the defendant.[3]

As an example of usage of internet traffic data to solve an 'ordinary' crime relates to a murder investigation. In this case, a young woman was found murdered in her apartment. No technical traces were found at the crime scene. When the woman's computer was analysed, traces of Internet chat traffic were found. The person with whom the woman had been chatting could be traced by means of IP addresses and logs saved by the ISP. The offender was arrested and during the interviews he also confessed another attempted murder.

A recent public study on the necessity for law enforcement to have access to traffic data was presented by the Law Faculty of the Rotterdam Erasmus University on 20 June 2005[4]. This study focussed on 65 different cases in which telecommunications traffic data had played a major role, and confirmed the importance of traffic data for all sorts of investigations, including murder and kidnapping. Perhaps not surprisingly, especially in kidnap cases the data on the location of a mobile device often played a crucial role. It also confirmed that the more important the criminal case, the longer the investigation, and thus the older the data which are requested. In fact, the study suggests that especially investigations into serious organised crime, large fraud investigations, cases involving requests for mutual legal assistance, so called "cold cases" and terrorism would benefit most from a retention period of one year.

In addition to examples of cases where traffic data was in fact used successfully to solve crimes, examples were also provided where traffic data had already been deleted by the time the request reached the communications service provider in question, such as in a murder case in western France. The law enforcement authorities of another Member State indicated that of requests made for Internet related data, 30 to 40% remained unanswered because the data had already been deleted.

Cybercrime – understood within this document as offences committed through usage of the internet - continues to be an increasing threat. It erodes faith in further development of e-commerce, and contributes to damaging the interests of citizens and businesses alike through attacks against information systems, fraud and identity theft, and the on-line distribution of child pornography. Whilst the Member States and the European Union have taken a number of initiatives to combat cybercrime, including the recently adopted Framework Decision on attacks against information systems[5], recent figures illustrate that damage to business alone is staggering. As an example, the 2005 study commissioned by the UK National Hi-Tech Crime Unit on the damage to business of high tech crime in the UK alone showed that the estimate of this damage is around 2.5 billion pound, or 3.75 billion euro for 2004.

---

3 Statement of John Abbott, C.B.E, QPM, B.A. (Hons), former Director General of the National Criminal Intelligence Service, UK, at the First Plenary Session of the European Union Forum on Cyber crime.

4 "Wie wat bewaart die heeft wat" ; available at http://www.europapoort.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vh1iiavsmqwi.pdf

5 OJ L 069, 16/03/2005 P. 0067 - 0071

Some law enforcement experts have compared traffic data to fingerprints: whereas in the physical world physical evidence can be gathered, in a digital world traffic data is the digital equivalent to fingerprints.[6]

Apart from the significant monetary damages caused by cybercrime, the internet has also created extended opportunities for distribution and sales of child pornography. The necessity of having access to traffic data in such cases was also recently demonstrated in a large international child porn investigation, co-ordinated by Europol.[7] In that particular case, IP addresses of persons who were downloading child pornography of the internet were found by law enforcement in one Member State, and subsequent arrests were made in 12 Member States, based on those IP addresses. However, in five further Member States those IP-addresses could not be linked anymore to individual users, since the relevant data had already been deleted by the Internet Service Providers.

The retention of traffic data can also be important to combat organised crime in the area of intellectual copyright infringements.[8]).

Investigations into serious crime, such as organised crime and terrorism, are almost automatically international investigations, given the nature of the organisations involved. This often means that international co-operation needs to be sought, either using traditional methods of mutual legal assistance, or through the use of instruments such as Europol and Eurojust. Even with the increased speed these new institutions provide for requesting and exchanging relevant information, in particular traffic data, clearly these procedures take time. If traffic data is not retained for a reasonable period, requests for such data will be in vain – by the time the request reaches the operator through an authorised law enforcement officer, the data may well have been deleted already.[9]

It should come as no surprise then that Michael Kennedy, the President of Eurojust, stated at the extraordinary Council meeting of 13 July that a retention period of a year would be preferable.

1.3. Current Legal Situation

Whilst the Declaration on combating terrorism and the Council Declaration on the EU Response to the London bombings referred to in paragraph 1.1. clearly demonstrate the political imperative of adopting appropriate legislative measures at the level of the European Union on traffic data retention, the dilemma of how to find an appropriate balance between the fundamental rights of the individual to data

---

6 "In the case of a crime committed wholly or partially in the E-World, if there is not traffic data, there can be no investigation. It is as simple as that." Statement of John Abbott, C.B.E, QPM, B.A. (Hons), former Director General of the National Criminal Intelligence Service, UK, at the First Plenary Session of the European Union Forum on Cyber crime.

7 See Europol press release of 14 June 2005, available at www.europol.eu.int.

8 Letter of July 2005 to this effect by the CMBA, the Creative and Media Business Alliance.

9 One example of an international case, provided to the Commission during consultations, concerns an attack against a US Government website, which instigated a request for mutual legal assistance, through which identification of users of four IP addresses was requested. Even though in this case the time period between the request being received and acted upon was only just over a month, the identification of the users of the four IP addresses was not possible since the relevant data had already been deleted by the Internet Service Providers concerned.

protection and privacy and the freedom of expression, and the needs of the State to have adequate tools to safeguard the lives and property of its citizens is already reflected in the current legal framework, and in particular in Directive 2002/58/EC on Privacy and Electronic Communications[10]. This Directive complements Directive 95/46 on the processing of personal data and the free movement of such data as regards the electronic communications sector.

Directive 2002/58/EC does not however provide for a full harmonisation of conditions under which national legislative measures may provide for the retention of traffic data for 'public order' purposes. Under Article 15(1) of this Directive, such measures have to be necessary, appropriate and proportionate within a democratic society

While this leaves some discretion to Member States on the exact level of protection they intend to ensure on their territory using the 'public order' derogation, this does not exempt possible national measures from verification of their respect for their obligations under the Directive and Community law generally, including the obligation to respect fundamental rights and general principles of Community law such as those enshrined in the European Union Charter of Fundamental Rights and the European Convention on Human Rights.

