Shadow evaluation report on

the Data Retention Directive (2006/24/EC)

17 April 2011

European Digital Rights
Rue Montoyer 39/3, B-1000 Brussels
E-Mail: brussels@edri.org, http://www.edri.org

1. Introduction

The EU Data Retention Directive (2006/24/EC) requires telecommunications companies to store data about all of their customers' communications. Although ostensibly introduced to reduce barriers to the single market, the Directive was proposed as a measure aimed at facilitating criminal investigations. The Directive creates a process for recording details of who communicated with whom via various electronic communications systems. In the case of mobile phone calls and SMS messages, the physical location of the users is also recorded. The traceability of internet usage is also facilitated.

Over the past five years, the Data Retention Directive has proved to be an unnecessary and unprecedented violation of the fundamental rights of 500 million Europeans. According to the European Data Protection Supervisor, the Directive constitutes "the most privacy invasive instrument ever adopted by the EU".[1] It is also possibly the most controversial European surveillance instrument and has sparked protest throughout Europe.[2] After the Data Retention Directive came in effect in early 2006, several Constitutional Courts have either rejected the principle of blanket and indiscriminate telecommunications data retention out of hand or have firmly rejected national implementation laws.

Instead of harmonising the EU internal market, the Data Retention Directive has created a patchwork[3] of national blanket retention legislation, significantly larger than what would have existed without the Directive. Many Member States fail to fully respect the data security obligations of the Directive, while statistics provided by the Member States are unreliable and patchy. While the burden of proof concerning the necessity of this measure lies with the Commission, sound analysis of independent statistics point to the fact that the Data Retention Directive is superfluous to the investigation and prosecution of serious crime while creating data security problems and undermining fundamental rights.

The Commission is now publishing a report evaluating the Data Retention Directive and has announced its intention to propose a revision of the Directive later this year. The European Data Protection Supervisor has called the evaluation process "the moment of truth" for this "notorious" directive.[4] European Digital Rights welcomes the legislator's intention to have this controversial Directive and its impact evaluated, but the Commission's evaluation methods have turned out to be fundamentally flawed. Rather than procuring an independent assessment that satisfies scientific standards, the Commission has produced a political document.

Consequently, European Digital Rights has decided to publish this shadow evaluation report to be read alongside with the official report, focusing on the issues that are directly or indirectly relevant to the fundamental rights and freedoms of all EU citizens.

2. Background to the evaluation

1 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

2 Civil society calls for an end to blanket data retention, 106 organisations from all over Europe, 22 June 2010. http://www.vorratsdatenspeicherung.de/content/view/363/158/lang,en/.

3 See "Responses to 2009 EU consultation on data retention": http://wiki.vorratsdatenspeicherung.de/Resources#Responses_to_2009_EU_consultation_on_data_retention

4 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

Article 14 of the Directive obliges the European Commission (EC) to submit a report on the evaluation of the Directive and its impact on economic operators and consumers. The evaluation report should have been completed 'no later than 15 September 2010' (Article 14). The main reason for the seven months of delay is that some crucial mistakes were made at the beginning of the evaluation process. Firstly, the Commission failed to recognise that, under the EU Charter on Fundamental Rights, the Directive is legal only if it is both "necessary and genuinely meet(s) objectives of general interest." The Commission's second mistake was to have decided on the outcome before even having started its research, limiting its scope by only asking questions about the assumed value of data retention to national governments. The Commission then limited itself further by not seeking any information from those Member States that have not implemented the Directive. This has prevented the Commission from being able to assess the necessity of mandatory data retention throughout the EU.

As a result, when the Commission asked national governments for information in the second quarter of 2010, the replies were of little use. Commissioner Malmström subsequently made a personal plea to Member States during the July 15 Justice and Home Affairs Council, followed by a letter to Member States. The letter betrays the Commission's disregard for the EU Charter of Fundamental Rights (which each Commissioner has sworn a legally binding oath to support) by revealing that the Commission was not seeking to assess the "necessity" of blanket communications data retention. The Commission wrote: "without this information it will be difficult for the Commission to adequately demonstrate that the Directive is *useful*".[5] The Commission further lowered the standard of evidence it was requesting by asking for examples of cases where data retained under the Directive "played a determining role", rather than asking for examples of cases which relied on data that would not have been available in the absence of blanket communications data retention.

Having created this untenable situation, the Commission managed to dig itself even deeper during its "Taking on the Data Retention Directive" conference in December 2010.[6] For reasons that are far from obvious, Commissioner Malmström made a speech announcing that "data retention is here to stay", despite the fact that inadequate information had been received from the Member States (who mostly ignored her personal plea at the July Council meeting) and despite the fact that her services were still months from being able to provide a usable summary of the paltry information that had been provided by the Member States.

3. Data Retention in the European Union

3.1. Data retention for criminal justice and law enforcement purposes

Telecommunications data are processed by service and network providers for technical, billing and, where adequate permission from consumers is provided, marketing and other value-added service purposes. Under the E-privacy Directive (2002/58/EC, as amended by Directive 2006/24/EC), unauthorised interception of these data is prohibited and providers shall delete or depersonalise the data as soon as possible (Article 6).

The Data Retention Directive constitutes a radical shift from the E-privacy Directive. It obliges telecommunications companies to store traffic and location data of all their customers' communications, "in order to ensure that the data are available for the purpose of the investigation,

[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] The report of the conference by the European Commission can be found here: https://www.bof.nl/live/wp-content/uploads/295871-Report-conference-DRD-3-December-2010-1.pdf. The report of European Digital Rights can be found here: http://edri.org/edrigram/number8.24/evaluation-data-retention-directive.

detection and prosecution of serious crime" (Article 1 of the Directive). The companies themselves are not permitted to use the retained data and are required to destroy the data at the end of the retention period (Article 8 of the Directive).

Over the past few months, there has been much discussion on the relationship of the Data Retention Directive and Article 15.1 of the E-Privacy Directive. During the negotiations of Article 15.1 of the E-Privacy Directive, the Commission made it clear that this article merely acknowledges the existing legal framework concerning the processing of communications data for law enforcement and other purposes. The Commission pointed out that the E-Privacy Directive could not approve or limit any specific measure, because a single market instrument could not place limits on a third pillar (i.e. law enforcement) policy area.

Article 15.1 of the E-Privacy Directive therefore does not in itself authorise any law enforcement activity by Member States. In the exact words of the Commission: "As the Commission explained in its position on the common position, the present Directive based on Article 95 of the Treaty cannot include substantive provisions on law enforcement measures. It should neither prohibit nor approve any particular measure Member States may deem necessary." Drawing from this analysis, the Commission should not now assign any other meaning to Article 15.1 of the E-Privacy Directive.[7] This analysis is repeatedly contradicted by the Commission's evaluation report, which seeks now, for political reasons, to give the text a new and unjustified meaning.

While the concept of blanket data retention appeals to law enforcement agencies, it has never been shown that the indiscriminate retention of traffic and location data of over 500 million Europeans was necessary, proportionate or even effective. The Commission has never, neither before nor in the years since the Directive came into force , commissioned independent research into whether such data retention without cause is "necessary in a democratic society", which is the minimum standard for a measure to be legal under the EU Charter of Fundamental Rights and the European Convention on Human Rights.

Unfortunately, this lack of evidence has not prevented the Commission from trying to justify blanket and indiscriminate telecommunications data retention by claiming it necessary for prosecuting serious crime. In paragraph 5.3 of this report below we will show that blanket and indiscriminate data retention is neither necessary nor effective, and we will explain the flaws in the Commission's reasoning in detail.

