ANSWERS TO THE QUESTIONNAIRE ON THE EVALUATION OF THE DATA RETENTION DIRECTIVE – DG JLS
ICRI-K.U.Leuven (Eleni Kosta, Jos Dumortier)

QUESTIONS ADDRESSED TO THE EUROPEAN PARLIAMENT AND CIVIL SOCIETY

2.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10

2.A.1 Which has been the effect, if any, on civil liberties of the use by law enforcement authorities of data retained under the Directive? Please provide examples of these effects as well as indications of the size of their impact.

The Data Retention Directive foresees the blanket retention of some categories of personal data (traffic and location data on both legal entities and natural persons and the related data necessary to identify the subscriber or registered user). The providers of publicly available electronic communications or of public communications networks (hereinafter providers) shall make sure that these data are available for the purpose of the investigation, detection and prosecution of serious crimes.

HUMAN RIGHTS: RIGHT TO RESPECT OF PRIVATE LIFE AND CORRESPONDENCE – Article 8 of the European Convention of Human Rights (ECHR) safeguards, among others, the right to respect of private life and correspondence. Regarding the collection of data, the European Court of Human Rights has recently issued a judgment on the case Copland v. UK, according to which “the collection and storage of personal information relating to the applicant's telephone, as well to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for their private life and correspondence within the meaning of Article 8 [ECHR]”1. This approach has been repeatedly followed by the Court2 and indicates that interferences with Article 8 ECHR are not easily accepted3. The blanket retention of traffic and location (and identification) data of all citizens can be considered as infringing Article 8 ECHR, as it is a disproportionate

PRINCIPLES OF NECESSITY AND PROPORTIONALITY – The Article 29 Working Party, as well as the European Data Protection Supervisor and the European Data Protection Commissioners, have repeatedly sustained that the retention of traffic data –including location data– shall be seen as an exceptional measure that can apply only when the general privacy principles and mainly the principles of necessity and proportionality are respected4. The Article 29 Working Party, already in September 1999 in a recommendation regarding the preservation of traffic data by Internet Service Providers for law enforcement purposes, expressed the opinion that the “principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their privacy and the secrecy of their correspondence […] need to be taken into account”5.

CATEGORIES OF DATA TO BE RETAINED – As the retention of data is an exception to the general data protection rules, respect to the principle of proportionality dictates that the categories of data to be retained, as described in Article 5 of the data retention directive, shall be seen as the maximum. The Member States in the

1 Copland v. U.K., Judgment 3 April 2007, Application no. 62617/00, par. 44
2 Amman v. Switzerland, Malone vs. the United Kingdom
5 Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes”, WP25, 07 September 1999
national implementation of the directive shall not expand the list of data that is included in the directive into other data.

Respect to the data minimisation principle demands that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Article 5 of the data retention directive contains a detailed list of data that have to be retained, classifying them in six main categories: Data necessary to (a) trace and identify the source of a communication, (b) identify the destination of a communication, (c) identify the date, time and duration of a communication, (d) identify the type of communication, (e) identify users’ communication equipment or what purports to be their equipment and (f) identify the location of mobile equipment. The aforementioned categories are further divided into data related to fixed network telephony, mobile telephony and Internet access, Internet e-mail and Internet telephony.

The European Data Protection Supervisor in his Opinion, before the adoption of the directive, had stressed that the number of data to be stored “must reflect the demonstrated needs of law enforcement” and the Article 29 Working Party expressed the opinion that “the data to be retained should be kept to a minimum”. However, it has not been efficiently justified why the specific categories of data that are included in Article 5 are adequate, relevant and not excessive for the purpose of investigation, detection and prosecution of serious crime. Furthermore, the wording of Article 5 is not always very clear having raised several points of dispute, regarding the retention or not of data relating to calls that are not answered and of location data regarding the mobile equipment. The Article 29 Working Party tried to resolve the aforementioned disputed issues, holding on the one hand that the categories of data related to unsuccessful communication attempts shall not be retained, contrary to the explicit provision of Article 3(2) of the data retention directive stipulating that “the obligation to retain data […] shall include the retention of data […] relating to unsuccessful call attempts”. On the other hand, it clarified that storing location data should not go beyond the CellID at the beginning of a communication, an opinion that has been repeated by the Dutch DPA.