1.4. Impact of the current situation on the electronic communications industry

The data retention regimes introduced or planned by the Member States vary significantly with respect to *inter alia* their scope, the purposes for which they have been adopted or planned, the data to be retained, the duration of the retention, the reimbursement possibilities, and the conditions for access to the data. As already indicated in the Eight Report on the Implementation of the Telecommunications Regulatory Package, the Commission is of the view that there is '*a need for clarity from Member States regarding their overall approach to traffic data retention'*.[11]

There is at present a patchwork of national data retention obligations in Member States, which can be summarised as follows:

- A majority (about 15 according to 2004 figures) of Member States at present do not have mandatory data retention obligations;
- In about half of the Member States with mandatory data retention obligations laws in place, data retention is not operational since implementing measures are still missing;
- In those Member States with data retention obligations in operation, the period (between 3 months and 4 years) and scope vary substantially e.g. just pre-paid mobile, not the Internet, all services etc.

Within this context it should be recalled that the ICT industry is a major economic sector in its own right, covering information technology, electronic communications and audio-visual markets. The EU has long recognised that this is a key sector whose development is to be encouraged. At the European Council in Lisbon in March 2000,

---

[10] OJ No L 201, 31.7.2002

[11] Communication of 3 December 2002, p. 6 (COM(2002) 695)

Heads of State and Government of the European Union launched a strategy to prepare the EU for the challenges of the new century. This has become known as the "Lisbon strategy". The objectives set at Lisbon – higher growth, more and better jobs and greater social inclusion – were ambitious. Information and communication technologies (ICT) were identified as playing a key role in achieving them. This key role of the 'Information Society for all' was confirmed at the European Spring Council 2005[12] and in the Communication of the Commission: i2010 – A European Information Society for growth and employment[13].

The impact of the current situation is mainly twofold. On the one hand, diverging national legislations on traffic data retention have a significant negative impact on this major economic sector. This point has also been stressed time and again by contributions from industry to the public debate on data retention.

On the other hand, obligations related to traffic data retention have in any event cost effects on the providers of electronic communication services. As analysed below, these costs are notably associated with the adaptation of existing systems, the storage, and the resources to deal with requests for access to data from law enforcement authorities. These depend in particular on the types of data which need to be retained; the actual length of the retention period, and whether or not these periods are harmonised throughout the European Union.

1.5. Conclusion

In summary, the problem which the proposal for a Directive on retention of traffic data aims to address is that law enforcement authorities are slowly but surely losing one of their most important instruments for preventing and combating (organised) crime and terrorism – access to traffic data retained by electronic communications providers. The current situation is therefore one which is unsatisfactory in terms of addressing the serious concerns voiced by the European Council, and in terms of addressing the consequences of the diverging measures adopted by Member States for the effectiveness of international law enforcement co-operation, as well as the consequences for electronic communications service providers, especially those who provide services in different Member States of the European Union.

2. WHAT ARE THE OVERALL POLICY OBJECTIVES ?

The overall policy objective of the proposal is to provide for a European wide harmonisation of legislation on retention of traffic data which balances in a proportionate manner the needs of law enforcement, the fundamental rights of the citizens and the interests of the electronic communications industry. This European wide harmonisation should furthermore be achieved on the appropriate legal basis in order to provide legal certainty to all involved.

In terms of concrete policy objectives the proposal should:

---

12 "Report from the Commission to the Spring European Council. Delivering Lisbon. Reforms for an Enlarged Union", COM(2004) 29.

13 COM(2005) 229 final

– ensure that traffic data remains available for a reasonable period of time in order to contribute to the continued efforts to prevent and combat serious crime, such as terrorism and organised crime, including cybercrime;

– ensure that the retention and further processing of traffic data is in line with the general Community legal framework, and in particular with existing legal instruments on fundamental rights and data protection;

– ensure that traffic data retained may be only provided to law enforcement authorities in specific cases and in accordance with national law for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences such as terrorism or organised crime;

– ensure the creation of a level-playing field for operators, so that no distortions in the market for electronic communication services are created or continue to exist due to different national approaches to the issue of traffic data retention, including the compensation of the additional cost incurred;

– ensure that traffic data is retained in such a manner that legitimate requests from law enforcement authorities for information can be answered swiftly;

– ensure that the rules to be established with respect to the actual data to be retained can be adapted quickly to respond to changes in the electronic communications technology or law enforcement needs;

– ensure that reliable statistical information is gathered and analysed on traffic data retention in order to be able to reliably assess the impact of the Directive on law enforcement, citizens and industry;

– ensure that a constructive dialogue is instituted between law enforcement, industry and data protection authorities in order to create an effective public-private partnership in this area.

All these policy objectives should be achieved in line with the overarching policy objectives established under the Lisbon Agenda, the creation of a European Area of Justice, Liberty and Security, as well as the general policies on the Information Society, Safer Internet and combating of cybercrime.

In this last area in particular, reference is made to the Commission's Communication on Creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime.[14] The retention of traffic data was already mentioned in paragraph 5.2. of that Communication: "The Commission considers that any solution on the complex issue of retention of traffic data should be well founded, proportionate and achieve a fair balance between the different interests at stake. Only an approach that brings together the expertise and capacities of government, industry, data protection supervisory authorities and users will succeed in meeting such goals. A consistent approach in all Member States on this complex issue would be highly desirable, to meet the objectives of both effectiveness and proportionality and to avoid the situation where both law

[14] 26.1.2001, COM(2000) 890 final.

enforcement and the Internet community would have to deal with a patchwork of diverse technical and legal environments."

The proposal should constitute a positive answer to the concerns of law enforcement authorities to have access to certain data when necessary and proportionate, while preserving the coherence of Community law, ensuring the necessary degree of harmonisation in terms of both the fight against terrorism and organised crime, and the functioning of the internal market.

3. WHAT ARE THE MAIN POLICY OPTIONS AVAILABLE TO REACH THE OBJECTIVES?

3.1. Introduction

A number of different policy options to reach the objectives described above in Section 2 have been considered by the Commission in the preparation of this proposal, most of which were discarded at an early stage given the developments in this area over the past few years. The options which were discarded at an early stage were the "do nothing" option, self-regulation and "soft-law" approaches. Other options included a third pillar legal instrument, in the form of a Framework Decision on data retention. This is the option which was preferred by four Member States when they presented a draft Framework Decision on data retention in April 2004, but was discarded by the Commission on legal grounds, as explained below. A final option was an instrument on data preservation, as suggested by industry and data protection authorities.