3.2. The aim and legal basis of the Data Retention Directive

The Data Retention Directive is based on article 114 (1) of the Treaty on the Functioning of the European Union, which allows the EU to approximate national laws "with the aim of establishing or ensuring the functioning of the internal market". The EU argues that differing national data retention requirements "may involve substantial investment and operating costs" for service providers,[8] "may constitute obstacles to the free movement of electronic communications services" and "give rise to distortions in competition between undertakings operating on the electronic communications market."[9]

---

7 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.

8 EU Court of Justice (ECJ), case C-301/06, § 68.

9 Opinion by the Advocate General in case C-301/06, § 85.

In truth, the Directive has proven to counter-productive in these respects, creating a far more disjointed situation than had previously existed. When the Data Retention Directive was adopted in 2005/2006, only 5 of the then 25 Member States required communications service providers to retain certain types of communications data on all consumers without suspicion, typically requiring the retention of fewer data for shorter periods of time than the Directive does. Another 5 Member States had legislation in place that would have allowed them to impose data retention requirements in the future.[10] 15 of the then 25 Member States had not enacted any data retention legislation.[11]

Today, the Directive being in force, 22 of 27 Member States are requiring service providers to retain communications data without specific cause,[12] with national obligations varying widely as to:

1. the categories of service providers affected (the Directive imposes minimum requirements only);[13]
2. the types of communications data to be retained (the Directive imposes minimum requirements only);
3. the retention period for each type of data (the Directive imposes a period of 6-24 months for certain types of data and certain purposes);
4. the data security requirements (not harmonised by the Directive);
5. the purposes for which retained data can be used (the Directive imposes minimum requirements only);
6. the conditions and procedure for access to and use of the data (not harmonised by the Directive);
7. the reimbursement of costs (not harmonised by the Directive).

It is apparent from these facts that by requiring all Member States to enact blanket retention legislation, the Directive has led to much higher "investment and operating costs" for service providers in the EU and has resulted in a far larger patchwork of national blanket retention legislation than would have existed without the Directive. The Directive itself therefore constitutes an "obstacle to the free movement of electronic communications services" and "gives rise to distortions in competition between undertakings operating on the electronic communications market".

From an internal market perspective, several options exist to really remove "obstacles to the internal market for electronic communications" without imposing the concept of blanket and indiscriminate telecommunications data retention on all Member States and citizens:

1. The EU could prohibit national legislation mandating blanket data retention without cause in favour of a system of expedited preservation and targeted collection of traffic data as agreed in the Council of Europe's Convention on Cybercrime, an instrument which is otherwise strongly supported by the European Commission.
2. The EU could require Member States with national retention legislation in place to fully compensate the providers affected.

3. The EU could amend the Directive so as to impose limits on (optional) national retention legislation only, rather than impose the concept of blanket communications data on all

[10] Legislation with a view to imposing data retention obligations had been enacted in Belgium, France, Italy, Ireland, Latvia, Lithuania, the Netherlands, Poland, Spain and the Czech Republic.

[11] Commission, SEC(2005)1131.

[12] Legislation transposing the directive is not in effect in Austria, the Czech Republic, Germany, Greece, Romania and Sweden. Based on recent Constitutional Court decisions, blanket retention is likely to be discontinued in other Member States where it is challenged in Constitutional Courts.

[13] For example, the UK does not require small operators to retain data, arguing that "the costs outweigh the benefits".

Member States, and still create a more harmonised market than exists at present. For example, a blanket retention period of 0 to 3 months would create a far more harmonised situation than imposing a retention period of 6-24 months.

When proposing the Data Retention Directive, the Commission itself considered compulsory compensation to be the key element to prevent market distortions: "The cost reimbursement principle will allow creating a level playing field for the electronic communication providers in the internal market."[14] When the Directive was adopted, however, the one element that would have contributed to creating a more level playing field – compulsory cost reimbursement – had been removed from the Directive. For many Member States, data retention is apparently "necessary in a democratic society" but not worth paying for.

Interestingly, the Commission is now citing a study according to which the retention costs of an ISP with half a million subscribers is around 0.75 Euro per subscriber in the first year and 0.24 Euro in subsequent years, with data retrieval costs of about 0.70 Euro per subscriber and year. If blanket retention requirements have "no significant impact" on competition or investment, this removes the legal justification for the EU to harmonise such national legislation. The European Court of Justice has repeatedly held that the EU may rely on article 114 TFEU with a view to "eliminating *appreciable* distortions of competition" only.[15] If national data retention requirements result in costs of no more than 1 or 2 Euros per customer and year, differences cannot seriously be claimed to appreciably distort cross-border competition.

3.3. Data preservation

Rather than collecting information on every electronic communication made by every citizen ("data retention"), a system of expedited preservation and targeted collection of traffic data that assists in a specific investigation ("data preservation") has been agreed internationally in the Council of Europe's 2001 Convention on Cybercrime (described recently by Commissioner Malmström as "an impressively up-to-date instrument"[16]). This approach of targeting suspects of crime instead of putting the entire population under surveillance has been adopted by 30 states world-wide.

Recently Canada has announced plans to create a preservation order that would require a telecommunication service providers to safeguard and not delete its data related to a specific communication or a subscriber when police believe the data will assist in a criminal investigation. A preservation order is a "quick-freeze" temporary order, and is only in effect for as long as it takes law enforcement to return with a search warrant or production order to obtain the data. Canada stresses:

"This is not data retention. Contrary to what is the case in some countries, the amendments would not require custodians of data to collect and store data for a prescribed period of time for all subscribers, regardless of whether or not they are subject to an investigation. A preservation order would be restricted to the data that would assist in a specific investigation."[17]

In the EU, Austria, Belgium (regarding Internet data), the Czech Republic, Germany, Romania and Sweden are currently successfully investigating and prosecuting crime by way of data preservation orders and other targeted investigation techniques.

---

14 SEK(2005)438.

15 ECJ, C-376/98, § 106; C-58/08, § 32.

16 See http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/260&format=HTML&aged=0&language=EN&guiLanguage=en

17 http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32567.html.

Although much less information on confidential communications is recorded under a data preservation scheme, availability is not the same as necessity. The Commission's evaluation report does not demonstrate that any benefits communications data may have for prosecuting crime depend specifically on blanket retention schemes and cannot likewise be achieved under targeted data preservation schemes.

A meaningful assessment of any net effectiveness of blanket retention schemes needs to look at whether, in a given country, serious crime as a whole is prosecuted more effectively under a blanket retention scheme than under a targeted investigation scheme. In a recent study, the Scientific Services of the German Parliament have found no practical effects of data retention on crime clearance rates in EU Member States. After analysing crime clearance rates throughout the EU, the report comes to the following conclusion:

"In most states crime clearance rates have not changed significantly between 2005 and 2010. Only in Latvia did the crime clearance rate rise significantly in 2007. This is related to a new Criminal Procedure Law though and is not reported to be connected to the transposition of the EU Data Retention Directive."[18]

It follows that, in practice, taking all relevant factors into account, crime is investigated and prosecuted just as effectively with targeted investigation techniques that do not rely on blanket retention are used. Blanket and indiscriminate telecommunications data retention has no additional statistically significant impact on the investigation of crime.

4. Transposition of the Data Retention Directive

4.1. Purpose of data retention (Article 1)

The Directive does not regulate the purposes for which retained data can be used. This is because the EU is not competent to legislate on the access by government authorities to communications data held within their own territory for law enforcement purposes. The EU Court of Justice has ruled that the Directive is based on the correct legal basis as it "harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use [...] of those data [by] those authorities".[19] It follows that the EU is not competent under Article 114 TFEU to legislate on the purposes for which national law enforcement agencies can access retained communications data. Nor is the EU competence for police co-operation, judicial co-operation or the approximation of criminal law concerned where a government authority accesses data held within its own territory.[20] Finally the EU is not competent to regulate such access under Article 16 TFEU as the access by government authorities to communications data held within their own territory for law enforcement purposes does not fall within the scope of Union law.