**RETENTION PERIOD** – The Data Retention Directive foresees the retention of data for periods of not less than 6 months and not more that two years from the date of the communication. There are two major problems with regard to the retention period of the data. On the one hand the retention period is set between six months and two years, which does not work in favour of harmonisation. On the other hand, the maximum period of two years is not proportionate. The fact that a retention period of two years is not proportionate to the purposes of data retention has already been repeatedly expressed by the European Data Protection Commissioners and the Article 29 Working Party.

In September 2002 the European Data Protection Commissioners besides confirming once again their view that traffic data retention is an improper invasion of the fundamental rights of the individuals they also expressed their ‘great doubt as to the legitimacy and legality of such broad measures’, pointing out that ‘systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case’ (emphasis added). The Article 29 Working Party considered that a “routine storage period for billing [should have the duration of] maximum 3-6 months, with the exception of particular cases of dispute where the data may be processed for a longer period. In addition, only traffic data that are average,

---

6 Article 6(1)(c) data protection directive
9 Ibid, p.9
10 Article 3 (2) Data Retention Directive
12 Opinion of the Dutch Data Protection Authority [College bescherming persoonsgegevens (CBP)], Legislative proposal (Bill) for the implementation of the European Directive on Data Retention, Pertaining to the tender letter of 22 January 2007, 24 January 2007.
relevant and non-excessive for billing and interconnection purposes may be processed. Other traffic data must be deleted”14.

With regard to the issue of data retention the Article 29 Working Party has in an early Opinion of 1999 expressed the opinion that “telecommunications operators, telecommunications service [providers] and ISPs should not be obliged to keep data for a period of time longer than necessary for billing purposes”15 and added that “the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes and the national laws should not oblige telecommunications operators, telecommunications service and Internet Service providers to keep traffic data for a period of time longer than necessary for billing purposes”16. The European Data Protection Commissioners also stated that “systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case”17. This opinion was reaffirmed by the Article 29 Working Party in its opinion 9/2004 stating that “analysis carried out by telecommunication companies in Europe reveal that the biggest amount of data demanded by law-enforcement were not older than six months. This shows that longer periods of retention are clearly disproportionate”18. In support of this view, it referred to the model chosen by the Council of Europe in the Convention of Cybercrime for the preservation of traffic data. Article 16 in conjunction with Article 17 of the Convention provide only for individual secure storage on the ‘fast-freeze – quick thaw’ model, allowing the preservation of traffic data for the period of time deemed necessary, but under no circumstances will the traffic data be retained beyond a maximum period of 90 days.

All the policy documents were mentioned above to illustrate the opinion of several European data protection bodies, that have clearly considered a retention period longer than 12 months at the very most, as not proportionate and unjustified. The same retention period was suggested as desirable by the Erasmus University, which prepared a study on the use of and need for a retention duty for historical traffic data from telecommunication traffic19. However the data retention directive chose for a retention period between six months and two years from the date of the communication.

HUMAN RIGHTS: FREEDOM OF EXPRESSION – The blanket retention of traffic and location data has a serious effect on the freedom of expression, as all citizens have the feeling that they are under continuous surveillance and they are refrained from using the communications infrastructures, whenever they can avoid it. The free exchange of information is deeply affected.

THE RIGHT TO ANONYMITY – Anonymity is considered as a fundamental right of every citizen for their everyday transactions. People can pay in cash and nobody will know what they bought, people can avoid the use of fidelity cards and nobody will know their shopping habits. On-line anonymity is equally important. Actually, with regard to on-line anonymity, the Article 29 Working Party recognised that “[t]he principle that the collection of identifiable personal data should be limited to the minimum necessary must be recognised in the evolving national and international laws dealing with the Internet. It should also be embodied in codes of conduct, guidelines and other ‘soft law’ instruments that are developed. Where appropriate this principle should specify that individual users be given the choice to remain anonymous.”20. Although anonymity should be offered to all users of electronic communications and services, whenever possible (for instance it is reasonable that a telecom operator has the identification data of a subscriber in order to be able to pursue payment), the Data Retention Directive seems to bring an end to all anonymous communications. And there is no actual justification for doing

