26 September 2011

cc: Vice-President Kroes
Vice-President Reding

Dear Commissioner Malmström,

As you know, civil society groups have been closely involved in consultations with the European Commission with regard to the impact assessment on, and probable review of, the Data Retention Directive. In keeping with this ongoing cooperation, European Digital Rights and the organisations listed at the end of this letter would like to share our views on the current deliberations on this important legislation.

We remain committed to the impact assessment for the new legislative proposal being as credible and complete as possible. Since the impact assessment supporting the original Directive was exceptionally poor and since this Commission has sworn a legally binding oath to respect fundamental rights,[1] it is very important that the impact assessment address all concerns regarding the compatibility of the Directive with the Charter of Fundamental Rights and the European Convention on Human Rights, in particular in the light of relevant recent case law.[2]

We remain convinced that a comprehensive impact assessment will definitively show that data retention is neither necessary for market harmonisation nor for the fight against serious crime and is, therefore, illegal.

This letter is to provide you with our views on the minimum criteria for the impact assessment and subsequent legislative proposal.

A: Fundamental Rights Checklist

We believe that the Commission has already given itself a valuable tool for ensuring that adequate attention is given to fundamental rights in all of its proposals, namely Communication COM(2010)573 and its "fundamental rights checklist". Full respect for the checklist, and articles 5 and 6 in particular, should result in an impact assessment and legislative proposal which respect the EU's legal obligations on fundamental rights.

Point 5 of that list asks "*Would any limitation of fundamental rights be formulated in a clear and predictable manner?"*

This would require the following questions to be asked:

–In the absence of a definition of "serious crime", is it possible (and if so, why) to have a clear and predictable implementation of the Directive across the EU, particularly for cross-border communications?
–Does the huge time range – from 6 months to 24 months – offer clarity and predictability, particularly for citizens involved in cross-border communications?

1 European Commission swears oath to respect the EU Treaties, IP/10/487, 3 May 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/487
2 Such as S. and Marper v. the United Kingdom (application nos. 30562/04 and 30566/04) and ECJ 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke.

–What elements of the review process have identified systemic breaches of fundamental rights that need to be addressed in order to ensure that citizens can have reasonable legal certainty regarding how their data is being processed?[3]

Point 6 of that checklist list asks:

"Would any limitation of fundamental rights:

> *–be necessary to achieve an objective of general interest or to protect the rights and freedoms of others (which)?*
> *–be proportionate to the desired aim?*
> *–preserve the essence of the fundamental rights concerned?"*

A.1: Necessity and Proportionality

This point can only be answered if a full assessment of alternatives in *every* aspect of the Directive is undertaken. This would include an assessment of each category and size of service provider addressed, of each individual type of data and of the retention period for each type of data in order to assess its necessity to achieve the objectives of the existing or revised legislation.

Furthermore, it will be crucial for the credibility of the impact assessment not to repeat the fault in the evaluation report (COM(2011) 225 final) where the necessity and proportionality of data retention and the necessity of having a Directive on data retention, were treated as if they are the same. Both elements need to be evaluated in isolation in order to assess if data retention is "necessary to achieve an objective of general interest" and "proportionate to the desired aim" and if a Directive is necessary for this purpose.

A second flaw in the evaluation report that must be avoided is that it refers to "retained data" in general. It should distinguish between the data available through the storage of traffic and location data regulated by the E-Privacy Directive (2002/58/EC) and the additional data required by the Data Retention Directive.

The third element that must be adequately addressed is assessing the range of other options available:

–a ban on blanket data retention regimes in Europe

The anecdotes provided in the original impact assessment are far from being compelling evidence of the necessity of data retention.[4] Their weight is further diminished by the fact that, in several of the anecdotes, data was used that would have certainly been available in any case. If data retention is, indeed, pointless and even counterproductive and is undermining the Single Market as the evaluation report suggests, the Commission has a duty to act in order to remove this impediment.