4.2. Operators required to comply with data retention (Article 1)

Finland and the UK exempt small operators from obligations to retain data. This adds another item to the list of options available to perpetrators to avoid the retention of data relating to them.

4.3. Access to data: authorities and procedures and conditions (Article 4)

---

18 Scientific Services of the German Parliament, Report WD 7 – 3000 – 036/11, http://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.docx.

19 ECJ, C-301/06, § 83.

20 Advocate General, C-301/06, §§ 99 and 100.

Apart from law enforcement agencies accessing communications data, we can see individuals and businesses demanding and often getting access to the confidential communications data retained under the Data Retention Directive. In Sweden, a case has been referred to the European Court of Justice after Bonnier Audio, a copyright holder, requested an Internet Service Provider to disclose retained telecommunications data.[21] The copyright industry also participated in the procedure before the German Constitutional Court.[22] Function creep, the use of communications data for other purposes than those defined in the Directive, is thus increasingly becoming a reality. Experience has shown that the only way to effectively prevent function creep is to prevent the collection of personal information in the first place.

4.4. Scope of data retention and categories of data covered (Articles 1(2), 3(2) and 5)

Anonymisation services do not come under the Directive as they do not provide Internet access. In view of the current introduction of IPv6 technology, this is becoming ever more important. Requiring such services to retain data would be without significant value for law enforcement as non-European VPN services could still easily be used to avoid detection.

4.5. Periods of retention (Article 6 and Article 12)

The patchwork of retention periods demonstrates the failure to harmonise national data retention schemes. Some countries retain data for four times longer than others. The German Constitutional Court has held that a retention period of six months is at the upper limit of what could be considered legal, while the Romanian Constitutional Court has ruled the principle of blanket and indiscriminate communications data retention illegal no matter how long the information is kept.

4.6. Data protection and data security and supervisory authorities (Articles 7 and 9)

The Article 29 Data Protection Working Party has stressed that risks of breaches of confidentiality are inherent in the storage of any traffic data. Only erased data is safe data. That is why the ePrivacy Directive 2002/58/EC established the principle that traffic data must be deleted as soon as no longer needed for the purpose of the transmission of a communication.

After a joint inquiry carried out by national data protection authorities, the Article 29 Data Protection Working Party concluded that "the obligation to retain all telecom and internet traffic data resulting from the directive is not applied correctly in the EU member states. Most importantly, service providers were found to retain and hand over data in ways contrary to the provisions of the directive. The provisions of the Data Retention Directive are not respected".[23]

In many Member States, data security and supervision is inadequate. These Member States are in breach of Article 7 of the Data Retention Directive, which sets out some data security standards.

The German Constitutional Court has ruled data safety requirements that corresponded to those mandated by the Directive to be insufficient and in violation of fundamental rights. The Court criticised the fact that "the persons with a duty of storage are neither required in a manner that can be enforced to use the instruments suggested by the experts in the present proceedings to guarantee data security (separate storage, asymmetric encryption, the four-eyes principle in conjunction with

---

21 ECJ, C-461/10.

22 BVerfG, 1 BvR 256/08, §§ 173, 174.

23 Article 29 Data Protection Working Party, press release of 14 July 2010, http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf.

advanced authentication procedures for access to the keys, audit-proof recording of access and deletion), nor is a comparable level of security otherwise guaranteed."[24]

4.7. Statistics (Article 10)

The Article 29 Data Protection Working Party has pointed out that "the lack of available sensible statistics hinders the assessment of whether the directive has achieved its objectives."[25] As the Commission cannot rely on the statistics provided by Member States, its conclusion that "EU rules on data retention remain necessary as a tool for law enforcement, the protection of victims and the criminal justice systems" is a political rather than an evidence-based statement.

Qualitative data, such as statements on the types of crime that allegedly could be cleared are not statistics in the sense of Article 10 of the Directive. We can even see that Member States are unable to provide relevant statements on the usefulness of data retention: nine out of ten court rulings the Dutch Ministry of Justice submitted to the Commission relate to crimes that are committed long before the date the Directive was implemented in the Dutch Telecommunications Act.[26]

4.8. Transposition in the EEA countries

According to the Commission, data retention legislation is in place in Iceland, Liechtenstein and Norway.

4.9. Decisions of Constitutional Courts in transposing laws

Since the Data Retention Directive became effective in 2006, implementation laws have repeatedly been challenged before Constitutional Courts in several Member States. We remain concerned that the analysis of these rulings by the Commission does not fully cover all fundamental rights aspects. Constitutional Courts have either rejected the principle of blanket and indiscriminate telecommunications data retention out of hand (in Romania) or have firmly rejected national implementation laws (in Germany, Cyprus, Bulgaria and very recently in the Czech Republic). Furthermore, there are cases pending in Hungary and Ireland, the latter aiming at a referral to the European Court of Justice on the legality of the principle of data retention.

<u>The Romanian Constitutional Court ruling:</u>

In 2009, the Romanian Constitutional Court ruled that data retention fundamentally breaches Article 8 of the European Convention on Human Rights.[27] The Court argued that the "continuous limitation of privacy" that comes with blanket communications data retention "makes the essence of the right disappear." Data retention "equally addresses all the law subjects, regardless of whether they have committed 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 users of electronic communication services or public communication networks, so it cannot be

[24] BVerfG, press release of 2 March 2010, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html.

[25] Article 29 Data Protection Working Party, press release of 14 July 2010, http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf.

[26] The Dutch submission is available at the conference website: http://www.dataretention2010.net/docs.jsp.

[27] 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.

considered to be in agreement with the provisions in the Constitution and the Convention for the Protection of Human Rights and Fundamental Freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression." Making reference to case-law of the European Court of Human Rights, the Romanian Constitutional Court did not only question the compatibility of blanket retention with Article 8 of the European Convention on Human Rights, it definitively ruled that it is incompatible.

The German Constitutional Court ruling:

In 2010, the Federal Constitutional Court of Germany annulled the German data retention provisions for violating the fundamental right to secrecy of telecommunications.[28] The Court considered that blanket retention "constitutes a particularly serious encroachment with an effect broader than anything in the legal system to date. Blanket retention is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas." It is "part of the constitutional identity of the Federal Republic of Germany that the citizens' enjoyment of freedom may not be totally recorded and registered." Although the Court considered that blanket data retention did not per se breach the German constitution, it did not assess its compatibility with the European Convention on Human Rights or with the EU Charter of Fundamental Rights. The Court pointed out though that surveillance measures may not exceed an absolute overall constitutional threshold that exists for the collection of personal data by governments, and that telecommunications data retention would bring the surveillance situation in Germany very close to this barrier. Future surveillance measures may therefore be found unconstitutional not for being disproportionate in themselves, but for exceeding this absolute overall surveillance barrier. Therefore, maintaining blanket and superfluous data retention jeopardises the constitutionality of more effective and targeted future investigation measures.

The Czech Republic Constitutional Court ruling:

In 2011, the Constitutional Court of the Czech Republic annulled the Czech data retention requirements for violating the rule of law as well as the rights to data protection and informational self-determination.[29] In the reasons given for the judgement, the Constitutional Court expressed fundamental doubts as to "whether, having regard to the intensity of the interference and the myriad of private sector users of electronic communications, blanket retention of traffic and location data of almost all electronic communications is necessary and appropriate". Referring to crime statistics, the Court pointed out that "blanket retention of traffic and location data had little effect on reducing the number of serious crimes committed".

5. The role of retained data in criminal justice and law enforcement

The Commission tries to justify blanket and indiscriminate telecommunications data retention by claiming it necessary for prosecuting serious crime. As evidence for this claim the Commission cites statistics and examples provided by Member States concerning access to and subsequent use of retained communications data for purposes such as convictions for criminal offences. Without data retention, the Commission claims, such cases "might" not have been solved.

