Cecilia Malmström
European Commissioner for Home Affairs
BE-1049 Brussels

3 September 2010

Dear Ms Malmström,

Thank you for your reply of 12 July to the joint letter of more than 100 organisations from 23 European countries asking you to "propose the repeal of the EU requirements regarding data retention in favour of a system of expedited preservation and targeted collection of traffic data".

I welcome your intention to assess the proportionality of directive 2006/24, and I support the opinion you gave in this regard as a Member of European Parliament: "*I have so far not been convinced by the arguments for developing extensive systems for storing data, telephone conversations, e-mails and text messages. Developing these would be a very major encroachment on privacy, with a high risk of the systems being abused in many ways. The fact is that most of us, after all, are not criminals.*"[1] This statement illustrates an understanding of the fact that such encroachments must be necessary and proportionate rather than simply occasionally useful.

In your reply of 12 July you ask for more information regarding two statements in our letter: "*Studies prove that the communications data available without data retention are generally sufficient for effective criminal investigations. Blanket data retention has proven to be superfluous, harmful or even unconstitutional in many states across Europe, such as Austria, Belgium, Germany, Greece, Romania and Sweden.*" We have compiled some evidence on these points:

1) Blanket data retention has proven to be superfluous

This statement firstly relies on the experience of states around the world whose law enforcement agencies operate successfully without relying on blanket data retention. Among these states are Austria, Belgium, Germany, Greece, Romania, Sweden, Canada and EU member states with data retention legislation in place that is not yet being applied. In none of these states has the absence of a data retention scheme lead to a rise in crime, or to a decrease in crime clearance rates, not even in regard to Internet crime. Nor did the coming into force of data retention legislation in other states have any statistically significant effect on crime or crime clearance.

1 Debate of 7 September 2005, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20050907+ITEM-002+DOC+XML+V0//EN&query=INTERV&detail=3-044.

This is exemplified by statistics published by the German Federal Crime Agency (BKA):

German Crime Statistics	2005 *(no data retention)*	2006 *(no data retention)*	2007 *(no data retention)*	2008 *(telephone data retention in force)*	2009 *(telephone and Internet data retention in force)*
Registered crime	6'391'715	6'304'223	6'284'661	*6'114'128*	*6'054'330*
Clearance rate	55.0%	55.4%	55.0%	*54.8%*	*55.6%*
Registered Internet crime	118'036	165'720	179'026	167'451	*206'909*
Clearance rate for Internet crime	84.9%	84.4%	82.9%	79.8%	*75.7%*

This picture is confirmed by statistics published by the Ministry of the Interior of the Czech Republic and by the Police of the Czech Republic:

Czech Crime Statistics	2003 *(no data retention)*	2004 *(no data retention)*	2005 *(telephone and Internet data retention introduced)*	2006 *(telephone and Internet data retention in force)*	2007 *(telephone and Internet data retention in force)*	2008 *(telephone and Internet data retention in force)*	2009 *(telephone and Internet data retention in force)*
Registered crime	357'740	351'629	*344'060*	*336'446*	*357'391*	*343'799*	*332'829*
Clearance rate	37.9%	38.2%	*39.3%*	*39.7%*	*38.9%*	*37.2%*	*38.3%*
Requests for retained data	0	0	*[n/a]*	*[n/a]*	*[n/a]*	*131'560*	*145'368*

An independent study commissioned by the German government found that among a sample set of 1.257 law enforcement requests for traffic data made in 2005, only 4% of requests could not be (fully) served for a lack of retained data.[2] Taking into account the total number of criminal investigation procedures in 2005, only 0.01% of investigations were affected by a lack of traffic data.[3] About one third of the suspects in those procedures were still taken to court on the basis of other evidence.[4] Moreover 72% of investigations with fully successful requests for traffic data did still not result in an indictment.[5] All in all, blanket data retention would have made a difference to 0.002% of criminal investigations at most.[6] This figure does not change significantly when taking into account that in the absence of a blanket data retention scheme, less requests are made in the first place.[7]

Similarly a Dutch study of 65 case files found that requests for traffic data could "nearly always" be served even in the absence of compulsory data retention.[8] The cases studied were almost all solved or helped using traffic data that was available without compulsory data retention.[9]

The German Federal Crime Agency (BKA) counted only 381 criminal investigation procedures in which traffic data was lacking in 2005.[10] In view of a total of 6 million procedures in 2005, no more than 0.01% of criminal investigation procedures were potentially affected. In the absence of a blanket traffic data retention regime, German law enforcement agencies have consistently cleared more than 70% of all reported Internet offences, significantly outperforming the average crime clearance rate (about 50%).

