

A civil society response
to the [opinion](#) of Advocate General Cruz Villalón
in cases Digital Rights Ireland et.al.
([C-293/12](#) and [C-594/12](#))
regarding the Data Retention Directive [2006/24/EC](#)



Table of contents

1. Introduction.....	1
2. Not covered by EU competence for market harmonisation.....	2
3. Illegitimate and disproportionate interference with fundamental rights.....	6
3.2.1. Does the investigation, detection and prosecution of serious crime lack communications data in the absence of a blanket retention scheme?.....	9
3.2.2. To the prosecution of how many serious crimes does such extra communications data ultimately make a positive difference?.....	11
3.2.3. Is any such benefit offset by counter-productive side effects of blanket data retention?.....	11
3.2.4. All in all, does blanket and indiscriminate telecommunications data retention have a statistically significant impact on crime or the investigation of crime?.....	12
3.2.5. Conclusions.....	18
4. No suspension of judgement.....	22
5. Conclusion.....	23

1. Introduction

The blanket and indiscriminate bulk recording of telecommunications information on all 500 million EU citizens is, according to the European Data Protection Supervisor, “the most privacy invasive instrument ever adopted by the EU”.¹ It is also possibly the most highly controversial EU surveillance instrument and is subject to protests throughout the EU. A poll of 2,176 Germans found in 2009 that 69.3% opposed blanket data retention, making it the most strongly rejected surveillance scheme of all, provoking more opposition than measures such as biometric passports, access to bank data, remote computer searches and PNR retention.² 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.³

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

3 Flash Eurobarometer, Data Protection in the European Union, February

We welcome the European Court of Justice's assessment of the “data retention experiment”'s compatibility with fundamental rights. As the Advocate General's opinion appears not to address several salient issues, we have decided to supply the following comments.

2. Not covered by EU competence for market harmonisation

→ **Blanket and indiscriminate telecommunications data retention has proven superfluous and counter-productive for removing market distortions.**

The Advocate General's opinion states:

“97. It is, in that regard, not disputed that Directive 2006/24 constitutes an appropriate means of achieving the first, formal, objective which it pursues, namely ensuring the proper functioning of the internal market.

98. It may also be accepted, having regard to the discretion of the institutions, that the harmonisation achieved by Directive 2006/24 was actually necessary for the purpose of reducing legal and technical differences between the requirements imposed on providers of electronic communications services concerning the types of data to be retained and the periods and conditions of retention.”

We believe that there is a crucial difference between the theoretical possibility that EU legislation *could* create a more level playing field for providers and the apparent assumption that the data retention directive 2006/24 specifically is an effective device in this regard. If one considers the actual impact of the directive, taking into account the European Commission's own implementation report,⁴ blanket and indiscriminate telecommunications data retention has proven superfluous and counter-productive for removing market distortions.

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”. The EU argues that differing national data retention requirements “may involve substantial investment and operating costs” for service providers⁵, “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”.⁶

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 communications data without cause, typically requiring the retention of less data for shorter periods of time than the Directive does. Another 5 Member States had legislation in place that

2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf, p. 48 (32+18+19=69%, 35+21+25=81%).

4 Communication [COM\(2011\)225](#); see also the shadow reports published by [European Digital Rights](#) and [AK Vorrat](#).

5 EU Court of Justice (ECJ), C-301/06, [§ 68](#).

6 ECJ Advocate General, C-301/06, [§ 85](#).

would have allowed them to impose data retention requirements in the future.⁷ 15 of the then 25 Member States had not enacted any data retention legislation.⁸

Today, the Directive being in force, nearly all of the Member States are requiring service providers to retain communications data without cause⁹ with national obligations varying widely as to

1. the categories of service providers affected (the Directive imposes minimum requirements only),¹⁰
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, otherwise not harmonised by the Directive),
4. the data safety requirements (not harmonised by the Directive),
5. the purposes for which retained data can be used (not harmonised by the Directive),
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 ensued much higher “investment and operating costs” for service providers in the EU than they would have been faced with without the Directive, and has resulted in a far larger patchwork of national blanket retention legislation than would have existed 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”.

From an internal market perspective, several options exist to truly 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 Cyber-crime.
2. The EU could require Member States with (optional) national retention legislation in place to fully compensate the providers affected.
3. The EU could require Member States without (optional) national retention legislation in place to impose a levy on their communications service providers, thus

⁷ 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.

⁸ Commission, [SEC\(2005\)1131](#).

⁹ Legislation transposing the directive is not in effect in Austria, Belgium (concerning Internet data), the Czech Republic, Germany, 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.

¹⁰ For example, the UK and Finland do not require small operators to retain data, arguing that “the costs outweigh the benefits”.

eliminating any competitive advantage they might have as a result of not having to retain data indiscriminately.