---

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

[29] Constitutional Court of the Czech Republic, decision of 31 March 2011, http://www.concourt.cz/clanek/GetFile?id=5075.

The Commission fails to realise that law enforcement interests cannot justify the Directive for the simple reason that its purpose is not facilitating law enforcement. According to the settled case-law of the EU Court of Justice, interferences with fundamental rights caused by an EU measure needs to be justified by the "objectives pursued by the measure chosen."[30] The predominant objective of the Data Retention Directive is ensuring the functioning of the internal market (Articles 114 and 26 TFEU).[31] The EU has no competence to legislate in the area of law enforcement, except where specifically police co-operation, judicial co-operation or the approximation of criminal law is concerned, which is not the case with data retention.[32] If the EU relies on internal market objectives for establishing its competence, it cannot rely on a completely different purpose (facilitating law enforcement) for establishing conformity with fundamental rights. If the proper functioning of the internal market is the "predominant" purpose of the Directive, the interference with fundamental rights that comes with it cannot be "predominantly" justified with a completely different purpose which the EU may not legally pursue on the basis of Article 114 TFEU.

Furthermore, even if law enforcement purposes were to be considered, the Commission has failed to prove the necessity of blanket and indiscriminate telecommunications data retention for that purpose (see section 5.3).

5.1. Volume of retained data accessed by competent national authorities

(no comment)

5.2. Age of retained data accessed

(no comment)

5.3. Cross-border requests for retained data

During the preparation of the Directive, one of the arguments used was that mutual legal assistance rules that create a legal framework for accessing data in other Member States can be quite slow and, therefore, data needs to be retained long enough for those processes to be undertaken. The Commission's report now reveals that, in fact, fewer than 1% of requests for retained data concern data held in another Member State. Bizarrely, the Commission seeks to explain away this inconvenient fact by saying that Member States are using domestic communications providers to obtain data regarding communications in other Member States. More surprisingly still, the legal basis for obtaining such data is so dubious that there would not be "any guarantee that access to data would be granted," if agreed legal procedures were followed.

5.4. Value of retained data in criminal investigations and prosecutions

The criterion for whether data retention is justified under the ECHR is 'strict necessity':

The detection, investigation and prosecution of serious crime is a "legitimate purpose" for interferences in the right to privacy (Article 8 of the European Convention on Human Rights). But to justify blanket and indiscriminate telecommunications data retention, the measure would need to be, *inter alia*, "necessary in a democratic society". In 2008, the Court ruled: "An interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social

30 ECJ, C-58/08, § 53; C-92/09, § 74.
31 ECJ, C-301/06, §§ 72 and 85.
32 Advocate General, C-301/06, §§ 99 and 100.

need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."[33] The European Court of Human Rights has consistently held that mere usefulness does not satisfy the test of necessity.[34] This has been reaffirmed by the European Court of Justice in the *Schecke* case.[35] The ECJ ruled that "derogations and limitations in relation to the protection of personal data must apply only in so far as is 'strictly necessary'". Strict necessity is therefore the test for judging whether data retention can be justified under the EU Charter of Fundamental Rights.

In this context, it was disturbing to see the Commission ask Member States, in a letter sent on 27 July, for data that could "adequately demonstrate that the Directive is useful".[36] In light of this request, it comes as no surprise that the data provided by Member States are not fit to meet the test of necessity. It was equally disturbing to note that the Commission made no effort to obtain data from the various Member States that have not implemented the Directive. Any serious attempt to independently review the Directive would have included these Member States in order to assess the necessity and the viability of "less restrictive alternatives". This is the test used by the European Court of Justice in the Schecke case[37] and by the European Court of Human Rights in numerous cases. If some Member States have viable measures in place that interfere less with fundamental rights but still achieve similar results, blanket retention is not necessary, and therefore illegal.

Data retention not 'strictly necessary' but superfluous for the detection, investigation and prosecution of serious crime:

The European Data Protection Supervisor has pointed out that it is "highly doubtful whether the systematic retention of communication data on such a wide scale constitutes a strictly necessary measure" and that "without such evidence, the Data Retention Directive should be withdrawn".[38]

In fact, blanket and indiscriminate telecommunications data retention has proven to be superfluous for the the detection, investigation and prosecution of serious crime. Studies prove that the communications data available without data retention are generally sufficient for effective criminal investigations. According to crime statistics, serious crime is investigated and prosecuted just as effectively with targeted investigation techniques that do not rely on blanket retention. Blanket data retention has proven to be unnecessary to law enforcement in many states across Europe, such as Austria, Belgium, Germany, Greece, Romania and Sweden. These states prosecute crime just as effectively using targeted instruments, such as the data preservation regime agreed in the Council of Europe Convention on Cybercrime.

The Commission's evaluation report does not deal with these facts and, for that reason, fails to prove that the strict criteria for justifying interferences are met. In order to establish the necessity of blanket and indiscriminate telecommunications data retention "for the purpose of the investigation, detection and prosecution of serious crime" in a scientifically valid way, the Commission would have had to examine at least the following three points:

---

33 ECtHR 4 December 2008, appl. 30562/04, (S. and Marper v. The United Kingdom), § 101.
34 ECtHR 25 March 1983, appl. 5947/72, (Silver a.o. v. The United Kingdom), § 97.
35 ECJ 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke, § 86.
36 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.
37 ECJ 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke, § 86.
38 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

1. In how many cases does the investigation, detection and prosecution of serious crime lack communications data that are available under a blanket retention scheme?
2. To the prosecution of how many serious crimes did such extra communications data that would not otherwise have been available ultimately make a positive difference?
3. Does any such benefit offset the counter-productive side effects of blanket data retention?

1) In how many cases does the investigation, detection and prosecution of serious crime lack communications data where a blanket retention scheme is absent?

A wealth of communications data is available for law enforcement purposes, even where providers are in principle obliged to erase such data once it is no longer necessary for the purpose for which it was generated (see Article 6 of directive 2002/58/EC). Law enforcement authorities can request that providers preserve communications data that is available while a communication is ongoing (e.g. Internet access). Law enforcement authorities can request access to communications data that providers retain for billing purposes (e.g. telephone records). In addition to freezing existing data (i.e. "quick freeze" as agreed in Convention on Cybercrime), law enforcement authorities can also order providers to preserve data relating to future communications of suspects.

The evidence presented by the Commission mostly concerns situations where "useful" communications data was available in Member States that have transposed the Directive. Such access statistics and examples of usefulness fail to demonstrate necessity though, because it is not shown that the data would have been lacking in the absence of a blanket retention scheme. Most of the evidence presented by the Commission is furthermore irrelevant, because it fails to identify the reason for which communications data were retained (i.e. commercial purposes, request by law enforcement authorities or blanket retention requirements), thus failing to demonstrate that the data would have been lacking in the absence of a blanket retention scheme. For example, the communications data used to investigate the Madrid bombings were available in the absence of a blanket retention scheme. The evaluation report fails to demonstrate that any benefits communications data may have for prosecuting crime depend specifically on blanket retention schemes and cannot likewise be achieved under targeted data preservation schemes. 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 on every citizen in the EU.

In order to examine in how many cases the investigation, detection and prosecution of serious crime lacks communications data, the situation in countries where no blanket retention requirements are or were in place needs to be analysed, which the Commission fails to do. An evaluation which fails to address countries which have not transposed the allegedly "necessary" Directive is, by definition, inadequate.

In Germany, data retention has been annulled by the Federal Constitutional Court. 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.[39] The German Federal Crime Agency (BKA) counted only 381 criminal investigation procedures in which traffic data was lacking in 2005[40] and 880 failed requests in

[39] 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.