---

3 Such as the implementation report's reference to domestic operators providing access to data on foreign communications as an alternative to following the proper mutual legal assistance procedures. Evaluation report on the Data Retention Directive (Directive 2006/24/EC, COM(2011) 225 final, p.22/23.

4In one of the examples provided, a proper analysis of the incident in question would show that long-term retention would not have been necessary in the absence of profound failures in the efficiency of international police cooperation which, instead of being addressed and resolved, are propagated by the existing data retention regime.

–replacement of the Directive with a less restrictive alternative such as targeted collection of data and expedited data preservation

In its preparation of the evaluation report, the Commission did not seek to obtain information from Member States that have not implemented the Directive, in order to compare the efficacy of alternative approaches.[5] It also did not look at the experience of countries which have implemented the approach preferred by the Council of Europe's Cybercrime Convention, namely expedited data preservation. This approach is quite clearly a “measure which affects less adversely the fundamental rights of natural persons” than massive long-term storage of communications data on all citizens “and which still contributes effectively to the objectives of the European Union rules in question.”[6] This alternative should be thoroughly assessed in order to credibly show whether any amount of untargeted data retention is strictly necessary and proportionate and that a Directive is needed.

–removing the minimum retention period and re-assessing the maximum retention period

Taking into account the strict criteria set out in the Charter, the Convention and relevant case-law, the European Union may enact legislation that places restrictions on the fundamental rights of citizens. In the case of data retention – and the post-Lisbon Treaty legal framework will inevitably lead to this issue coming up repeatedly - the democratically elected parliaments as well as Constitutional Courts of several sovereign Member States quite clearly do not consider that the fundamental rights restrictions are, as *required* by the European Convention on Human Rights, “necessary in a democratic society” and, as a result, have not implemented the Directive. The Commission is taking infringement proceedings against these countries, offering no margin of appreciation and no respect for subsidiarity and, in essence, is forcing those countries - according to the assessment of those democratically elected governments - to breach the Convention.

One option to avoid this problem is to establish a maximum retention period but not minimum periods. If, as the Commission says, cross-border requests for data represent fewer than 1% of uses of retained data - and bearing in mind that a proportion of these would be available under expedited preservation - this would:

–not present particular problems for cross-border law enforcement;
–provide a “margin of appreciation” for Member States that believe that data retention is not necessary and;
–measurably and significantly support the single market, particularly if cost reimbursement for providers under a blanket retention obligation were made compulsory.

In order to assess the impact of the various options presented on the prosecution of serious crime in a scientifically valid way, the impact assessment would need to address the following points:

–In how many cases does the detection, investigation or prosecution of serious crime in the absence of blanket retention legislation lack communications data that

5 COM HOME A3/JV/cn D (2010) 11574, 27 July 2010, https://www.bof.nl/live/wp-content/uploads/Letter-to-MS-supp-info-on-DRD.pdf
6 ECJ 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke, §86.

would be available under a blanket retention scheme (quantify as a percentage of all serious crime being investigated or prosecuted)?

–To the prosecution of how many serious crimes does such extra communications data ultimately make a positive difference (quantify as a percentage of all serious crime being prosecuted)?

–Is any such benefit offset by counter-productive side effects of blanket data retention (e.g. furthering the use of circumvention techniques and other communication channels)?

–All in all, does the presence or absence of blanket data retention legislation in practice have a demonstrable, statistically significant impact on the prevalence or the investigation of serious crime in a given Member State? If it does have a significant impact, by how many percent does it increase or decrease the prevalence, the clearance or the prosecution of serious crime? Has the introduction or the absence of blanket data retention legislation in the past made a significant difference to the number of prosecutions or acquittals or the closure or discontinuation of serious crime cases in any given state? By how many percent did the number of condemnations, acquittals or the closure or discontinuation of serious crime cases increase or decrease as a result of blanket data retention legislation or its absence?