This Section also presents the main arguments which have led the Commission to conclude that the only viable option to reach the policy objectives outlined above is a Directive on the retention of telecommunications traffic data. In terms of policy options within that chosen alternative a number of other important choices made in the preparation of the proposal. are also clarified. These relate to the actual retention periods chosen, the differentiation between telephony data and data based on the Internet Protocol, as well as the importance of a cost reimbursement scheme.

3.2. The "do nothing" option

The first option to be considered with any proposal is what the consequences would be if no action were to be taken at all. In that case, the difficulties described in detail in Section 1 would in all likelihood continue to increase: less availability of crucial data for (international) law enforcement investigations, and a patchwork of different national laws dealing with data retention which would hamper international co-operation, and put an increased burden on the telecommunications industry, leading to increased costs and a possible lack of innovation. For these reasons this option was considered to be unacceptable.

The possibility that the Council would adopted a Framework Decision on data retention would also be less than satisfactory from the Commission's point of view, mainly given the legal difficulties associated with this option identified in paragraph 3.4.

3.3. Self-regulation and soft law

When considering self-regulation and possible "soft-law" options such as recommendations, reference needs to be made to the efforts in previous years to come to such solutions through intensified consultation with stakeholders. In 2002, for example, the Council explicitly called for a dialogue at national and EU level *aimed at finding solutions to the issue of traffic data retention that satisfies both the need for effective tools for prevention, detection, investigation and prosecution of criminal offences and the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy, data protection and secrecy of correspondence.*[15] Although public consultation and debate on this issue has been wide-spread, including discussions at the European Parliament, no common solutions have emerged from this.

Another important consideration, however, is that the European Council has already called for a legislative proposal in this area. A legislative solution has also been proposed in the form of a draft Framework Decision.

Given these various elements, there is little doubt that the only way in which the objectives described in Section 2 can be reached is through legislation.

3.4. First or third pillar legal instrument?

The call for action on European legislation in the area of retention of traffic data mentioned in paragraph 1.1. has given rise to a first initiative by four Member States (France, Sweden, the UK and Ireland) which have proposed a draft Framework Decision on this topic on 28 April 2004[16]. This initiative has in the meantime been discussed at numerous Council Working Groups and at the Council. itself. Whilst it would go too far within the context of this document to analyse the proposal in all its details, the main point to be recalled here is that its proposed legal basis is Title VI of the Treaty on European Union – a third pillar legal basis. In terms of its content, the proposal aims to regulate two distinct issues: harmonisation of retention periods across the EU, including the types of data to be retained, and access to and exchange of such data by the law enforcement authorities of the Member States.

This issue of the correct legal basis for such proposals has recently been addressed in a Commission Staff Working Paper.[17] In short, the position outlined in this document is that the issue of retention of traffic data has already been dealt with in previous legal instruments based on a first-pillar legal basis, such as Directives 2002/58/EC and 95/46/EC mentioned above. The analysis continues to state that it was only due to the fact that no political agreement on the actual length of retention could be reached that this issue was not harmonised more fully in Directive 2002/58/EC, and concludes that therefore any further legal instruments on retention of traffic data as such (as opposed to provision regulating the exchange of and access to such data by law enforcement) must also take place on a first pillar legal basis. This logic is confirmed in Article 47 of the Treaty on European Union, which regulates the relationship between the Treaty on European Union and the EC Treaty, stipulating

---

15 Council Conclusions of 19 December 2002.

16 Doc 8954/04, CRIMORG 36, TELECOM 82.

17 "Projet de décision cadre sur la conservation des données – Analyse juridique" – (SEC(2005) 420) – 22.3.2005

that no legal instruments adopted under the Treaty on European Union may affect the legislative framework adopted under the EC Treaty.

In summary then, whilst the Commission shares the concerns of the Member States which have presented the proposal for a Framework Decision on traffic data retention, and wants to achieve the same objectives as those specified in the proposed Framework Decision, it is of the opinion that the legal basis chosen to achieve those objectives is partially not legally correct. It is the Commission's position that the legal basis for imposing obligations on electronic communications service providers can only be found in the first pillar, whilst regulation on access to and exchange of such data by law enforcement authorities can only be built upon a third pillar legal basis.

The reasons for choosing a first-pillar legal basis for regulating the obligation on providers of electronic communication services are indicated above. At the same time, an option would have been to present an additional proposal to regulate the aspects of international law enforcement co-operation, as well as access to retained data, which should properly be regulated under a third pillar legal instrument.

However, the Commission is of the opinion that there is no real necessity to provide for a sectoral approach to the issue of mutual legal assistance, which would only be applicable to the exchange of traffic data, and to the conditions under which requests from authorities from other EU member states must be complied with. These issues are to a large extent already regulated in general mutual legal assistance treaties and other co-operation mechanisms. If there is indeed a need to provide for specific regulation on these issues, this should take place through inclusion of relevant provisions within those general instruments and mechanisms.

3.5. Which first pillar legal instrument?

When considering the different options for a first pillar legal instrument, the choice then needed to be made between a regulation or a Directive. The option of a proposal for a Directive provides the harmonisation level needed in the internal market. Compared to a regulation, it leaves in a sensitive area some margin of manoeuvre to Member States on the implementation. A regulation would have been too stringent, notably in view of the different technical architectures used by the various operators in different countries. The Directive will leave sufficient margin to Member States to adapt to national constraints. In any case, the status quo is no longer tenable in view of the obstacles created by the national differences in this area.

Harmonisation of retention periods can not be achieved by the Member States themselves. Given the fact that the effectiveness of law enforcement investigations in these cases is heavily dependant on international co-operation, and the negative effects of different national choices on the electronic communications market, European wide harmonisation of traffic data retention schemes is the most appropriate policy choice. The same is true for the choice for a cost reimbursement scheme – without inclusion of such a scheme in the Directive a level playing field for the providers of electronic communication services would not be guaranteed (see also paragraph 3.8). Nevertheless, the choice for a Directive, as well as the choice for a rather 'generic' list of data to be retained, in combination with a Comitology procedure to provide for regular updates of that list as necessary, will provide for the necessary flexibility.