[40] http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf.

2010[41]. In view of a total of about 6 million criminal investigations per year, no more than 0.01% of criminal investigation procedures were potentially affected by a lack of traffic data.[42]

Similarly, a Dutch study of 65 case files found that requests for traffic data could "nearly always" be served even in the absence of blanket data retention.[43] The cases studied were almost all solved or helped using traffic data that was available without compulsory data retention.[44]

It follows that in most cases, sufficient communications data for the investigation, detection and prosecution of serious crime is available without blanket retention.

2) To the prosecution of how many serious crimes did such extra communications data ultimately make a positive difference?

Where otherwise unavailable communications data are accessed by law enforcement authorities under a blanket retention scheme, these data often make no difference to the outcome of the criminal investigation. Often an investigation will be unsuccessful whether or not communications data are available. For example, communications data can be without benefit to an investigation where they lead to a public telephone booth, a public Internet café, a public Internet access point, a VPN "anonymising" service, an unregisered prepaid mobile telephone card or a device the user of which at the relevant time cannot be established. On the other hand, many criminal offences are successfully prosecuted in spite of the unavailability of communications data by using other evidence. The making available of more data to law enforcement agencies does therefore not in itself demonstrate that this extra data was necessary for the prosecution of serious crime. Availability is not necessity.

Law enforcement authorities in states that require the deletion of communications data often present statistics on how many requests for communications data were not served due to a lack of communications data. This evidence is irrelevant because it fails to demonstrate any influence extra data would have had on the outcome of these investigations. Likewise, the number of cases in which retained data is used and which result in criminal prosecutions does not demonstrate that blanket retention ultimately made a difference to the outcome of these cases, i.e. to the prosecution of serious crime.

An independent study commissioned by the German government found that about one third of the suspects in procedures with unsuccessful requests for communications data were still taken to court on the basis of other evidence.[45] Moreover, 72% of investigations with fully successful requests for traffic data did still not result in an indictment.[46] All in all, blanket data retention would have made a difference to only 0.002% of criminal investigations.[47] This number does not change significantly

---

41 Report of 17 September 2010, p. 6.

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

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

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

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

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

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

when taking into account that in the absence of a blanket data retention scheme, fewer requests for data are made in the first place.[48]

3. Does any such benefit offset the counter-productive side effects of blanket data retention?

It has been shown that blanket communications data retention may make a positive difference to the prosecution of a tiny fraction of criminal offences. Even so, data retention cannot even be considered "useful" for the prosecution of crime in general if its benefits in some cases are offset by counter-productive side effects on the prosecution of serious crime in other cases.

The indiscriminate retention of communications datahas counter-productive side-effects on the prosecution of serious crime, since it furthers the use of circumvention techniques and other communication channels (e.g. Internet cafés, public wireless Internet access points, anonymisation services, public telephones, unregistered mobile telephone cards, non-electronic communications channels). According to a representative poll commissioned after the implementation of the Directive in Germany, 24.6% of Germans declared that they use or intend to use public Internet cafés, 59.8% said that they use or intend to use an Internet access provider that does not indiscriminately retain communications data, and 46.4% of Germans declared that they use or intend to use Internet anonymisation technology.[49] Such avoidance behaviour can not only render retained data meaningless, but also frustrate more targeted investigation techniques that would otherwise have been available for the investigation and prosecution of serious crime.

In this context, it should be noted that this should not be considered an argument to widen the scope of the Directive: technologies will always develop faster than the law. The EU will always lose the arms race with new technologies, while creating mass surveillance measures as a collateral damage.

Overall, blanket data retention can thus be counterproductive to criminal investigations: facilitating a few, but rendering many more investigations futile.

All in all, blanket and indiscriminate telecommunications data retention has no statistically significant impact on the investigation of crime:

The evaluation report fails to assess the effectiveness of law enforcement in Member States and non-Member States that do not have a blanket retention scheme in place. Many law enforcement agencies around the world operate successfully without relying on blanket data retention. Among these states are Austria, Germany, Greece, Norway, Romania, Sweden and Canada. The absence of data retention legislation does not lead to a rise in crime in those states, 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 have any statistically significant effect on crime or crime clearance.

5.5. Technological developments and the use of prepaid SIM cards

(no comment)

6. Impact of data retention on operators and consumers

(no comment)

---

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

49 infas institute poll, http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf.

7. Implications of data retention for fundamental rights

Although the Directive has been in place for more than five years, its impact on fundamental rights has never been assessed by the Commission. In this section, EDRi analyses the impact of telecommunications data retention on the right to privacy and the protection of personal data on the basis of recent case-law of the EU Courts and several national Constitutional Courts.

7.1. The right to privacy and the protection of personal data

Blanket and indiscriminate telecommunications data retention severely restricts the right to privacy and data protection of 500 million Europeans. The Romanian Constitutional Court unequivocally ruled that data retention violates privacy and secrecy of communications, the presumption of innocence and can lead to destroying democracy on the grounds of defending it:

"The regulation of a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear by removing the safeguards regarding its execution. The physical and legal persons, mass users of the public electronic communication services or networks, are permanent subjects to this intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays. (...) Another aspect that leads to the unjustified restrain of the privacy right of a person is the one according to which law 298/2008 [the Romanian transposition law of the Directive] has as effect the identification not only of a person that sends a message, an information through any communication mean, but, as this results from Art.4, also on the receiver of that information. The called person is thus exposed to the retention of the data connected to its private life, irrespective of his own act or a manifestation of will but only based on the behaviour of another person – of the caller- whose actions he can't censure to protect himself against bad faith or intent of blackmail, harassment etc. Even though he is a passive subject in the intercommunication relationship, the called person can become, without his will, suspect from the point of view of the state authorities that carry out the criminal investigation. (...) This operation 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. (…)As the ECHR has remarked in the case Klass and others vs Germany, 1978, taking surveillance measures without adequate and sufficient safeguards can lead to 'destroying democracy on the ground of defending it'."[50]

The German Constitutional Court analyses that data retention has an unparalleled impact on fundamental rights:

"[data retention] constitutes a particularly serious encroachment with an effect broader than anything in the legal system to date. Blanket retention is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas."[51]

In the ECHR Marper and ECJ Schecke cases, the Courts deemed cases of blanket and indiscriminate processing of personal data to bea violation of our fundamental rights and freedoms.[52] We are concerned that the Commission's understanding of European fundamental rights jurisprudence is flawed. In its S. and Marper v. The United Kingdom judgement, the European Court of Human Rights ruled against the UK not on the basis of inadequate safeguards or due to retention periods, as the Commission has claimed. Instead, the Court found a violation of Article 8 ECHR in the fact that personal data of persons not convicted of offences were being retained indiscriminately, as is the case with Directive 2006/24:

50 http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

51 BVerfG, 1 BvR 256/08 vom 2.3.2010, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

52 ECtHR 4 December 2008, appl. 30562/04, (S. and Marper v. The United Kingdom), § 121. ECJ 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke, § 86.

"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."[53]

Furthermore, the Commission has frequently downplayed the significance of the recent ground-breaking Schecke ruling by the European Court of Justice. The ECJ annulled an EU regulation requiring the blanket publication of personal data for being disproportionate, arguing that alternative, targeted measures were available "which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life". In the same ruling, the ECJ stated that derogations and limitations in relation to the protection of personal data must apply only in so far as is "strictly necessary".[54]

In 2010, the average European had his/her traffic and location data logged in a telecommunications database once every six minutes. According to official Danish statistics, every citizen is logged 225 times a day.[55] With a blanket and indiscriminate telecommunications data retention regime in place, sensitive information about social contacts (including business contacts), movements and the private lives (e.g. contacts with physicians, lawyers, workers councils, psychologists, helplines, etc.) of 500 million Europeans is collected in the absence of any suspicion.