A.2: Preserving the essence of the right

Article 52 of the Charter of Fundamental Rights of the European Union states that limitations of fundamental rights must not restrict or reduce the right in such a way or to such extent that the very essence of the right is impaired. The European Court of Human Rights has ruled similarly on numerous occasions.[7] In its Evaluation Report, the European Commission identified points that are peripheral to the achievement of the goals of the Directive, but undermine the essence of the fundamental rights impacted by the Directive.

–Experience of the impact on fundamental rights

It will be impossible for the European Commission to fully respect its own fundamental rights checklist without a comprehensive analysis of the extent to which the rights in question have been undermined by the existing Directive. Without learning from this experience, it will be impossible to ensure respect for the Charter. In particular, attention should be given to experience with regard to:

-Data losses and abuse.[8]
-Mistakes in data retrieval.[9]
-Damage to the right to communication caused by citizens and businesses feeling unable to confidentially communicate with health professionals,

7 ECtHR 11 July 2002, nr. 28957/95, Goodwin v The United Kingdom, §99: '*... the limitations (thereby) introduced must not restrict or reduce the right in such a way or to such an extent that the very essence of the right is impaired*'. The ruling also refers to the ECtHR *Rees* and *F. v. Switzerland* judgements.
8 Examples of data losses and data abuse across Europe can be found in: Arbeitskreis Vorratsdatenspeicherung, 'There is no such thing as secure data', http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf
9 'ISP Wrongfully Sent 300 “First Strike” Letters To Innocents', 17 June 2011, http://torrentfreak.com/isp-wrongfully-sent-300-first-strike-letters-to-innocents-110617/

lawyers, journalists,[10] etc.[11]

–Definition of “serious crime”

As some Member States do not have a definition of serious crime, we already see that the scope is far broader than intended by the legislator. Therefore, in addition to the fact that the outcome of legislation has proven problematic in the area of foreseeability, many uses of data retained under the Directive fail to respect the essence of the fundamental rights in question. The far-reaching consequences of not strictly defining 'serious crime' in the Directive have been illustrated clearly in Poland, where authorities accessed communications data more than 1 million times in 2009, using the retained data far beyond the prosecution of 'serious crimes' – even in civil proceedings.[12] Alarmingly, the Commission recently seemed to argue that the telecommunication data retained only for the investigation and prosecution of serious crime can also be used without problems in order to investigate intellectual property-related offences, that might not even be crimes, let alone serious crimes.[13]

–Analysis of each data set

When legislation mandates indiscriminate storage of personal data that is not strictly necessary, the legislation harms the essence of the fundamental right to privacy. It is illogical to assume that retention of all communications data would be necessary, or even useful, for the same periods of time and that each type of data is of equal value. The Commission should therefore make a credible effort to demonstrate the alleged necessity of each data set that is in the current Directive or in the new legislative proposal. Furthermore, in the absence of the necessary practical data being made available by the Member States, the Commission must explain to the Council that lack of data proving necessity means that it is legally obliged to remove that data set from the Directive.

–Access and security restrictions

For the same reasons as mentioned above, the Commission needs to assess if and exactly which minimum access restrictions and data security safeguards could be set by the Directive in order to better protect fundamental rights. It would be far easier to establish a baseline in the revised Directive than seek to impose minimum safeguards on Member States after transposing legislation has been adopted.

–Centralised storage and direct access

The European Commission should analyse whether it considers that circumstances exist where the advantages of centralised data storage outweigh the security and privacy risks that such an approach inevitably entails. If such circumstances do not exist, this approach should be explicitly excluded by the Directive. Similarly, are there circumstances in which direct access to this data would not automatically be in breach of Article 8 of the European Convention on Human Rights? Again, if no such circumstances exist, this option should be specifically excluded by the Directive.

