COUNCIL OF THE EUROPEAN UNION

Brussels, 15 December 2011

18620/11

LIMITE

DAPIX 167
TELECOM 214
COPEN 365
DATAPROTECT 156

NOTE

From:	Commission Services
To:	Working Party on Data Protection and Exchange of Information
No. Cion prop.:	9324/11 DAPIX 38 TELECOM 47 COPEN 85
Subject:	Consultation on reform of Data Retention Directive: emerging themes and next steps

1. The purpose of this paper is to inform DAPIX of the results of the Commissions consultation on the reform of the Data Retention Directive (DRD), to set out the main problems, and to put specific questions on which the Commission, in determining the way forward, will rely on evidence supplied by Member States.

Consultation

2. Following the presentation of its evaluation report on the Data Retention Directive, the Commission has been consulting all interested groups on whether and if so how the DRD should be reformed, including:

- Member States governments and other government e.g. *Länder*
- Law enforcement including Europol and Eurojust
- Judiciary
- Data protection authorities
- Industry including trade associations
- Consumer associations
- Civil society: privacy-advocates, journalist association, victims groups
- Open public consultation on DG Home website

Emerging themes

I. Need to explain better the value of data retention

3. We have received strong views from law enforcement and the judiciary from all Member States that communications data are crucial for criminal investigations and trials, and that it was essential to guarantee that these data would be available if needed for at least 6 months or at least a 1 year. We have also received strong qualitative evidence of the value of historic communications data in specific cases of terrorism, serious crime and crimes using the internet or by telephone – but only from 11 out of 27 Member States.

4. There is a continued perception that there is little evidence at an EU and national level on the value of data retention in terms of public security and criminal justice, nor of what alternatives have been considered. Member States' evidence tends to consist of statements of the importance of the data. It is unclear whether data requested would be available anyway without the retention obligation, because there is no logical separation between data stored and then accessed for a) business purposes, b) for purposes of combating 'serious crime' and c) for purposes other than combating serious crime. There is no agreement on how to report implementation in qualitative terms. Data Protection Authorities do not know what is being kept or deleted by operators. The statistics required under Article 10 do not, as it is currently interpreted, enable evaluation of necessity and effectiveness.

5. There is, therefore, currently no monitoring system whereby the citizens can see that a) the data would not have been available to law enforcement without mandatory retention and b) the outcome of using that data in investigations and prosecutions.

II. Some data categories are being retained unnecessarily, other types of data needed by law enforcement cannot be easily accessed

6. Law enforcement favour 'technological neutrality' so that their ability to know *who* communicated with *whom*, *when*, *where* and *how*) is not diminished as technologies develop. However, unclear definitions in the DRD have encouraged heterogeneous interpretations of the scope - both operators and types of data - and this can result in frustration for law enforcement. For example, instant messaging, chat, uploads and downloads (but not anonymous SIM cards) are types of data held by information society services which is almost identical to traffic data but which is outside the scope of the DRD. There is no standard EU approach to accessing this data, so some law enforcement find it very difficult to get this data on time for their investigations

7. The majority of requests received for internet data are to resolve IP addresses to a subscriber, with other requests for email traffic data not as common. However, this could be an issue of lack of training or weakness in forensic capacity.

8. Business-to-business service providers very rarely receive requests for data which they retain. Small and medium operators also tend to receive requests for data very rarely.

III. Concern about proportionality, legal precision and data protection

9. The DRD purpose (Article 1) concerns 'serious crime', which is not defined at EU level or in many Member States, although the Council statement on adoption of the Directive said that MS should have 'due regard to the crimes listed in… the European Arrest Warrant… and crime involving telecommunication'.[1] Certain crimes, e.g. hacking, may not be deemed 'serious' but can only be tackled through telecoms data. The DRD does not cover urgent cases for protection of life and limb not related to crime e.g. suicide/ self harm, missing persons, emergencies. There are also some calls for extension of the purpose to include copyright infringements, which may include illegal downloads/ piracy.

10. Data protection authorities and NGOs are concerned at the lack of a clear limitation of the purposes for which data may be retained. In some Member States, the retention requirement is not limited to a specific purpose. The European Court of Justice has ruled that the use of personal data in civil proceedings is not prevented by the DRD.[2] Such a lack of clarity, it is claimed, leads to risk or fear of 'function creep'. This endangers the principles of finality and predictability.

---

1 Joint Statement by the Council and the Commission in relation to Article 12 (Evaluation) of the Draft Directive, 5777/06 ADD1 February 10, 2006.

2 *Promusicae vs Telefonica*

11. Operators do not provide consistent notification to users in contracts of potential data disclosure to authorities. There is no procedure for reporting and redressing data breaches. There is no clear distinction between data kept for commercial purposes, and data kept under the retention requirement. Citizens often do not know who has access to the data. The absence of standard procedures means that access cannot be monitored and audited.

IV. Difficulties in police and judicial cross-border cooperation

12. Law enforcement finds it difficult and inefficient to share acquired data across borders, including for joint investigations by Europol. This is often due to divergences in data retention, especially where Member States have not transposed at all and therefore cannot participate in joint operations. However, where there is a good level of trust data is more likely to be exchanged. The EIO may assist if and when it is adopted and fully implemented, where there will be an assumption that a request for evidence will be executed where it concerns 'the identification of persons holding a subscription of a specified phone number or IP address'.[3]

[3] See Article 10 of draft dated 17 June 2011 http://register.consilium.europa.eu/pdf/en/11/st11/st11735.en11.pdf

V. Effect on industry: Uneven data retention practices continue to impede and distort the internal market

13. Businesses in the telecommunications sector complain about legal uncertainty, saying that it is often unclear which data should be stored. Some Member States consider that the data categories in Article5 of the DRD are not exhaustive but rather the minimum requirement. The Article 29 Working Party has argued that unsuccessful communication attempts (which are covered by Article 3(2)) should not be stored.[4] Electronic communications service and Internet email have been interpreted in certain Member States as including webmail and social networking sites which provide email exchange services, instant messaging, chat and video conferencing. There is some confusion about the distinction between 'Electronic mail' (Directive 2002/58/EC Article2 (h)) which could be deemed to include instant messaging, and 'internet email' which may not. While the intention of the DRD was that data should only be retained once,[5] in reality data is stored by the operators of the sender and receiver of communication, and each server is backed up.