3.6. Data Preservation versus Data Retention

The call for traffic data preservation as an alternative to a traffic data retention scheme has come not only from industry, but also from data protection authorities and civil rights interest groups. Under data preservation schemes, law enforcement authorities have the opportunity to request electronic service providers to retain particular data on a particular person or persons, whereas data retention schemes provide for the retention of traffic data on all users of electronic services. At first glance, this seems an attractive policy option: the number of persons on whom data will be retained and processed for law enforcement purposes is drastically reduced under this option, and consequently the associated costs for industry will be negligible. An additional argument which is sometimes put forward by proponents of this alternative is that this is the approach taken in the United States, and that it seems to work satisfactorily there. This impact assessment therefore needs to explain why this policy option is not satisfactory in terms of addressing the objectives outlined under Chapter 2 of this document.

In fact, data preservation is a very useful tool for law enforcement authorities. Undoubtedly, in those cases where a suspect has been identified, or where an investigation into for example an organised crime group or terrorism cell is underway, requests for preservation of traffic data are an indispensable tool to establish the connections between suspects and their contacts and associates. At the same time, the logical limitations of this approach can be easily explained – with only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects.

The simple scenario given by one of the law enforcement experts during consultations, which was outlined above in paragraph 1.2., already indicates that data preservation by itself is not enough for law enforcement authorities to actually be able to investigate and solve crime and terrorism cases. As indicated above as well, the investigation into the Madrid bombings relied heavily on obtaining and analysing traffic data going back 3 to 6 months. It should be clear to anyone that depriving law enforcement authorities of the possibility to look into what happened prior to the crime being committed makes their work next to impossible. One can draw a comparison with investigations in the physical world – how effective would law enforcement be if prior to the start of an investigation all physical evidence were to be removed from the crime scene?

In comparison with the situation in the US, it should be noted that there is a significant difference between the US situation and the European one – there is no data protection legislation in the US which obliges communications service providers to delete data once they are no longer necessary for business purposes. As a consequence, data can be kept for a longer period by those service providers, making it somewhat easier for US law enforcement authorities to obtain the necessary data. US Government representatives have stated, however, that "data preservation could be much less effective in the European context".[18]

---

[18] Statement US Government on data retention at Article 29 Working Party meeting on data retention, 14 April 2005. These statements were followed by the observation that "This affirmative obligation to destroy traffic data may seriously undercut the effectiveness of a data preservation model because, with

It should be noted here as well that the US model of choice for industry to retain or destroy traffic data in accordance with its own requirements has also led to a situation where some US Internet Service Providers actually market their services through emphasizing that they will destroy traffic data immediately after it has been generated, so that no-one may have access to the data at a later stage. It seems clear to the Commission that this situation can be harmful to the fight against terrorism and organised crime.

In conclusion then, the option of having a data preservation regime only has been discarded since it does not contribute sufficiently to meeting the established policy objectives.

3.7. Retention periods – differentiation between telephony and internet data

One of the most important policy choices made in the preparation of this proposal, once the conclusion was reached that a Directive would be the only appropriate option, has been on the actual retention periods, as well as on the differentiation between telephony data and internet data. The choice for the different periods has an immediate impact on both the effectiveness of the proposal for law enforcement and in terms of the cost implications. Longer retention periods also mean more impact on the privacy of individuals..

In terms of the actual retention periods for the different categories of data, the Commission has looked at the different periods established by the different Member States in their data retention regimes, as well as indications given by data protection authorities, civil liberties groups, and of course law enforcement authorities. As indicated before, Member States have made widely diverging choices in their data retention regimes, ranging between three months and four years. The impacts of this choice in terms of costs are discussed below under Chapter 4.

The proposal contains two different, but harmonised, retention periods for these categories of data – one year for telephony data and six months for 'internet' data. The choice for a one year retention period for telephony data has been based mainly on a cost-benefit analysis, as explained in more detail in paragraph 4.3. The main concern in establishing this period has been to find the most acceptable compromise between the different interests at stake. In terms of the effectiveness of the measure to increase the possibilities of law enforcement authorities to prevent and combat serious crime, such as terrorism and organised crime, recent research by one of the Member States has provided clear indications that most requests for data could be answered by the providers of electronic communications services if such data is retained for these periods. This was confirmed through contributions of other law enforcement representatives. A more detailed description is included in paragraph 4.3.1.

When discussing traffic data generated through usage of the Internet, it is immediately clear that the amount of such data is vastly greater than the amount of data generated by 'standard' mobile and fixed telephony. Moreover, the duration of the storage of data by industry for their own purposes is much shorter. In addition,

---

European data protection requirements, much less data will exist when law enforcement requests preservation of data relating to a specific investigation".

any individual surfing the internet for even a short period leaves a very significant traffic data 'trail', whereas traffic data generated by telephone calls is much more limited. In most scenarios, data on internet usage will be more revealing on a person's habits and interests than data on whom a person has contacted by telephone.

3.8. Cost reimbursement scheme versus costs left for industry to bear

Different considerations have led the Commission to proposing a cost reimbursement scheme. One of those considerations is that the initiative should not have a negative impact on market development within the telecommunications sector. If costs associated with a traffic data retention scheme would have to borne solely by the service providers, this could have had a significant impact, especially for smaller entrants into the market.

This is important in order to avoid discriminations between the market players. Reimbursement will also allow the creation of a level-playing field throughout the European Union.

This choice must also be seen in the context of the important role of this sector in the Lisbon strategy pursued by the European Union and its Member States, as indicated above.

There are examples where co-operation from industry groups to law enforcement efforts has been sought – particularly in the efforts to combat money laundering – which have not given rise to cost reimbursement schemes. Law enforcement experts have indicated, however, that normally during the course of investigations traffic data is requested on a far more regular basis than bank records. Also these cases are not comparable in view of the structure of the respective markets concerned.