14 Working Party 29 Opinion 1/2003 on the storage of traffic data for billing purposes, WP69, 29 January 2003
15 Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes’, WP25, 07 September 1999
16 Ibid
18 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 (Council doc. 8958/04 – April 28, 2004)], WP99, 09 November 2004, p. 5
Serious Crime – The Data Retention Directive does not define what shall be considered as “serious crime”. It is left to the Member States to decide on this. Realising the problems that may arise from the lack of this definition already at the time of the adoption of the Directive, the Council of the European Union urged the Member States in defining “serious crime” to have due regard to the crimes listed in article 2(2) of the Framework Decision on the European Arrest Warrant and crime involving telecommunication. However, it is already at this moment obvious that the Member States have interpreted the term “serious crime” in a very divergent way. For instance Malta considers as “serious crime” a crime that is punishable by imprisonment of at least 1 year, while Finland foresees that a “serious crime” is an offence or attempt thereto punishable by imprisonment of not less than four years. In various EU countries, copyright holders have asked that the data records retained under the Data Retention Directive are available for civil-law disclosures, so that file sharers can also be tracked down.

The fact that serious crimes are not clearly defined in the Directive also endangers the finality principle, according to which “personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”. With regard to the finality principle, it shall be noted that the data that have to be retained according to the Directive are initially collected from the providers for commercial purposes. Thus the data are used for another purpose that the one originally collected. Such an exemption can be nevertheless justified under Article 13 of the Data Protection Directive that allows the Member States to adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 6(1), when such a restriction constitutes a necessary measure to safeguard, among others, the prevention, investigation, detection and prosecution of criminal offences.

The recent judgement of the European Court of Justice (ECJ) in the Passenger Name Record (PRN) case complicates however this reasoning. The ECJ annulled the Council Decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Bureau of Customs and Border Protection (CBP) and the Commission Decision on the adequate protection of those data. According to the judgement the “transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law”. As the data have been initially collected for commercial purposes, the Court found that the actual purpose of their transfer falls within a framework established by the public authorities that relates to public security and thus the processing falls outside the protective ambit of the data protection directive. As the General Advocate already supported, the Court also distinguished between the activities of collection of data and the purpose of their (further) processing based on public safety needs, in order to exclude the latter from the scope of application of the data protection directive. In short, the judgement admits that the processing of data collected for commercial purposes falls within the protective ambit of the data protection directive but when the same data are further transferred for public security reasons, they no longer enjoy the same protection. The judgement created thus a substantial lacuna legis in the protection of PNR data, raising the general problem of protection of personal data that are not covered by the Data Protection Directive. If the same reasoning is applied in the case of the Data Retention Directive, where the data are also initially collected for commercial purposes and are further accessed for law enforcement purposes, the finality principle is severely infringed and the whole legal basis of the directive based on the first pillar is at stake.

23 Article 6 (b) Data Protection Directive.
28 Paragraph 56 of the Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006).
29 See also the analysis made by Hielke Hijmans, in Hielke Hijmans 'De derde pijler in de praktijk: leven met gebreken Over de uitwisseling van informatie tussen lidstaten'. SEW 2006:91, under chapter 4.1.
**SCOPE OF APPLICATION: PROVIDERS & SERVICES** – The Directive applies to providers of publicly available electronic communications or of public communications networks. However, it is not always easy to determine whether a service qualifies as an electronic communications service and consequently whether the providers of such a service fall under the scope of application of the data retention directive. In the case of Webmail for instance, ambiguity arises as to whether such a service shall be considered solely as an information society service (ISS) or as an electronic communications service (ECS) as well. In case the former opinion is accepted and Webmail service is not rendered as ECS, i.e. as a service that consists mainly or wholly in the conveyance of signals, then all Webmail Service Providers shall be excluded from the application area of the data retention directive.

The wording of the definition of electronic communications network (Art. 2(c) Framework Directive) can lead to a very broad interpretation of the term and thus to a very broad group of providers that qualify as ‘providers of public communications networks’. Shall the access to the Internet, for instance, be provided under remuneration or as the main activity of the provider? Interesting is for instance the discussion with regard to the applicability of the Data Retention Directive with regard to social networking sites (SNS). Some legal scholar are of the opinion that when SNS offer their users the possibility to exchange e-mails via these platforms, the Data Retention Directive applies and the SNS providers serve as providers of electronic communications services. To our opinion this goes beyond the wishes of the legislator of the Data Retention Directive and this issue should be clarified.

