Patrick Breyer [...] 29/08/04

Contribution to DG INFSO - DG JAI consultation on traffic data retention

I am writing this contribution as a citizen. This contribution, but not the attached essay, may be made public.

A. The need for a common data retention regime

The consultation document mentioned above states: "*From a European single market point of view, a proportionate and consistent approach in all Member States is desirable. Consistency would avoid the situation where the providers of electronic communications services are confronted with a patchwork of diverse technical and legal environments.*"

Providers of electronic communications services in the EU are confronted with a multitude of different regulation regimes and laws in Member States today. So why would exactly the issue of data retention need to be harmonised? Quite clearly, the real reason for the initiative for a common data retention regime is to benefit law enforcement (see reasons 1-6 of proposal). If that is so, then harmonisation should not be used as a pretext. That is especially so because the current proposal for a framework decision would not harmonise retention periods (see Art. 4-1 of proposal) and requirements at all, but providers would still be confronted with a patchwork of requirements. The only "harmonisation" it would bring about is that data retention would be compulsory in every Member State.

However, service providers complain strongly about any data retention legislation[1]. Surely, they would prefer not to be subjected to such legislation in some member states rather than having to retain data in all member states due to "harmonisation" measures. In fact, I do not know of a single provider who is not under obligation to retain traffic data at present but calls for the introduction of a harmonised regime.

Furthermore, there is a strong concern that Member States use the intransparent and undemocratic procedure under the current TEU to introduce data retention legislation which national parliaments or the European Parliament would otherwise reject. In fact, proposals for data retention legislation have been repeatedly rejected by the German parliament, for example. Likewise, the European Parliament has spoken out against data retention[2]. Art. 34 and Art. 39 TEU do not provide for an appropriate procedure for deciding on an issue as sensitive and controversial as data retention.

In addition, the principle of subsidiarity (Art. 5 TEC, Art. 2 TEU) should be strictly applied. Just like in other areas of law enforcement, Member States should retain the right to decide for or against data retention by themselves.

---

[1] See various submissions to the European Commission for the Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/PublicHearingPresentations/; *ECTA, European Competitive Telecommunications Association*: ECTA attacks EU Government plans to undermine internet users privacy and increase costs, ECTA News release, 11/09/2002, https://www.ectaportal.com/uploads/-1413Data_retention_110902.doc; *ECTA, European Competitive Telecommunications Association*: ECTA position on data retention in the EU, August 2002, https://www.ectaportal.com/uploads/-1412ECTAdataretentionstatement.DOC; *EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.)*: Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30/09/2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf; *ICC/UNICE/EICTA/INTUG*, Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, 04/06/2003, www.statewatch.org/news/2003/jun/CommonIndustryPositionondataretention.pdf; *G8 Government-Industry Workshop on Safety and Security in Cyberspace:* Report of Workshop 1: Data Retention, Tokyo, May 2001, www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.html.

[2] Recommendation A5-0284/2001 of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001/2070(COS)), dated 06/09/2001; see also *Art. 29 Data Protection Working Party*, Opinion 2/99, dated 03.05.1999, europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp18en.pdf, p. 5.

The only legitimate need for harmonisation exists in the area of the exchange of traffic data between member states as well as in the area of international data preservation requests. However, these issues are already addressed by the Council of Europe Cybercrime Convention, which makes it debatable whether there is a need for EU action in these areas already covered by the Convention. Even if it was decided that there was a need, it is important not to include any data retention provisions in a common instrument. An opt-out clause would definitely not be sufficient since there would be de-facto pressure on member states not to opt out of a data retention clause.

B. The need for data retention

The consultation document seeks information on "*the number and frequency at which requests for given types of data are made*". On this subject, I would like to comment that calculations made by the biggest internet service provider in Germany, T-Online International AG, show that only 0.0004% of all traffic data they process is later requested by government agencies for law enforcement purposes[3]. Therefore, only one in 250,000 communications needs to be traced by government officials, a minuscule portion of all communications taking place.

The consultation document further seeks information on "*the effectiveness of current access regimes*".

It needs to be pointed out that no studies exist on the effectiveness of current access regimes or on whether their effectiveness can be improved by data retention. The benefit of access to traffic data is therefore completely unproven.