4. WHAT ARE THE IMPACTS – POSITIVE AND NEGATIVE – EXPECTED FROM THE RETAINED OPTION?

4.1. Introduction

Under this Section of an Impact Assessment report, normally the positive and negative aspects of the different options identified as viable under the preceding chapter are presented and discussed. Given the fact, however, that the analysis made of the different available options above only identified one viable option to achieve the objectives outlined under Section 2, the current Section will only focus on the positive and negative impacts of that particular option.

4.2. Expected positive and negative impacts of the option selected

As explained above, the positive impacts of the option chosen mainly consists of a better availability of certain data for law enforcement purposes, in line with the call made by the European Council, and the creation of a level-playing field for the electronic communications industry. This initiative in itself should allow a move away from the current disparity of national laws which is creating obstacles to the internal market. At the same time, it would not compromise the Lisbon strategy which expects the ICT sector, not least in the area of electronic communications, to contribute substantially to the growth of the EU economy.

The negative impact of this measure is mainly twofold: the intrusion upon the privacy of citizens, and the burden on electronic communications operators and eventually on Member States. However, as explained above, maximum efforts have been put in trying to minimise these impacts.

4.3. How large are the effects?

Qualitatively, the option chosen – a Directive based on Article 95 EC - will deliver in particular the following results: the cross-border availability of data to prevent and combat crime and terrorism will be ensured for the periods of 12 and 6 months respectively. Legal certainty will be improved for the benefit of all parties concerned. A level-playing field will be created for industry across the various Member States. Personal data on EU citizens will be protected in the same manner throughout Europe. Too heavy requirements, in particular longer periods of retention, or more extensive data sets to be retained, would have been disproportionate, from the internal market viewpoint, and not in line with the Lisbon agenda.

Quantitatively, the economic impact of the data retention measures can be broken down into different categories of costs.

There are direct costs which can be assessed relatively precisely, provided that the extent to which data need to be retained is known at the time of calculation. These include costs for setting up the systems that generate certain data, the cost of secure data storage, and the cost to make the data available to law enforcement authorities on request. This includes both upfront investment and operational costs such as hardware and software to generate and/or keep given data, security features, investment in storage, data retrieval and analysis systems, maintenance and human resources. The overall cost of data retention will be higher if it implies an important redesign of systems. This would normally be the case for operators which do not keep a certain set of data covered by the proposed measures. This may also be the case for IP-based services which only keep certain IP data for a limited number of days or weeks.

As an illustration of the latter, consultation with industry has indicated that interpreting traffic data almost always requires knowledge of the particular state of the network at the time it was collected, and this can change rapidly. The common practices of dynamic address allocation and network address translation mean that the same Internet address may be used by many different computers in a day; dynamic load-balancing means the same Internet name may refer to a different physical computer each time it is referenced; communications may vary their route across the network depending on fluctuations in traffic load and the direction they are travelling. Currently, this dynamic information is often not recorded in full, making historical data much less meaningful.

Indirect costs – often quoted in consultation though even more difficult to quantify – may have some impact as well. Industry representatives have indicated that there might be an indirect cost related to the anticipated lesser use of certain electronic communications services, due to the loss of confidence in their confidentiality. On the other hand, lack of measures in the area of data retention will make it much more difficult for law enforcement to perform its tasks within the internet environment, which may lead to an even bigger economic effect of cybercrime. Indirect benefits could thus include a possible reduction in cybercrime, and in any case a situation

which is not worse than the current one for law enforcement efficiency. It will therefore be difficult to assess indirect costs can before some years of implementation of the Directive.

These elements are all the more important since e-services are expected to contribute substantially to EU growth. Information and communication technologies (ICT) are a powerful driver of growth and employment. A quarter of EU GDP growth and 40% of productivity growth are due to ICT[19]. Within ICT, telecommunications services have been the largest contributor to the growth of European productivity over the last few years (around 24% in the period 1996-2000).

More importantly, electronic communications, and in particular the Internet, are expected to grow substantially in future. For instance, it is estimated that internet traffic in Germany doubles every 14 months (Bundesverband der Deutschen Industrie, BDI, 2004). This implies that the same requirements will become proportionally more cumbersome over time. This is another reason why the IP dataset to be retained is set at an acceptable minimum level.

As explained in detail below and elsewhere in this document, consultations have indicated that the most proportionate, efficient period of retention time would be 12 months for telephone data, and 6 months for IP data.

4.3.1. Added value for law enforcement authorities

As indicated previously under paragraph 3.7., a period of 12 months for fixed line and mobile telephony, and six months for IP related data would allow operators to respond successfully to almost all data requests received, while limiting the cost on operators and the intrusion upon privacy. In contrast, a longer retention period would appear to be of little added value for law enforcement authorities while having important financial consequences for operators and infringe disproportionately on citizens' privacy.

It has to be clarified that it is difficult to provide consistent data on the costs associated with certain retention periods, as well as on the needs of law enforcement in this area. For example, the results of the comparative study completed in October 2004 and covering Austria, France, Italy, The Netherlands, Sweden, Spain, and the UK[20], which would seem to indicate that in the countries concerned, regardless of the data retention period, 80 to 85% of the data requests are reported to be satisfied with data not older than 3 months, and 95% percent of the requests concern data not older than 6 months. At the same time, law enforcement authorities have indicated these results are not entirely reliable, since they would not ask for data if they know that it is in fact not available.

In contrast, the Interpol High Tech Crime Working Group has indicated in its contribution to the debate that a minimum period of one year is necessary.[21] Other

---

19 Communication "i2010 – A European Information Society for growth and employment" (COM (2005) 229)

20 This study made by the research company WIK is available at the following URL address: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf

21 Statement of the Interpol High Tech Crime Working Group, included in the contribution from Belgium to the Data Retenion Questionnaire of the Council General Secretariat, 2004

contributions form law enforcement authorities indicate that most of the requests for traffic data will take place within the first few months after the crime under investigation has been committed. One UK expert indicated that for volume crime, 95% of case demand is satisfied within 3 months. He went on to state, however, that for serious and organised crime, 85% of cases require data between 6 and 24 months, and for murder and terrorist cases there are examples of requirements for data up to 5 years old. Experts from other countries have confirmed this. These statistics also make sense from a point of view of priority setting by law enforcement – it will naturally be the more important crimes which will be investigated for longer periods, and which will thus generate requests for older traffic data. Organised crime investigations, especially international ones, can easily take a long time to complete, necessitating a longer availability of traffic data.