With regard to the Internet, the Directive only requires the retention of data relating to Internet Access, Internet e-mail and Internet Telephony. Especially the unclear nature of Internet e-mail, in view of the definition of e-mail in the ePrivacy Directive creates unclarity in relation to specific services, such as Instant Messaging, chat, Video Conferencing…

**COMPETENT AUTHORITIES** – According to the Directive, the retained data shall be disclosed only to the competent authorities when they are entitled to access the data, according to the national laws of the Member States. Nevertheless the fact that the Directive does not define who can fall under the term ‘competent authorities’ leaves very broad margin of interpretation to the Member States. Any unclarity whether data shall be provided to an authority or not causes great distress to the providers who bear the burden to decide whether they will reveal the data or not.

---

2.A.2 What additional measures (administrative, technical, legal, or other) would be appropriate for the offset of any negative impact(s) which has been identified?

Although the Directive as it stands can be considered as infringing Arts. 8 and 10 ECHR, based on the analysis conducted above we can propose the following measures:

**SERIOUS CRIME** – The ECJ in their judgment on the *Promusicae vs Telefonica* case ruled that it is up to the Member States to decide on the disclosure on personal data in the context of civil proceedings. As the ECJ did not rule out the possibility to use personal data (thus, also personal data that are retained under the Data Retention Directive) for civil cases, this is something that should be done in the Directive. The Directive should explain which crimes shall be considered as serious crimes and should clearly exclude the possibility to use retained data for other purposes (e.g. in the context of civil proceedings). In this way higher level of harmonisation will be achieved and the divergences between the Member States will be minimised.

**CATEGORIES OF DATA TO BE RETAINED** – It shall be clarified in the Directive that the categories of data to be retained, as defined in Art. 5, shall be treated as the absolute maximum.

**RETENTION PERIOD** – The retention period shall be limited to six to twelve months in order to comply with the necessity and proportionality principle.

**SCOPE OF APPLICATION: PROVIDERS & SERVICES** – It shall be defined who falls under the definition of providers of publicly available electronic communications or of public communications networks. The services that fall under the Directive, especially with regard to the Internet shall also be clarified (does the Directive cover Instant Messaging, chat, Video Conferencing etc?).

---

2.A.3 Which ones of the measures mentioned under 2.A.2 should be addressed at the level of the European Union?
All of the above

The European Commission can compile a public list of the competent authorities to which retained data shall be disclosed in all the Member States.

2.A.4 Having regard to changes in technology and experience gathered with the operation of the Data Retention Directive, is the balance provided for by the Directive between enhancing security by means of retaining communication data and protecting civil liberties still appropriate. If a different balance is deemed to be appropriate, please provide details how to adjust the balance as well as the motivation underlying the assessment. (can entail Quantitative elements)

The need for further balance between enhancing security by means of retaining communication data and the protection of civil liberties has been already analysed extensively above and relevant measures than need to be taken are already proposed.

2.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure the traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards.

2.B.1 What has been the effect, if any, on civil liberties of measures taken at national level to increase the traceability of users of communication devices? Please provide examples of these effects as well as indications of the size of their impact.

The increase of the traceability of users of communication devices creates a feeling of constant surveillance to the citizens, as already analysed in the previous question. In the short to medium term, all EU Member States will impose legislation for the registration of pre-paid mobile phone cards, in view of ensuring the identification and traceability of the users. No matter how many measures are taken to prevent the anonymous use of electronic communications, it can not be expected that criminals will obey the rules. It is rather easy to steal a mobile device, to use a public telephone booth or to hack a computer, for the more technology-savvy criminals. Moreover, since the Data Retention Directive applies only to providers of publicly available electronic communications or of public communications networks established within the EU, it will be rather easy for criminals to use services and networks, established outside the EU in order to avoid the application of the Directive. In view of these facts, the Directive will lead to the collection of data of law-abiding citizens, while criminal can escape without much difficulty.

2.B.2 Which additional measures (administrative, technical, legal, or other) should be taken for the offset of negative impacts, if any?

Anonymity is a fundamental right of citizens and shall be safeguarded in a democratic society. The penalisation of the use of anonymisation devices and services (as it is proposed in some Member States) will infringe the fundamental rights of the citizens. Anonymity shall remain as an option for the citizens. Instead more efficient international measures shall be found against criminals that make use of electronic communications.

2.B.3 Which ones of these measures should be addressed at the level of the European Union?

The European Union shall cooperate with other States outside the EU, such as the US, where the majority of Internet Service Providers are established, as well as with international organisations in order to find more effective measures to fight against criminals that make use of electronic communications.