4. The EU could amend the Directive in such a way as to impose limits on (optional) national retention legislation only, rather than impose the concept of blanket communications data on all 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 the key instrument to prevent market distortions:

“The cost reimbursement principle will allow creating a level playing field for the electronic communication providers in the internal market.”¹¹

When the Directive was adopted, however, the one element that would have contributed to creating a more level playing field - cost reimbursement - was removed from the Directive. Yet this element is a simple and far less invasive way of preventing market distortions than trying - and failing - to establish a harmonised data retention scheme throughout the EU.

Interestingly, the Commission cites 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, there is no justification for the EU to harmonise such national legislation at all. 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.¹² If national data retention requirements result in costs of no more than 1 or 2 Euros per customer and year, they cannot seriously be claimed to appreciably distort cross-border competition.

Besides we remain unconvinced by the EU Court of Justice's decision that EU legislation mandating the retention of data for law enforcement purposes “have as their object the establishment and functioning of the internal market” within the meaning of Article 114 (1) TFEU. If it were the case that such an instrument was, in fact, permissible, it follows that the EU would be competent to harmonise all national information keeping or other requirements imposed on companies for purposes such as law enforcement, taxation, national defence and educational purposes. For example the EU could harmonise tax record keeping requirements or national standards for manufacturing police weapons, military equipment or school textbooks, all in the name of internal market harmonisation. In our opinion this greatly exceeds the intended scope of article 114 TFEU.¹³

In summary, the Directive has not only failed its purpose of creating a more level playing field for service providers but has proven to be counter-productive in this respect, creating a far more disharmonised situation than had existed before. Several alternative approaches “consistent with the objective” of removing market distortions “while at the

¹¹ [SEK\(2005\)438](#).

¹² ECJ, C-376/98, [§ 106](#); C-58/08, [§ 32](#).

¹³ The German Federal Constitutional Court has held that the government may, in principle, not confer criminal procedure or military competences on the EU except for cross-border issues: BVerfG, 2 BvE 2/08, [§ 253](#).

same time causing less interference”¹⁴ exist, other than imposing the concept of blanket communications data on all Member States and citizens.

→ If the Union 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.

The Advocate General's opinion states:

“106. ... It is necessary, from that point of view, to acknowledge that, in the context of examining the proportionality of Directive 2006/24 within the meaning of Article 5(4) TEU, there is actually room for taking into account the ultimate objective of preventing serious crime pursued by it.”

The Advocate General does not explain how purposes outside the legal basis of the Directive can be used to support the legality of the instrument in question. Law enforcement interests cannot justify the Directive because its purpose is not facilitating law enforcement.

According to the settled case-law of the EU Court of Justice, the interference with fundamental rights an EU measure ensues needs to be justified by the “objectives pursued by the measure chosen”.¹⁵ The predominant objective of the Data Retention Directive is ensuring the functioning of the internal market (Articles 114 and 26 TFEU).¹⁶ The EU has no competence 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.¹⁷ 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.

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”.¹⁸ 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 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 plainly disproportionate for the EU to require all Member States to have confidential communications data retained without cause, 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.

¹⁴ Test applied by the ECJ in case C-92/09, [§ 81](#).

¹⁵ ECJ, C-58/08, § 53; C-92/09, § 74.

¹⁶ ECJ, C-301/06, [§§ 72 and 85](#).

¹⁷ Advocate General, C-301/06, [§§ 99 and 100](#).

¹⁸ ECJ, C-301/06, [§§ 72 and 85](#).

So far, there has been no measurable damage to the single market as a result of several Member States having long refrained from enacting blanket data retention legislation. An interference with fundamental rights as far-reaching as the indiscriminate retention of the entire population's communications data cannot legitimately 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), all the more so when these objective have quite clearly not been attained, and almost certainly could not have been attained by the instrument in question. 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.

→ The Data Retention Directive goes far beyond harmonising pre-existing national data retention requirements.

The Advocate General's opinion states:

“115. It is necessary in that regard, first of all, to explain that a situation in which the European Union restricts itself to adopting legislation harmonising provisions invariably adopted by the majority of the Member States is not comparable to a situation in which the European Union decides, additionally, to make such legislation applicable generally.”

Contrary to the Advocate General's opinion, the European Union did not restrict itself to adopting legislation harmonising provisions invariably adopted by the majority of the Member States. 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 communications data without cause, typically requiring the retention of less 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.¹⁹ 15 of the then 25 Member States had not enacted any data retention legislation.²⁰

If the aim of the directive was harmonisation of existing national blanket retention regimes, there would be no need for the EU to require the introduction of new blanket retention legislation in Member States. As explained above, several alternative approaches “consistent with the objective” of removing market distortions “while at the same time causing less interference”²¹ exist, other than imposing the concept of blanket communications data on all Member States and citizens.