Recent research (May 2005) conducted in one of the Member States and presented within the discussions on this topic within the Council indicates that whilst it is true that the bulk of requests from law enforcement are for data which are between 0-6 Months old, there is still a significant number of requests (around 13% of the total) for data which is between 6 and 12 months old. That research also confirmed that those requests for data between 6 and 12 months old relate predominantly to serious crime such as murder and terrorism.

The argument is sometimes made that retention of traffic data will not help law enforcement authorities since it is easy to circumvent controls through using alternative ways to access the internet, such as internet-cafes or libraries. Whilst it is true that such possibilities exist, the numerous examples provided during consultation where traffic data has been successfully used suggest that this argument is not supported by practice. One example provided in the consultation process demonstrates that even where criminals go to great lengths to avoid being identified, this does not always work so well. In this case an offender informs the national police authorities by mail that a bomb has been placed at a Central Station. By means of IP addresses and logs saved by the ISP, it appeared that that mail had been sent from a public library. The library staff was consequently able to provide information that made it possible to identify the offender.

4.3.2. Costs for individual companies

Comments on the Council initiative made in the course of the consultation mentioned above confirmed that the cost of complying with the requirements of the Framework Decision would be very significant, as explained below. Although these figures are indicative, they can not be considered to be definitive, mainly because of the fact that these figures were derived from assumptions on the actual types of data to be retained. As explained earlier, this is one of the main factors which will influence the overall cost picture. In this area, there are important differences between the proposal for a framework decision originally put forward by the Member States and the present Commission proposal.

Firstly, the main difference remains that the list of data which would need to be retained under the Framework Decision is a minimum list, which causes more uncertainty on the associated costs, as opposed to the harmonised list included in the Commission proposal.

Secondly, the length of retention proposed is significantly shorter than the periods indicated in the proposal for a Framework Decision put forward by the four Member States, on which most contributions to the debate have been based. Harmonisation of the retention periods also reduces costs and provides market opportunities to develop EU wide technological solutions. It will also force those Member States which currently have longer retention periods foreseen in national legislation to bring these in line with the Directive.

Finally, the Commission proposal provides for a reimbursement scheme for these costs, ensuring that they will not be borne by industry alone.

A final estimation and evaluation of the costs is only possible once these different factors have been taken into consideration.

4.3.3. Platform on data retention

The Commission envisages to create a Platform on data retention; such a group should bring together technical experts on electronic communications, as well as representatives from law enforcement and data protection authorities.

4.3.4. Quantitative examples

With the above reservations in mind, the estimates of costs which were submitted during the consultation process can be presented as follows.

ETNO (the European Association of Telecommunications Network Operators) indicated that for a 12 month retention period, costs would be above 150 million EURO for a large network and service provider (above 100 million EURO for retention of traffic data for software, server, security, and at least 50 million EURO for annual overhead expense). For big Internet Service Providers, the cost would even be higher, according to ETNO.

Similar figures have also been mentioned in MEP Alvaro's draft report presented on 7 June 2005 on the Council initiative. This report states that "According to estimates by a variety of large firms in the Member States, this would require investment in traditional circuit-switched telephony amounting to around EUR 180m a year for each firm, with annual operating costs of up to EUR 50m. In the case of small and medium-sized businesses, their ability to operate would no doubt be in jeopardy. According to estimates, the Internet-related burden would exceed that within traditional circuit-switched telephony many times over."[22]

A major internet and email service provider (ESP-ISP) estimates that 12 months retention of the IP data to be covered would amount to 75 million dollars (i.e. about 61 million EURO) over 4 years, with over 37.5 million dollars (about 29 million EURO) in the first year. In contrast, the retention of similar data for 3 months would reportedly imply negligible costs since that data is reportedly already kept. (These

22 Report of 31 May 2005 on on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (A6-0174/2005)

figures do not include retrieval costs.) If email headers had been required to be retained, costs would have amounted to about 200 million dollars (about 163 million EURO) over 4 years.

However, there is also research available which suggests that the actual costs will be far below the estimates provided by industry in the consultation process. According to a study by KPMG, commissioned by the Dutch Ministry of Justice, and published in November 2004[23]. That study indicates, as an example, that the costs for retaining data related to fixed and mobile telephony, would amount to investment and running costs in the order of hundreds of thousands of euro. Only the retention of an extended set of internet data would generate costs of between 1,5 and 2 million euro (for a large provider), possibly rising to double those amounts with increased internet usage. The current proposal provides for a much more limited set of IP data to be retained, which would consequently generate far lower costs.

In recent discussion in Council groups on the issue of costs associated with traffic data retention schemes, Member State which have experience in dealing with such schemes also indicate that the associated costs are relatively limited. One Member State indicated that the costs associated with retaining traffic data for fixed and mobile telephony for 3 years amount to around 5 million euro. Other Member States indicated similar costs – all below 10 million euro. Within these discussions a presentation was also made by a representative of a large mobile phone service provider, who indicated that the cost of adapting the systems of his company to retain data on incoming and outgoing calls from a period of 4 days to one year was around 1 million euro. It should be stressed that these figures came from Member States who actually have experience with retention and cost reimbursement schemes.

In any event, the proposal will lead to additional costs for electronic services providers and for the Member States who will reimburse these costs under the proposal.

In view of the different indications above, the development of these costs, as well as the effectiveness of the cost reimbursement scheme will have to be monitored closely. This may eventually lead to adaptations of the list of data to be retained, or indeed to the modification of other provisions of the Directive in the process of its evaluation (see also Section 5 on this point).