Furthermore, it is a common error to mistake the usefulness of access to traffic data in criminal investigations for its effectiveness in crime prevention. There is no indication that an increased access to traffic data would have any impact on crime rates and, therefore, on the citizens' safety. Especially the prevention of acts of terrorism (the reason now given to justify old demands of law enforcement agencies for data retention) cannot seriously be expected to be aided by traffic data retention.

Serious criminals dispose of a multitude of ways to circumvent data retention, such as the use of mobile phones registered on another person's name, the use of stolen mobile phones, of prepaid calling cards or proxy servers on the Internet, the use of public telephone booths or internet cafes. In all of those cases, data retention is useless because authorities cannot establish who the data relates to.

A German study on the surveillance of telecommunications contents has shown that wiretap orders were useful in only 17% of the investigations in which a wiretap order was issued[4]. It is likely that access to traffic data is similarly (in)effective.

The question of effectiveness is covered in more detail in my attached essay.

C. The legality of data retention

The consultation document states: *"In Community law, the 2002 Directive on Privacy and Electronic Communications, adopted after 11 September 2001, has set out conditions under which Member States may adopt legislative measures for law enforcement purposes, including data retention measures..."*. *"Directive 2002/58/EC on Privacy and Electronic Communications does however not fully harmonise the conditions under which traffic data might be retained or otherwise processed for 'public order' purposes." "Determining what would be proportionate and consistent implies an assessment..."*

---

[3] *Uhe, Bianca / Herrmann, Jens:* Überwachung im Internet – Speicherung von personenbezogenen Daten auf Vorrat durch Internet Service Provider, 18.08.2003, ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, p. 161.

[4] *Albrecht, Hans-Jörg / Arnold, Harald / Demko, Daniela / Braun, Elisabeth* et al.*:* Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003, www.bmj.bund.de/media/archive/136.pdf, pp. 455 *et seq*.

These statements imply that the proportionality and legality of data retention merely depend on determining an adequate retention period and other details. This assumption is wrong since data retention is not proportionate in any circumstances[5]. The disproportionality of data retention is demonstrated in detail in my attached essay according to which data retention violates the Articles 8 and 10 ECHR and also, if service providers are not compensated for compliance costs, Art. 1 PECHR.

The EU is bound by the ECHR (Art. 6-2 TEU) and may therefore not introduce a framework decision on data retention.

Neither can directives such as the directive 2002/58/EC deviate from Art. 6-2 TEU and the human rights provisions it refers to. Instead, the directive 2002/58/EC is subject to those human rights provisions. The directive 2002/58/EC can therefore not legalise legislation incompatible with the ECHR, as is the case with data retention legislation.

Besides, the consultation document is misleading in stating: *"In Community law, the 2002 Directive on Privacy and Electronic Communications, adopted after 11 September 2001, has set out conditions under which Member States may adopt legislative measures for law enforcement purposes, including data retention measures"*. Art. 15 of the directive merely sets out conditions under which Member States may deviate from some of the provisions of that directive. It does not legalise such measures in relation to other areas of European law.

Finally, Art. 15-1 of the directive 2002/58/EC does not legalise blanket data retention; it specifically states that "All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union." Art. 15-1 does legalise "legislative measures providing for the retention of data for a limited period", but this includes legislation providing for retention orders on a case-by-case basis. It is indisputable that the retention of traffic data associated with specified communications on a case-by-case basis (see Art. 20 of Convention on Cybercrime) is compatible with human rights. Blanket data retention, however, does not meet this condition.

Patrick Breyer

---

[5] Art. 29 Data Protection Working Party, Opinion 5/2002, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp64_en.pdf; Covington & Burling, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, dated 10/10/2003, http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf, p. 3; Recommendation of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001/2070(COS)), dated 06/09/2001, document reference A5-0284/2001; Statement of the European Data Protection Commissioners, dated 11/09/2002, http://www.fipr.org/press/020911DataCommissioners.html. See also European Parliament resolution on the First Report on the implementation of the Data Protection Directive (95/46/EG), dated 09/03/2004, document reference P5-0104/2004, http://www2.europarl.eu.int/omk/sipade2?SAME_LEVEL=1&LEVEL=5&NAV=S&LSTDOC=Y&DETAIL=&PUBREF=-//EP//TEXT+TA+P5-TA-2004-0141+0+DOC+XML+V0//EN, § 18.