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 bank data, remote computer searches or PNR retention.[56] A 2008 Eurobarometer poll found that a large majority of 69-81% of EU citizens rejected the idea of "monitoring" the Internet use or phone calls of non-suspects even in light of the fight against international terrorism.[57] The European Federation of Journalists strongly opposes data retention due to the damage done to the secrecy of communications and the freedom of the press.[58]

In Germany, a study showed that, as a result of data retention, half of Germans would not contact marriage counsellors and psychotherapists through telephone or e-mail. [59]

According to the European Data Protection Supervisor, the blanket and indiscriminate bulk recording of telecommunications data of all 500 million Europeans, imposed by the Data Retention Directive, is "the most privacy invasive instrument ever adopted by the EU".[60]

7.2. Criticisms of the principle of data retention

---

53 ECtHR 4 December 2008, appl. 30562/04, (S. and Marper v. The United Kingdom), § 119 & § 125.

54 ECJ 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke, § 86.

55 CEPOS, Logningsbekendtgørelsen bør suspenderes med hendblik på retsikkershedsmæssig revidering, p. 4, 20 July 2010, based on official figures for 2008 from the Danish Ministry of Justice, http://www.cepos.dk/publikationer/analyser-notater/analysesingle/artikel/afvikling-af-efterloen-og-forhoejelse-af-folkepensionsalder-til-67-aar-vil-oege-beskaeftigelsen-med-1370/.

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

57 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%).

58 European Journalists Warn EU Home Affairs Chief that European Data Law Threatens Freedom, 1 October 2010, http://europe.ifj.org/fr/articles/european-journalists-warn-eu-home-affairs-chief-that-european-data-law-threatens-freedom.

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

60 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

For all of these reasons and many more, 106 organisations from across Europe, not only civil liberties organisations, but also associations of journalists, lawyers, healthcare professionals, trades unions, consumer organisations, health hotlines and telecoms associations have joined forces in requesting an end to data retention in a letter sent to Commission Malmström on 22 June 2010.[61] In a keynote presentation at the "Taking on the Data Retention Directive" conference, organised by the European Commission on 3 December 2010, European Digital Rights again called for a repeal of the Directive.[62]

The booklet on abuse cases related to data retention, titled "There is no secure data" and prepared by the German Working Group on Data Retention, describes recurring unlawful uses and disclosures of telecommunications data:[63]

- German telecommunications giant Deutsche Telekom illegally used telecommunications traffic and location data to spy on about 60 individuals including critical journalists, managers and union leaders in order to try to find leaks. The company used its own data pool as well as that of a domestic competitor and of a foreign company.
- In Poland retained telecommunications traffic and subscriber data was used in 2005-2007 by two major intelligence agencies to illegally disclose journalistic sources without any judicial control.[64]

Meanwhile, in its Implementation Report, the Commission states that no breaches of privacy have taken places.

The Article 29 Group has stressed that risks of breaches of confidentiality are inherent in the storage of any traffic data.[65] Only erased data is safe data. That is why the ePrivacy directive 2002/58/EC established the principle that traffic data must be deleted as soon as no longer needed for the purpose for which it was generated.

7.3. Calls for stronger data security and data protection rules

It is important to realise that civil society is not criticising the Directive mainly for a lack of harmonised safeguards, but rather for the lack of necessity and the inherent lack ofproportionality of any kind of blanket communications data retention.

7.4. The upcoming European Court of Justice ruling – what to expect?

In 2010, the Irish High Court ruled in favour of a request to challenge the Data Retention Directive at the EU Court of Justice.[66] The Court considered 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

61 http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf.

62 https://www.bof.nl/live/wp-content/uploads/What_the_European_Commission_owes_500_million_Europeans_EDRi_Bits_of_Freedom_presentation_Data_Retention_Conference_031210final1.pdf.

63 http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

64 These are far from the only examples – see :"Garda accused of bugging her ex-boyfriend" http://www.tjmcintyre.com/2011/02/judges-report-reveals-allegations-that.html , Private security agency got list of phone communication of top-manager (in Czech) http://zpravy.idnes.cz/abl-sledovala-vlivneho-manazera-cez-ziskala-i-vypisy-jeho-telefonatu-1jh-/domaci.asp?c=A110413_215758_domaci_vel

65 Article 29 Data Protection Working Party, press release of 14 July 2010, http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf.

66 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.

it must be justified and generally should be targeted". The Court ruled that EDRi member Digital Rights Ireland had the right to contest "whether the impugned provisions violate citizens' rights to privacy and communications" under the EU treaties, the European Convention on Human Rights and the EU Charter of Fundamental Rights. The referral to the EU Court of Justice is expected to be made within the next few months.

The EU Court of Justice can be expected to annul the Data Retention Directive, having regard to the jurisprudence of the European Court of Human Rights. The Grand Chamber of the latter Court found in 2008 that the long-term blanket retention of biometrics on people who were suspected of a crime violated 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. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data".[67]

This assessment of the collection of identification data on 5 million citizens[68] must, a fortiori, apply to the much larger collection of information on the daily communications of 500 million citizens throughout the EU. The Court's finding did not rely on retention periods, but on the fact that personal data of persons not convicted of any offence were being retained indiscriminately, as is the case with Directive 2006/24/EC.

Furthermore, the EU Court of Justice will consider that the purpose of the Directive is fundamentally different from the purpose of national data retention laws that have been scrutinised by national Constitutional Courts so far. It is settled case-law that the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued by the EU legislation.[69] While national data retention laws have the objective of facilitating the prosecution of crime, the Directive has the "objective of safeguarding the proper functioning of the internal market".[70] It is in the name of the internal market that the Directive requires even those Member States to implement blanket and indiscriminate telecommunications data retention whose governments, parliaments or constitutional courts do not consider such measure necessary and proportionate for the detection, investigation and prosecution of serious crime. Insofar as the Directive obliges all Member States to enact blanket retention laws in the name of market harmonisation, the EU cannot primarily rely on the entirely different objective of facilitating law enforcement, which it may not legally pursue under the Directive's legal basis (Article 114 TFEU), for justification.

It is clearly disproportionate for the EU to require all Member States to have confidential communications data retained indiscriminately, merely to prevent competitive (dis)advantages that might exist in a "patchwork" situation where some Member States require providers to retain data and others require deletion. Such a far-reaching interference with the rights protected by Article 8 of

---

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

68 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.

69 ECJ, C-92/09, § 74.

70 ECJ, C-301/06, §§ 72 and 85.

the European Convention on Human Rights cannot credibly be justified and considered proportionate on the basis of justifications and objectives which are essentially economic (removing barriers to the internal market and distortion of competition). The interest in the better functioning of the internal market cannot be considered of such importance that it balances or even outweighs the negative consequences of the unsurpassed interference in privacy caused by the Directive.

It is untenable for the European Commission to be negotiating ratification of the European Convention on Human Rights and simultaneously taking Member States to court for failing to implement a Directive which they patently do not consider to be "necessary". When Constitutional Courts of Member States have ruled a particular piece of legislation to be not "necessary in a democratic society", it is profoundly dangerous for the European Commission to take legal action to force the adoption of such legislation. Dangerous for fundamental rights, but also dangerous for the credibility of the European Union itself.

In 2010, the EU Court of Justice annulled EU legislation requiring blanket processing of personal data (publication on the Internet) for disproportionately interfering with the fundamental right to privacy, arguing that alternative, targeted measures were available "which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life".[71] It has been shown that in the case of Directive 2006/24/EC, measures other than imposing blanket retention on all Member States are available which would be consistent with the Directive's objective of safeguarding the proper functioning of the internal market while at the same time causing incomparably less interference with the citizen's right to respect for their private life.