Notwithstanding this comprehensive evidence, I would like to recall that we cannot be expected to prove that blanket data retention is superfluous. The onus of proof regarding the alleged necessity of blanket data retention is clearly on its proponents. In our response[11] to your evaluation questionnaire we explained why access statistics, anecdotal evidence or perceived utility[12] do not prove a need for blanket data retention: Successful requests for traffic data retained under directive

2 Max Planck Institute for Foreign and International Criminal Law, The Right of Discovery Concerning Telecommunication Traffic Data According to §§ 100g, 100h of the German Code of Criminal Procedure, March 2008, http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf, p. 150.

3 Starostik, Pleadings of 17 March 2008, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf, p. 2.

4 Starostik, Pleadings of 17 March 2008, p. 2.

5 Starostik, Pleadings of 17 March 2008, p. 2.

6 Starostik, Pleadings of 17 March 2008, p. 2.

7 Starostik, Pleadings of 17 March 2008, p. 2.

8 Erasmus University Rotterdam, Who retains something has something, 2005, http://www.erfgoedinspectie.nl/uploads/publications/Wie%20wat%20bewaart.pdf, p. 43.

9 Erasmus University Rotterdam, Who retains something has something, 2005, http://www.erfgoedinspectie.nl/uploads/publications/Wie%20wat%20bewaart.pdf, p. 28.

10 Starostik, Pleadings of 17 March 2008, p. 2.

11 Antworten auf den Fragebogen der Europäischen Kommission vom 30.09.2009 zur Vorratsdatenspeicherung, http://www.vorratsdatenspeicherung.de/images/antworten_kommission_vds_2009-11-13.pdf, p. 29.

12 Such as cited in the "Overview of information management in the area of freedom, security and justice", COM(2010)385, p. 36, as well as in a "Room Document", http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf.

2006/24 do not prove that data would otherwise have been lacking, despite the commercial billing data stored under directive 2002/58 and extra data stored in compliance with specific judicial orders. Even in the relatively rare cases where extra data is disclosed under data retention schemes, it often has no influence on the outcome of the investigation procedure.

The possible occasional utility of access to communications data by law enforcement agencies does not mean that there was a need to retain such data indiscriminately. The European Court of Human Rights has consistently held that mere usefulness does not satisfy the test of necessity.[13] As there is a danger that the Commission might rely on inconclusive data provided by member states, I would like to cite the European Court of Human Rights' critical comments on similar data regarding the retention of biometric data: "*It is true, as pointed out by the applicants, that the figures do not reveal the extent to which this 'link' with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons. Nor do they demonstrate that the high number of successful matches with crime-scene stains was only made possible through indefinite retention of DNA records of all such persons.*"[14]

2) Blanket data retention has proven to be harmful

A poll[15] of 1,000 Germans found in 2008 that indiscriminate bulk communications data retention is acting as a serious deterrent to the use of telephones, mobile phones, e-mail and the Internet. The survey conducted by research institute Forsa found that with communications data retention in place, one in two Germans would refrain from contacting a marriage counsellor, a psychotherapist or a drug abuse counsellor by telephone, mobile phone or e-mail if they needed their help. One in thirteen people said they had already refrained from using telephone, mobile phone or e-mail at least once because of data retention, which extrapolates to 6.5 mio. Germans in total. There can be no doubt that obstructing confidential access to help facilities poses a danger to the physical and mental health of people in need as well as to the safety of the people around them.

In a poll of 1,489 German journalists commissioned in 2008, one in fourteen journalists reported that the awareness of all communications data being retained had at least once had a negative effect on contacts with their sources.[16] This extrapolates to more than 3'000 affected German journalists in total. The inability to electronically receive information through untraceable channels with blanket data retention in place affects not only the press, but all watchdogs including government authorities.

---

13 Silver v. UK (1983) 5 EHRR 347, § 97.

14 Marper v United Kingdom (2009) 48 EHRR 50, § 116.

15 Forsa, Opinions of citizens on data retention, 2 June 2008, http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf or http://www.webcitation.org/5sLeT8Goj.

16 Meyen/Springer/Pfaff-Rüdiger, Free Journalists in Germany, 20 May 2008, http://www.dfjv.de/fileadmin/user_upload/pdf/DFJV_Studie_Freie_Journalisten.pdf or http://www.webcitation.org/5sLdXIt55, p. 22.

Apart from this statistical evidence the German Working Group on Data Retention has received ample reports on negative effects of data retention, which have been summarised in our response to your evaluation questionnaire.[17] The indiscriminate retention of all communications data has turned out to disrupt confidential communications in many areas, affecting victims of sexual abuse or family violence, political activists, journalists, accountants, lawyers, businessmen, psychotherapists and operators of crisis lines for drug abuse victims, pregnant teenagers, molested children etc.