4.4. Fundamental Rights - positions of advisory bodies

The proposal is in line with Community law and with the Charter on Fundamental Rights. Even though it is clear that the proposed Directive will have an effect on the privacy right of citizens as guaranteed under Article 7 of the Charter, as well as on the right to protection of personal data as guaranteed under Article 8 of the Charter, the interference with these rights is justified in accordance with of Article 52 of the Charter. Specifically, the limitations on these rights provided for by the proposal are proportionate and necessary to meet the legitimate objectives of preventing and combating serious crime such as organised crime and terrorism.

---

[23] Available at http://www.europapoort.nl/9345000/1f/j9vvgy6i0ydh7th/vgq8mlyezvzt

Furthermore, the proposal limits its effects on the private life of citizens: firstly it clearly establishes the data can only be retained for preventing, detecting, investigating serious crime such as organised crime and terrorism. Secondly it limits the categories of data which need to be retained to what is necessary for this purpose. Thirdly it limits the period of retention.

A further important safeguard is that this Directive is not applicable to the content of communications - this would amount to interception of telecommunications which is more intrusive, and which falls outside the scope of this legal instrument.

Finally, the processing of the personal data retained by the service and network providers under the provisions of this Directive are covered by the general and specific data protection provisions established under Directives 95/46/EC and 2002/58/EC - which means in practice that specific additional provisions on general data protection principles and data security are not necessary. It also means that the processing of such data will be under the full supervisory powers of the data protection authorities established in all Member States. It also means that citizens can exercise their powers as granted under those instruments to obtain access to, as well as correction and deletion of the data under the conditions specified in national law.

A data retention period of 12 months has however met with a negative response from the two main European bodies dealing with privacy and data protection issues, within the context of discussion on the draft Framework Decision. Mr Hustinx, the European Data Protection Supervisor, has mentioned six months as a reference period at a public hearing organised by the European Parliament[24]. Also, a 12-month or longer period of retention has been criticised as creating tensions with human rights by the Article 29 Data Protection Working Party[25]. The present section indicates why the Commission believes that the differences between the draft Framework Decision at the basis of the opinions given and the present proposal will allow the mentioned bodies to consider the proposal as compatible with human rights.

The main argument presented by the Article 29 Working Party in its opinion on the draft framework decision appears to be one of proportionality, based on the fact that law enforcement authorities have not proven that there is effectively a need for retention periods longer than six months. Elsewhere in this document arguments have already been given for why such longer retention periods are in fact necessary for law enforcement purposes, which do not need to be repeated here.

Other comments provided by the Article 29 Working Party have been largely met in the proposal – once again, through a strict limitation of the cases for which data may be provided to law enforcement authorities, through limiting the retention period for

---

24 see e.g. Peter Hustinx, Parlement européen, Commission LIBE Séminaire public "Protection des données et sécurité des citoyens: quels principes pour l'Union européenne?" Bruxelles, le 31 janvier 2005.

25 Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]. Available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf

traffic data generated through the usage of the internet to 6 months, as well as the data-set to be retained, and through assuring that the retention and processing of the data must take place in full conformity with the existing legal framework for the protection of data. This includes the rights of individuals to access, correction and deletion of the data, as well as the right to ask for compensation in cases of processing which contravene the legal framework.

In addition, the proposal foresees the setting up by the Commission of the Platform mentioned above, which will ensure that representatives of data protection authorities are fully involved in the ongoing discussions on this topic. Also, involvement of the Article 29 Working Party in the evaluation process of the Directive, as well as in the Comitology procedure foreseen to amend the list of data as necessary is guaranteed by existing Community law.

In conclusion on this point the Commission is convinced that its proposal can stand the test of compatibility with fundamental rights and freedoms. It is confident that the bodies mentioned will be able to revisit their position on the basis of the indications above.

4.5. Are there impacts outside the Union on the Candidate Countries and/or other countries ("external impacts")?

External impacts of the proposal are likely to be positive, especially when considering the fact that requests for international law enforcement co-operation are more likely to be answered than currently the case – naturally as far as allowed under the applicable legal framework. European wide harmonisation on this issue is also likely to have a positive effect on any enterprise from outside of the EU who would wish to invest in the EU-wide electronic communications market in Europe.

4.6. What are the impacts over time?

The expected increase in the use of electronic communications will necessarily lead to a higher amount of data being kept in the future. This will reinforce the impact of the measures over time.

As an illustration, innovation in mobile and broadband and to some extent traditional fixed services is driving the search for growth[26]. In Italy for instance, in less than three years the traffic over Telecom Italia's networks has grown from around 200 billion to over 380 billion minutes. Since the voice traffic has remained approximately stable (between 120 and 140 billion minutes), the increase is largely due to broadband over ADSL[27]. The key drivers are fixed data and mobile services, which show strong growth of 11.5 % and 7% respectively. The growth in broadband lines is considerable. Recent figures show that there have been over 16,5 million new broadband lines in 2004, corresponding to above 70 percent growth[28].

It is expected that the use of electronic communications, in particular the internet, will increase substantially in future. Experts agree that vastly more people should be

---

26 10th Implementation report, COM(2004) 759 final

27 Dr. Marco Tronchetti Provera, Executive Chairman Telecom Italia "Regulation vs. Competition in the light of technological market development", ETNO, Brussels, 30 May 2005.

28 See working document 'Broadband access in the EU: situation at 1 January 2005 (COCOM 05-12).

online in the next ten years. Broadband offers a much faster connection to the internet, and offers the potential of changing the way the internet is used[29]. Taken together, these elements will imply that, with similar data retention requirements, more data should be retained by operators in the future.

The expectation is that these factors will remain largely untouched by the proposal. When contrasted against a 'do nothing' scenario, the fact that there will be a stable and harmonised approach on this issue within the EU will reduce risks for enterprise, and technical solutions for storage and retrieval costs will mature, leading to further cost reductions.

In order to ensure that the Directive can be adapted quickly to developments in electronic communications technology or to changes in the needs of law enforcement, amendment of the types of data to be retained can be achieved using a Comitology procedure.

5. HOW TO MONITOR AND EVALUATE THE RESULTS AND IMPACTS OF THE PROPOSAL AFTER IMPLEMENTATION?

As indicated, the policy will consist of a directive harmonising data retention obligations for the electronic communications industry. The directive will have to be adopted by Parliament and Council, and be implemented by Member States. The implementation of this directive will be monitored by the Commission – the Commission will be aided in this respect through a specific clause in the Directive which provides for the obligation to collate statistical data on the actual requests made, and to provide the results to the Commission.