8. Conclusions and recommendations

More than five years after the Data Retention Directive was adopted, both the evaluation report of the European Commission and the shadow report of European Digital Rights show that the Directive has failed on every level. It has failed to respect the fundamental rights of European citizens, it has failed to harmonise the single market and has proven to be unnecessary to fight serious crime.

Data retention: an unprecedented violation of the fundamental rights of all 500 million EU citizens

In the past five years, the Data Retention Directive has proven to be an unnecessary and unprecedented violation of the fundamental rights of all 500 million Europeans. According to the European Data Protection Supervisor, the Directive constitutes "the most privacy invasive instrument ever adopted by the EU".[72] It is also possibly the most highly controversial European surveillance instrument and has provoked protest throughout Europe.[73] Since the Data Retention Directive has came in effect in early 2006, several Constitutional Courts have either rejected the principle of blanket and indiscriminate telecommunications data retention out of hand or have firmly rejected national implementation laws.

Data retention: unnecessary to fight serious crime

[71] ECJ, C-92/09 and C-93/09, § 81.

[72] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

[73] Civil society calls for an end to blanket data retention, 106 organisations from all over Europe, 22 June 2010, http://www.vorratsdatenspeicherung.de/content/view/363/158/lang,en/.

The burden of proof in order to justify the massive interference with fundamental rights that comes with blanket telecommunications data retention lies with the Commission. From its evaluation report, it becomes clear that the statistics provided by the Member States do not prove the necessity of data retention. Remarkably, many Member States were unable to provide any relevant statistics to the Commission at all. Those that did indicated that the vast majority of data used by law enforcement authorities would be available if the Directive did not exist at all. Sound analysis of independent statistics must point to the fact that indiscriminate data retention is superfluous to the detection, investigation and prosecution of serious crime.

Many law enforcement agencies in the EU and around the world operate successfully without relying on blanket data retention. The absence of data retention legislation does not lead to a rise in crime in those states, nor to a decrease in crime clearance rates, not even in regard to Internet crime. Nor did the coming into force of data retention legislation have any statistically significant effect on crime or crime clearance.

Harmonisation of internal market failed dramatically

Instead of harmonising the EU internal market, the Data Retention Directive has created a patchwork of national blanket retention legislation, larger than would have existed without the Directive. Some countries retain data for four times longer than others, some reimburse the capital investment of telecoms companies, others pay for retrieval of data, some pay for both while some pay for nothing at all.

Flawed legal basis

The Data Retention Directive is based on article 114 (1) TFEU which allows the EU to approximate national laws "with the aim of establishing or ensuring the functioning of the internal market". By requiring all Member States to enact blanket retention legislation, the Directive has ensued much higher "investment and operating costs" for service providers in the EU than they would have been faced with without the Directive. The Directive thus itself constitutes an "obstacle to the free movement of electronic communications services" and "gives rise to distortions in competition between undertakings operating on the electronic communications market".

Data security obligations violated by several Member States

Many Member States fail to fully respect even the insufficient data security obligations that are imposed by the Directive. Once the statutory retention period is over, some Member States do not even have a process for deleting the data and of verifying this deletion. This has contributed to the recurring unlawful uses and disclosures of telecommunications data, as set out in this report, even though the Commission seems to deny that data retention has led to concrete cases of abuse of personal data.

In conclusion: the EU should reject the principle of data retention

European citizens, and Europe's hard won credibility for defending fundamental rights, have paid dearly for this Directive, both in terms of a reduction in the right to privacy and also in the chaos and lawless treatment of personal data. What have we gained? The vast reservoirs of citizens' communications data and the security risk that are inherent in any such databases are a cost for which there is no benefit, no justification and, ultimately, no credible legal basis.

European Digital Rights urges the European Commission to reject dogmatism, reject pressure from certain Member States and to respect the Charter on Fundamental Rights by proposing amendments to the Directive that reject the principle of blanket and indiscriminate telecommunications data retention.

Annex: Joint letter of 22 June 2010 to EU Commissioners Malmström, Reding and Kroes, signed by more than 100 organisations from 23 European countries

Cecilia Malmström

European Commissioner for Home Affairs

BE-1049 Brussels

22 June 2010

Dear Commissioner,

The EU Data Retention Directive 2006/24 requires telecommunications companies to store data about all of their customers' communications. Although ostensibly to reduce barriers to the single market, the Directive was proposed as a measure aimed at facilitating criminal investigations. The Directive creates a process for recording details of who communicated with whom via various electronic communications systems. In the case of mobile phone calls and SMS messages, the respective location of the users is also recorded. In combination with other data, Internet usage is also to be made traceable.

We believe that such invasive surveillance of the entire population is unacceptable. With a data retention regime in place, sensitive information about social contacts (including business contacts), movements and the private lives (e.g. contacts with physicians, lawyers, workers councils, psychologists, helplines, etc.) of 500 million Europeans is collected in the absence of any suspicion. Telecommunications data retention undermines professional confidentiality, creating the permanent risk of data losses and data abuses and deters citizens from making confidential communications via electronic communication networks. It undermines the protection of journalistic sources and thus compromises the freedom of the press. Overall it damages preconditions of our open and democratic society. In the absence of a financial compensation scheme in most countries, the enormous costs of a telecommunications data retention regime must be borne by the thousands of affected telecommunications providers. This leads to price increases as well as the discontinuation of services, and indirectly burdens consumers.

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. These states prosecute crime just as effectively using targeted instruments, such as the data preservation regime agreed in the Council of Europe Convention on Cybercrime. There is no proof that telecommunications data retention provides for better protection against crime. On the other hand, we can see that it costs billions of Euro, puts the privacy of innocent people at risk, disrupts confidential communications and paves the way for an ever-increasing mass accumulation of information about the entire population.

Legal experts expect the European Court of Justice to follow the Constitutional Court of Romania as well as the European Court of Human Rights's Marper judgement and declare the retention of telecommunications data in the absence of any suspicion incompatible with the EU Charter of Fundamental Rights.

As representatives of the citizens, the media, professionals and industry we collectively reject the Directive on telecommunications data retention. We urge 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 as agreed in the Council of Europe's Convention on Cybercrime. In doing so, please be assured of our support.

Yours faithfully,

1. Dr. Patrick Breyer, Seckenrain 8, D-69483 Wald-Michelbach for the **Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention)**, Germany
2. Gergana Jouleva for the **Access to Information Programme**, Bulgaria
3. Terri Dowty for **Action on Rights for Children**, UK
4. Rainer Hammerschmidt for **Aktion Freiheit statt Angst e.V.**, Germany
5. Andrea Monti for **ALCEI - Electronic Frontiers Italy**, Italy
6. David Banisar for **ARTICLE 19: Global Campaign for Free Expression**, UK
7. Dr. Roland Lemye for **Association Belge des Syndicats Médicaux**, Belgium
8. Alen Nanov for the **Association for Advising, Treatment, Resocialization and Reintegration of Drug Users and Other Marginalized and Vulnerable Groups IZBOR**, Macedonia
9. Bogdan Manolea for the **Association for Technology and Internet - APTI**, Romania
10. Martine Simonis for **L'association Générale des Journalistes Professionnels de Belgique (AGJPB)**, Belgium
11. Ute Groth for **bdfj Bundesvereinigung der Fachjournalisten e.V.**, Germany
12. Ot van Daalen for **Bits of Freedom**, The Netherlands
13. Gabriele Nicolai for **Berufsverband Deutscher Psychologinnen und Psychologen e.V.**, Germany
14. Torsten Bultmann for **Bund demokratischer Wissenschaftlerinnen und Wissenschaftler e.V.**, Germany
15. Marina Jelic for **Center for Peace and Democracy Development CPDD**, Serbia
16. Sabiha Husic for **Citizens' Association Medica Zenica**, Bosnia and Herzegovina
17. Zdenko Duka for the **Croatian Journalists' Association CJA**, Croatia
18. Christian Jeitler for **Cyber Liberties Union**, Austria
19. Vagn Jelsoe for the **Danish Consumer Council**, Denmark