A poll of 2,176 Germans found in 2009 that 69.3% oppose data retention, making it the most strongly rejected surveillance scheme of all, including biometric passports, access to financial data, remote computer searches and PNR retention.[18] It appears the public opinion has not yet been tested on a European scale. We would be happy to assist in preparing a Eurobarometer poll on the matter. A 2008 Eurobarometer poll found that a large majority of 69-81% of EU citizens rejected the idea of "monitoring" Internet use or phone calls of non-suspects even in light of the fight against international terrorism.[19]

3) Blanket data retention has proven to be unconstitutional

Last year the Romanian Constitutional Court found that data retention per se breached Article 8 of the European Convention on Human Rights: "*[Data retention] equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. Law 298/2008 [applies] practically to all physical and legal persons users of electronic communication services or public communication networks – so, it cannot be considered to be in agreement with the provisions in the Constitution and Convention for the defence of human rights and fundamental freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression.*"[20]

Earlier this year the Federal Constitutional Court of Germany ruled the German data retention requirements unconstitutional and void for being disproportionate in their concrete form.[21] Although the Court considered that data retention did not per se breach the German constitution, it did not assess the compatibility of data retention with the European Convention on Human Rights, or with the EU Charter of Fundamental Rights. Yet it made clear that surveillance programs may not exceed an absolute overall constitutional threshold for the collection of personal data by

17 Antworten auf den Fragebogen der Europäischen Kommission vom 30.09.2009 zur Vorratsdatenspeicherung, http://www.vorratsdatenspeicherung.de/images/antworten_kommission_vds_2009-11-13.pdf, p. 2.

18 Infas poll, http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf.

19 Flash Eurobarometer, Data Protection in the European Union, February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf, p. 48 (32+18+19=69%, 35+21+25=81%).

20 Constitutional Court of Romania, decision of 8 October 2009, http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

21 Federal Constitutional Court of Germany, decision of 2 March 2010, http://www.bverfg.de/en/press/bvg10-011en.html.

governments, and that telecommunications data retention would bring the surveillance situation in Germany very close to this barrier. Future surveillance measures might be found unconstitutional not even for being disproportionate in themselves, but for exceeding this overall surveillance barrier. Therefore, maintaining blanket and superfluous data retention jeopardises the constitutionality of more effective and targeted future measures.

There are further complaints pending before the Hungarian Constitutional Court[22] and before the Irish High Court. Recently, the Irish High Court ruled in favour of a request to challenge the Data Retention Directive at the EU Court of Justice. The Court found that data retention had the potential to be of "importance to the whole nature of our society". "*[I]t is clear that where surveillance is undertaken it must be justified and generally should be targeted*".[23] The Court ruled that civil liberties campaign group Digital Rights Ireland had the right to contest "whether the impugned provisions violate citizen's rights to privacy and communications" under the EU treaties, the European Convention on Human Rights and the EU Charter of Fundamental Rights. The reference to the EU Court of Justice is expected in the next weeks.

The EU Court of Justice can be expected to follow the previous rulings and, applying the jurisprudence of the European Court of Human Rights, annul directive 2006/24. The Grand Chamber of the latter Court found in 2008 that the retention of biometrics on mere suspects breached Article 8 of the European Convention on Human Rights: "*In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.*"[24] This assessment of the collection of identification data on 5 million citizens[25] must, *a fortiori*, apply to the much larger collection of information on the daily communications and contacts of 500 million citizens throughout the EU.

---

22 Hungarian Civil Liberties Union, Constitutional Complaint Filed by HCLU Against Hungarian Telecom Data Retention Regulations, 2 June 2008, http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention-regulat.

23 High Court of Ireland, decision of 5 May 2010, http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs.

24 European Court of Human Rights, decision of 4 December 2008, http://www.webcitation.org/5g6FzdBr4, § 125.

25 Human Genetics Commission, Nothing to hide, nothing to Fear?, November 2009, http://www.hgc.gov.uk/UploadDocs/DocPub/Document/Nothing%20to%20hide,%20nothing%20to%20fear%20-%20online%20version.pdf, p. 4.

4) Proposal

Repealing directive 2006/24 would not prevent member states from maintaining data retention schemes and would remove the upper limits the directive sets. We are therefore currently discussing, both in our coalition and with industry, a joint proposal to limit the application of directive 2006/24 to member states that decide to impose data retention nationally. According to this proposal, directive 2006/24 should be amended to give member states a choice: First the option of sticking with directive 2002/58 and the Council of Europe's Convention on Cybercrime that sets an international standard for a system of expedited preservation and targeted collection of traffic data. Second the option of a harmonised and minimised data retention scheme with compulsory cost reimbursement for providers. There are many advantages to such a two-pronged proposal in comparison to a mere repetition, more or less, of the initial proposal that was put forward by the Commission in 2005.[26] I am setting out some of those advantages in a separate document attached to this letter.