14. The industry has also provided evidence of considerable costs of compliance. The Data Retention Expert Group has recently approved a document describing these costs (list at Annex A) and various operators have provided confidential information on costs. The cost to the operator stems from having to retain it in such a way as to ensure it is available and valuable to competent authorities, which is explicitly required by the DRD Article8. It is a pure overhead if no reimbursement. There is a disproportionately high cost for smaller enterprises. The Commission is comparing and testing the cost estimates provided.

[4] Article 29 Working Party Opinion 3/2006. WP 119, 25 March 2006.
[5] Recital 13.

15. At the same time, some Member States argue that data retention is a standard overhead for an enterprise that decides to establish its operations in their territory. Therefore, there is no level playing field for industry because inconsistent cost recovery. Furthermore, operators claim that the requirement to invest in data retention systems means those resources cannot be dedicated to research and innovation into client-facing products.

16. There is no standard for handover and use. Operators say that they are not always aware of law enforcement powers, which raises questions of liability. The ETSI Technical Committee on Lawful Interception handover standard[6] aims to provide a two-way user-friendly gateway between the operators and authorities. But these standards are not mandatory and are followed only in a few Member States. Where there is no cost recovery, it is difficult to agree standards for handover. Competent authorities do not appreciate the economic value of the data they request, which could otherwise moderate their requests and make them more proportionate. In certain Member States it is unclear to operators which authorities are competent to request data – this puts operators in an invidious position and generates additional legal costs.

17. Where there are no agreements among the operators and between them and authorities, it can be very difficult for the latter to obtain the data, especially where communication equipment is owned by different legal entities.[7] Therefore, in at least three Member States, each request for data is sent to all major operators in the jurisdiction, distorting the statistics and giving misleading messages.

---

[6] ETSI Committee on lawful interception and retained data to operators and national bodies produces and promotes standards with the aim of cheaper products that take on board the requirements and concerns of a very broad stakeholder community and which lead to predictable workflows. TS 102 656– requirements of LEAs for handling retained data http://pda.etsi.org/pda/home.asp?wki_id=DjRAishnPhJLSLQQXSu,a ; TS 102 657 – Handover interface for the request and delivery of retained data http://pda.etsi.org/pda/home.asp?wki_id=ci3Mqc-sqchkhljoL3a-8 ; TR 102 661 - Security framework in Lawful Interception and Retained Data environment http://pda.etsi.org/pda/home.asp?wki_id=K9Z6zw2v6ISUYVWY8vfWe

[7] This is confirmed by the Experts Group Position Paper 3 on transit providers.

Questions for discussion

18. The following questions are suggested for the working group's discussion:

- How should the EU – at European and national level - address the concerns expressed by law enforcement, data protection authorities and industry, without limiting the operational effectiveness of law enforcement?
- What are the most effective ways of demonstrating value of data retention in general and of the DRD itself?
- What could be the most effective ways of ensuring data security?
- How can the exchange of retained data be best facilitated?
- How can the EU facilitate access for law enforcement to communications data held by information society services where needed?

Next steps

19. A number of possible policy options for reforming the DRD have been identified in response to feedback from stakeholders during the consultation process since May 2011, and taking into account views expressed by MEPs and Member States. At present, the evidence gathered appears to reinforce the conclusions of the evaluation report, namely that data retention remains a valuable tool, but that there are serious shortcomings with the EU framework – including retention periods, clarity of purpose limitation and scope, lack of reimbursement of cost to industry, safeguards for access and use - which must be addressed. In particular, all Member States - not just a minority – need to provide convincing evidence of the value of data retention for security and criminal justice.

20. The Commission is now carrying out an impact assessment on the future options. It has also commissioned a study into approaches to, and the costs and benefits of, data preservation in the EU and around the world. Both exercises should be completed by May 2012, in time for a Commission proposal in July 2012.

DATA RETENTION EXPERT GROUP: LIST OF COST ELEMENTS FOR COMPLYING WITH DATA RETENTION

There is not only the cost for development, maintenance and operation of data retention tools within a provider's PCN/PCS infrastructure but also the cost to the provider's business insofar as the delivery of new innovative services being negatively impacted by the need to implement DR functionality and integrate new equipment into the network whilst maintaining a data retention capability.

Cost Type	**Cost Item (examples)**
Capital expenditure	Training Testing Performance Quality control Continuity Procedures for faulty management Hardware Software Retrieval database enabling convenient and timely search and retrieval of data Collection equipment/ manage acquisition Secure storage equipment Security and encryption tools Development of 'existing network elements' to enable integration/ interface with 'DR elements'/ collection and delivery interfaces/ reengineering of system interfaces following network updates, network expansions or changes to network architectures security and access procedures Continuing integration
Operational expenditure	Wages of operations staff Maintenance of data retention systems equipment Training Operations Testing Performance Quality control Continuity Procedures for faulty management Liaison with competent authorities security and access procedures Continuing integration