20. Karl Lemmen, **Deutsche AIDS-Hilfe e.V.**, Germany
21. Ulrich Janßen for **Deutsche Journalistinnen- und Journalisten-Union dju in ver.di**, Germany
22. Michael Konken for **Deutscher Journalisten-Verband**, Germany
23. Stefanie Severin for **DFJV Deutscher Fachjournalisten-Verband AG**, Germany
24. TJ McIntyre for **Digital Rights Ireland**, Ireland
25. Martina Haan for **DPV Deutscher Presse Verband – Verband für Journalisten e.V.**, Germany
26. Prof. Michael Rotert for **eco - Association of the German Internet Industry**, Germany
27. Eleni Alevritou for **EKPIZO Consumers Association the Quality of Life**, Greece
28. Ville Oksanen for **Electronic Frontier Finland**, Finland
29. Katitza Rodriguez for the **Electronic Frontier Foundation**, U.S.A.
30. Thomas Gramstad for **Electronic Frontier Norway**, Norway
31. Máté Dániel Szabó for **Eötvös Károly Institute**, Hungary
32. Andreas Krisch for **European Digital Rights**, Europe
33. Anne Margrethe Lund, **European Movement in Norway**, Norway
34. Werner Korsten for the **Evangelische Konferenz für Telefonseelsorge und Offene Tür e.V.**, Germany
35. Simona Conservas for **exgae**, Spain
36. Stefan Hügel for **FIfF - Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.**, Germany
37. padeluun for **FoeBuD e.V.**, Germany
38. Beate Ziegler for **Forum Menschenrechte**, Germany
39. Stephan Uhlmann for the **Foundation for a Free Information Infrastructure (FFII) e.V.**, Europe
40. Valentina Pellizzer for **Foundation Oneworld - platform for Southeast Europe (owpsee)**, Bosnia & Herzegovina
41. Ross Anderson for **FIPR Foundation for Information Policy Research**, UK
42. Lutz Donnerhacke for **FITUG e.V.**, Germany
43. Matthias Kirschner for **Free Software Foundation Europe FSFE**, Europe
44. Martin Grauduszus for **Freie Ärzteschaft e.V.**, Germany
45. Jürgen Wahlmann for **GameParents.de e.V.**, Germany
46. Christoph Klug for **Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)**, Germany
47. Arvind Ganesan for **Human Rights Watch**, international
48. Joyce Hes for **Humanistisch Verbond**, The Netherlands
49. Sven Lüders for **Humanistische Union e.V.**, Germany

50. Dr. Balázs Dénes for the **Hungarian Civil Liberties Union**, Hungary
51. Jo Glanville for **Index on Censorship**, UK
52. Dr. Rolf Gössner for **Internationale Liga für Menschenrechte (Berlin)**, Germany
53. Rudi Vansnick for **Internet Society Belgium**, Belgium
54. Veni Markovski for the **Internet Society Bulgaria**, Bulgaria
55. Gérard Dantec for the **Internet Society France**, France
56. Jan Willem Broekema for **Internet Society**, The Netherlands
57. Marcin Cies'lak for the **Internet Society Poland**, Poland
58. Eamonn Wallace for **IrelandOffline**, Ireland
59. Mark Kelly for the **Irish Council for Civil Liberties**, Ireland
60. Niels Elgaard Larsen for the **IT-Political Association of Denmark**, Denmark
61. Markéta Nováková for **Iuridicum Remedium**, Czech Republic
62. Milan Antonijevic for **Koalicija za slobodu pristupa informacijama (Coalition for Free Access to Information)**, Serbia
63. Elke Steven for the **Komitee für Grundrechte und Demokratie**, Germany
64. Agata Szczerbiak for **Krytyka Polityczna (Political Critic)**, Poland
65. Jérémie Zimmermann for **La Quadrature du Net**, France
66. Milan Antonijevic for **Lawyers Commitee for Human Rights YUCOM**, Serbia
67. Klaus Jetz for **Lesben- und Schwulenverband LSVD**, Germany
68. Isabella Sankey for **Liberty (the National Council for Civil Liberties)**, UK
69. Astrid Thienpont for **Liga voor Mensenrechten (Human Rights League)**, Belgium
70. Manuel Lambert for **Ligue des droits de l'Homme (Human Rights League)**, Belgium
71. Bardhyl Jashari for **Metamorphosis Foundation**, Macedonia
72. Christian Bahls for **MOGiS e.V.**, Germany
73. Dennis Grabowski for **naiin - no abuse in internet e.V.**, Germany
74. Thomas Bruning for **Nederlandse Vereniging van Journalisten**, The Netherlands
75. Harry Hummel for **Netherlands Helsinki Committee**, The Netherlands
76. Albrecht Ude for **netzwerk recherche e.V.**, Germany
77. Christine Nordmann for **Neue Richtervereinigung e.V.**, Germany
78. Phil Booth for **NO2ID**, UK
79. Jim Killock for **Open Rights Group**, UK
80. Laurence Evrard for the **Ordre des barreaux francophones et germanophone**, Belgium

81. Annelies Verstraete for the **Orde van Vlaamse Balies**, Belgium
82. Katarzyna Szymielewicz for **Panoptykon Foundation**, Poland
83. Stefan Kaminski for the **Polish Chamber of Commerce for Electronics and Telecommunications**, Poland
84. Simon Davies for **Privacy International**, UK
85. Mag. Georg Markus Kainz for **q/uintessenz**, Austria
86. Christian Rickerts for **Reporter ohne Grenzen e.V.**, Germany
87. Jean Francois Julliard for **Reporters Sans Frontières**, international
88. Carsten Gericke for **Republikanischer Anwältinnen- und Anwälteverein e.V.**, Germany
89. Walter van Holst for **ScriptumLibre Foundation/Stichting Vrijschrift.org**, The Netherlands
90. Tony Bunyan for **Statewatch**, UK
91. Janet de Jonge for **Stichting Meldpunt Misbruik ID-plicht**, The Netherlands
92. Hans van der Giessen for the board of **Stichting NBIP - Nationale Beheersorganisatie Internet Providers**, The Netherlands
93. Lars-Henrik Paarup Michelsen for **Stopp Datalagringsdirektivet**, Norway
94. Paul Jansen for **The dotindividual Foundation**, The Netherlands
95. Karin Ajaxon for **the Julia Group**, Sweden
96. Bernadette Ségol for **UNI europa**, Belgium
97. Frank Bsirske for **United Services Union (ver.di - Vereinte Dienstleistungsgewerkschaft)**, Germany
98. Dr. Carla Meyer for **Verband der Freien Lektorinnen und Lektoren VFLL e.V.**, Germany
99. Dr. Werner Weishaupt for **Verband freier Psychotherapeuten, Heilpraktiker für Psychotherapie und Psychologischer Berater e.V.**, Germany
100. Gerd Billen for **Verbraucherzentrale Bundesverband e.V.**, Germany
101. Prof. Dr. Wulf Dietrich for **Verein demokratischer Ärztinnen und Ärzte**, Germany
102. Anna Bauer for **Vereinigung Demokratischer Juristinnen und Juristen e.V.**, Germany
103. Arnout Veenman for the **Vereniging ISPConnect Nederland**, The Netherlands
104. Miek Wijnberg for **Vereniging Vrijbit**, The Netherlands
105. Daniel Jahre for **Verein Linuxwochen**, Austria
106. Claudio Agosti for the **Winston Smith Project**, Italy