We would welcome very much your embracing of this concept in the upcoming evaluation report, and in a subsequent legislative proposal. Please be assured of our full support in removing compulsory EU requirements regarding blanket communications data retention in favour of an option to stick with the internationally agreed system of expedited preservation and targeted collection of traffic data.

Yours sincerely,

Dr. Patrick Breyer
Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention)

cc. Ms Viviane Reding, Vice President
Ms Neelie Kroes, Vice President

26 COM(2005)438.

Draft Proposal regarding Telecommunications Data Retention

The EU data retention directive, adopted in 2006, currently requires all 27 EU member states to compel telecommunications and Internet companies to indiscriminately collect data about all of their customers' communications. "*The majority of Member States do not reimburse costs incurred by operators to retain and retrieve data*", the Commission reports. The Commission is currently considering replacing the current directive with a harmonised and more limited data retention regime that would include a cost reimbursement provision.

Why should the Commission not solely propose a harmonised data retention regime with compulsory cost reimbursement?

A proposal to this effect is unlikely to succeed and may result in no changes to the data retention directive at all. This would mean that all providers in the EU would continue to be compelled to retain and hand over varying types of data, mostly at their own expense, and to the detriment of all 500 million citizens in the EU.

The Commission's initial proposal for the data retention directive (COM/2005/0438) already once suggested a uniform data retention regime with compulsory cost reimbursement. This proposal was clearly rejected by member states due to differing legal traditions and due to the high cost of blanket data retention. This situation persists in 2010. It is unlikely that a voting majority of the 27 EU member states would be prepared to accept a uniform data retention regime with compulsory cost reimbursement.

In addition, even where some cost reimbursement is in place, it generally covers only a share of the total cost of retrieving, storing and handing over of bulk data. Data retention is never profitable but always troublesome and distracts providers from their business. The constant risk of a theft, loss or abuse of sensitive communications data puts providers' reputation at risk. Citizens dislike a blanket retention of their communications data in the absence of any suspicion.

What should the Commission propose instead?

The EU data retention directive should offer two alternatives to member states: First the option of sticking with directive 2002/58 and the Council of Europe's Convention on Cybercrime that sets an international standard for a system of expedited preservation and targeted collection of traffic data. Second the option of a harmonised and minimised data retention scheme with compulsory cost reimbursement for providers.

What are the advantages of an optional approach?

National data retention provisions need to be harmonised only where they are in place. In member states that do not require blanket data retention, directive 2002/58 is achieving an even better harmonisation. While it is true that making data retention optional does not provide for total harmonisation, neither does the current directive. The national implementations currently in force

vary so widely in terms of data types, storage periods, reimbursement and access that the situation is actually more harmonised in countries that have decided to stick with directive 2002/58 and not impose blanket data retention at all. Making data retention optional at the EU level would also remove the legal risk of directive 2006/24 being annulled. Furthermore it would take into account the situation of member states that are legally unable (Romania) or politically unwilling to introduce blanket data retention legislation. Differences in legal traditions, constitutions and political preferences in member states are too great to impose data retention on all member states.

For industry, optionality is the only feasible way to prevent member states from adopting or maintaining costly and uncompensated data retention requirements. Member states are more likely to accept a harmonised data retention regime with compulsory cost reimbursement if they are given the alternative to opt out. Some member states would be happy not to introduce data retention requirements at all for political, constitutional of financial reasons. The German liberal coalition partner has already decided not to re-introduce data retention legislation if given a choice by the EU. Romania has been prohibited from introducing data retention legislation by its Constitutional Court. At present several states across Europe do not have data retention requirements in place (e.g. Austria, Belgium, Germany, Greece, Romania, Sweden). Whereas the current data retention directive will ultimately force thousands of providers in these countries to retain data at their own cost, an optional directive would take that burden off those providers entirely. Other member states would still insist on having data retained, but could be convinced to accept having to compensate providers by at least reimbursing a fair share of their costs.

For citizens, making data retention optional would finally give national parliaments, the citizens (in referendums) and Constitutional Courts the opportunity to opt for a targeted approach instead of indiscriminately having the entire population's communications data retained. In June, more than 100 organisations from 23 European countries set out in a joint letter the reasons for why data retention legislation should be repealed. Among the supporters of the letter are major NGOs such as EDRi, FFII and Human Rights Watch.

The Commission, industry and civil society jointly pushing for making the data retention directive optional and more harmonised as set out above could create political majorities that would otherwise not be possible to achieve. Civil society is a major political factor and has a strong interest in making the data retention directive optional. We invite the Commission to embrace the concept of optionality in the upcoming evaluation report.

3 September 2010