---

10 European Journalists Warn EU Home Affairs Chief that European Data Law Threatens Freedom, 01 October 2010, http://europe.ifj.org/fr/articles/european-journalists-warn-eu-home-affairs-chief-that-european-data-law-threatens-freedom

11 FORSA, Opinions of citizens on data retention, 2 June 2008, p. 3, http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf

12 'POLAND: Data retention and population surveillance', November 2010, Statewatch RefNo# 30113, http://database.statewatch.org/article.asp?aid=30113

13ECJ Hearing on Bonnier Audio c.s. case (only in Swedish), C-461/10, http://www.edri.org/files/C461-10-rapport.pdf

-Violation of protection of journalists' sources and media freedom.

B: Article 15.1 of Directive 2002/58

We were disturbed to see in the evaluation report an interpretation of the legal significance of Article 15.1 of the E-Privacy Directive that not only contradicts legal reality, but also contradicts the European Commission's own declaration on this text. At the time of adoption of the legislation, the European Commission pointed out the legal fact that the Directive could neither authorise nor prohibit any activity in the then third pillar.[14] We urge the European Commission to avoid making the same mistake in the impact assessment.

C: Impact on the Single Market

In its evaluation report, the European Commission listed a range of ways in which the Data Retention Directive undermined the Single Market and failed to provide any compelling evidence that the Directive has had any corresponding positive impact. This raises serious questions as to the legality and value of the Directive if the "objective of general interest" to be achieved is harmonisation. If the Commission intends to keep the same legal basis, it should specifically indicate how the objective of harmonisation has been achieved, or may be achieved, through this instrument. Furthermore, it should indicate exactly why it believes that the range of damaging effects that it has identified in the existing Directive will be resolved by the proposed changes to the legislation.

-Cost reimbursement

It is clear that a harmonised cost reimbursement scheme would be of more positive impact for the internal market than the current and somewhat chaotic situation described in the Commission's impact assessment. The impact assessment must therefore specifically address the viability of this approach. By "costs", we mean capital costs, access costs and personnel costs. Furthermore, it appears to be unquestionable that state authorities will be more restrained in their requests for retained data when this has to be justified in their budget.

We trust that this constructive input will assist you in preparing the impact assessment and reviewing the Data Retention Directive. We remain at your disposal as a constructive partner in this process.

Yours sincerely,

Andreas Krisch
EDRi President

European Digital Rights
39/9 Rue Montoyer
B-1000 Brussels
Tel: +32 2 550 4112
http://www.edri.org

14 COM/2002/0338 def, 17 june 2002, p. 3, under "Amendment 47 - Recital 11 ; Amendment 46 - Article 15, paragraph 1", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002PC0338:EN:HTML.

Co-signatories:

Access
Aktion Freiheit statt Angst
AKVorrat.at - Arbeitskreis Vorratsdaten Österreich
Arbeitskreis Vorratsdatenspeicherung
Association for Technology and Internet - Asociatia pentru Tehnologie si Internet
Assn of Democratic Lawyers (Vereinigung Demokratische Juristinnen und Juristen e.V)
Belgian Net Users' Rights Protection Association (NURPA)
Bits of Freedom
Centar za mir i razvoj demokratije/ Center for Peace and Democracy Development
Deutscher Presse Verband
Digital Rights Ireland
Electronic Frontier Foundation
European Federation of Journalists
Humanistisch Verbond
Hungarian Civil Liberties Union
Internet Society Netherlands
Ireland Offline
ISP-Connect
IT-POL Denmark
Iuridicum Remedium
Lawyers' Committee for Human Rights - Komitet pravnika za ljudska prava
Liga voor Mensenrechten
Ligue des Droits de l'Homme (Belgium)
Nederlandse Vereniging van Journalisten
Netzpolitik.org
NLNet Foundation
Panoptykon
Polish Chamber of Commerce for Electronics and Telecommunications
Privacy First Foundation
Privacy International
Spoločnosť pre otvorené informačné technológie - The Society for Open Information Technologies
Statewatch
Stichting meldpunt Misbruik ID-plicht
Verbraucherzentrale Bundesverband e.V. – Federation of German Consumer Organisations
Vereniging Vrijbit-NL
Vibe!AT
Vrijschrift