In addition, a specific review clause is provided in the proposal, providing for an overall evaluation of the Directive three years after its entry into force.

Monitoring of the impacts of the Directive after implementation will also be aided through the Platform on Law Enforcement, Electronic Communications and Data Protection to be set up by the Commission, which will be able to discuss the implementation in Member States, any practical or other difficulties identified, and other issues, and provide advice on this to the Commission.

6. STAKEHOLDER CONSULTATION

6.1. Consultation methods, main sectors targeted and general profile of respondents

Starting in 2001 with the meetings of the Cybercrime Forum, the issue of traffic data retention has been the subject of consultation with representatives of law enforcement authorities, the electronic communications industry and data protection experts.

On 14 June 2004, an ad hoc roundtable meeting was organised under the auspices of the Forum for the Prevention of Organised crime, in which representatives from law enforcement, industry and data protection organisations took part. On 30 July 2004, a

[29] See e.g.; Pew Internet, the Future of the Internet, January 9, 2005.

joint consultation document on traffic data retention was presented by DG INSFO and DG JLS, in preparation of a public workshop on the issue held on 21 September 2004. Contributions and reactions from various sides – in particular from industry and civil rights associations - were received in response to the joint consultation document. The public workshop of 21 September provided further input to the Commission.

In the preparation of the proposal, the Commission has also drawn on the wide-ranging public debate on this issue, including discussions at the European Parliament.

6.2. Summary of responses and how they have been taken into account

Many different examples of the results of the consultations conducted have already been discussed in earlier sections of this report. This paragraph provides an abbreviated overview of the responses received.

The consultation process confirmed that retention of traffic communications data is an essential tool for law enforcement authorities to prevent and combat serious crime and terrorism. Law enforcement authorities indicated that for their purposes, retention periods should be as long as necessary, and comprise as much data as necessary. Especially in complex investigations into serious crimes, which can take up to a number of years to conclude, older traffic data is still regularly required. A number of examples were given of cases where such data had proven to be essential for criminal investigations, mostly into crimes such as bombings or murders.

Representatives of the European representative organisations of the telecommunications and internet industry, as well as individual electronic communications companies, argued that whilst they were willing to co-operate with law enforcement, and had been doing so, long retention periods would generate considerable costs and data preservation would be sufficient. They pleaded anyway for retention periods no longer than six months since a large amount of data requested by law enforcement authorities is not older than six months, and for mechanisms to compensate them for the additional costs incurred.

Representatives from data protection authorities and civil rights associations argued that data retention is an interference with the private life of citizens, which is why retention periods should be kept as short as possible. In general terms, they questioned whether periods of retention longer than six months can be considered to be proportional. They also expressed concerns about the finality and aims of the retention, which should be clearly specified.

In the Commission's view, the current proposal constitutes a balanced approach, which takes the views expressed during consultation into account, as also explained in more detail elsewhere in this document. With respect to the main points raised above, the retention periods of 1 year for mobile and fixed telephony traffic data and six months for traffic data related to Internet usage will cover the main needs of law enforcement, whilst limiting the associated costs for industry and the intrusion into the private life of citizens. The cost reimbursement scheme, as well as a harmonised list of data to be retained, respond to the concerns expressed by industry. Issues raised by data protection authorities have been addressed as well through a strict

limitation of data to be retained and a shorter period for Internet related data, as well as through clear limitations on the purpose for which the data would be retained.

7. COMMISSION DRAFT PROPOSAL AND JUSTIFICATION

7.1. What is the final policy choice and why?

As explained in more detail elsewhere in this document, notably in Section 3, the initiative chosen consists of a proposal for a directive under Article 95 EC. It harmonises as far as necessary and proportionate data retention obligations bearing on providers of publicly available electronic communications.

In short, the text provides that data related to usage of mobile or fixed telephony through publicly available electronic communications services must be kept for 12 months, while a limited set of IP data must be kept for 6 months. A principle of reimbursement is also provided for any proven additional costs incurred.

The proposal for a Directive has taken account of the issue of proportionality through a number of different factors, most notably those in terms of the actual retention periods proposed, the distinction between telephony- and internet-related data, the limitation in the data sets to be retained, and the cost reimbursement scheme.

The proposed solution also provides for proportionality of the measure through a strict limitation on the cases for which the data retained may be provided for law enforcement authorities, and the fact that existing data protection legislation will be fully applicable to the storage and further processing of the data.

7.2. Why was a more/less ambitious option not chosen?

As indicated before, it is the Commission's view that the current proposal provides for the best balance between the different interests at stake. More or less ambitious options would not provide for the best possible response to the difficulties outlined in detail in Section 1 of this document.

7.3. Which are the trade-offs associated to the chosen option?

This initiative in itself should allow departing from the current disparity of national laws which is creating obstacles to the internal market. At the same time, it would not compromise the Lisbon strategy which expects the ICT sector, not least in the area of electronic communications, to contribute substantially to the growth of the EU economy. The trade-off is one between the costs for industry and the Member States, as well as a limitation of privacy of individuals, against a society which is more secure through more effective law enforcement action in preventing and combating serious forms of crime such as organised crime and terrorism.

7.4. If current data or knowledge are of poor quality, why should a decision be taken now rather than be put off until better information is available?

A proposal for a directive has become urgent, notably in view of the disparity in national laws. This disparity risks being reinforced if the Council adopts, as expected following the Council Declaration of 13 July 2005, the mentioned draft framework decision which would lead all Member States to adopt retention measures without

proper harmonisation. Better information is unlikely to become available before the Council takes a position on this issue.

7.5. Have any accompanying measures to maximise positive aspects and minimise negative impacts been taken?

As indicated previously, a number of accompanying measures have been taken to maximise positive aspects and minimise the negative impacts. More detail on this is provided in Section 4, but the main elements are a strict limitation in retention periods, a strict limitation for what purposes the data which are retained can be used, a reimbursement of costs to industry by the Member States, as well as flexible procedures to allow for adaptations of the legal instrument as necessary.