→ Fundamental rights do not extend the Union's competences to limiting or otherwise regulating communications data access for law enforcement purposes.

The Advocate General's opinion states:

“121. It has been stated and repeated that Directive 2006/24, as indicated in Article 4 thereof, regulates neither access to the data collected and retained nor their use, and indeed it could not in the light of the division of areas of competence

19 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.

20 Commission, [SEC\(2005\)1131](#).

21 Test applied by the ECJ in case C-92/09, [§ 81](#).

between the Member States and the European Union. However, the issue which now arises is precisely that of whether the European Union may lay down a measure such as the obligation to collect and retain, over the long term, the data at issue without at the same time regulating it with guarantees on the conditions to which access and use of those data are to be subject, at least in the form of principles.”

The Advocate General's view that blanket data retention requirements cannot be imposed without regulating data access for law enforcement purposes implies a logical need for the Union, once retention has been required, to regulate issues which are clearly outside of its competence. This goes to show, once again, that the entire data retention regime aims at facilitating law enforcement and cannot rely on market harmonisation provisions for establishing an EU competence.

Even if the Court's ruling in *Ireland v. Parliament and Council* were to be upheld, however, fundamental rights do not, in any case, establish a basis for extending the Union's competences to limiting or otherwise regulating data access for law enforcement purposes (see Article 6 TEU and Article 51 (2) of the Charter of Fundamental Rights). 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, including the limitations of such access required by the principle of proportionality. The EU Court of Justice has ruled that the Data Retention 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”.²² 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.²³ 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.

The EU Court of Justice has no jurisdiction to consider whether or not access to communications data for law enforcement purposes is in line with fundamental rights, or which requirements or guarantees need to be satisfied. The national courts and the European Court on Human Rights are competent in this area. The Member States may regulate data access for law enforcement purposes, and when doing so are obliged to respect fundamental rights as guaranteed in their national constitutions, in the European Convention on Human Rights and other applicable international instruments (but not EU law).

The Advocate General's opinion states:

“128. Similarly, it could have been expected to lay down the principle that Member States may provide for exceptions preventing access to retained data in certain exceptional circumstances or may prescribe more stringent requirements for access in situations in which access may infringe fundamental rights guaranteed by the Charter, as in the context of the right to medical confidentiality.”

It has been shown that the EU is not competent to legislate on access to retained data

²² ECJ, C-301/06, § 83.

²³ Advocate General, C-301/06, §§ 99 and 100.

by Member States for law enforcement purposes. Besides, even if one did not consider blanket and permanent communications data retention disproportionate per se, the EU must provide for exceptions from the obligation to retain data, at least for telecommunications that particularly rely on confidentiality. These might include, for example, communications with individuals, authorities and organisations active in the social or ecclesiastical fields which offer advice in situations of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staff are subject to obligations of confidentiality according to national law. Merely prohibiting government access to confidential communications data is not good enough, since it does not protect retained data from being illegally accessed or unintentionally lost.

3. Illegitimate and disproportionate interference with fundamental rights

→ **Blanket and indiscriminate telecommunications data retention has proven harmful to many sectors of society. In view of the scale of damage done to fundamental rights by data retention and the lack of evidence for a statistically significant impact on crime or the prosecution of crime, the concept of indiscriminately collecting information on the daily communications of every single citizen is disproportionate and incompatible with fundamental rights.**

The Advocate General's opinion states:

“136. Directive 2006/24 pursues a perfectly legitimate objective, that is to say, that of ensuring that the data collected and retained are available for the purpose of the investigation, detection and prosecution of serious crime, and may be regarded, given the limited powers of review that the Court may exercise in that regard, as appropriate and even, subject to the guarantees with which it should be coupled, as necessary for achieving that ultimate objective. It is those guarantees which, in particular, may justify the, certainly very long, list of categories of data to be retained, laid down in Article 5 of Directive 2006/24.”

Contrary to the Advocate General's opinion, Directive 2006/24 does not ensure that data collected and retained are available for law enforcement purposes. It is the Data Retention Directive itself that requires communications data to be retained that would not otherwise be stored (Art. 6 (1) Directive 2002/58). Whether or not those communications data are made available for law enforcement purposes is up to the Member States and is outside the scope of the Data Retention Directive and Union law. Member States are within their rights to decide not to grant any law enforcement authority access to retained communications data at all.

The Commission argues that the Directive protects (or should protect) personal data and fundamental rights by setting standards concerning purpose limitation, retention periods and procedures for access to retained data. It is true that the Directive would be a data protection instrument if it set limits on pre-existing national retention schemes and imposed safeguards only. In reality, however, the Directive allows Member States to go beyond its limits in most respects (e.g. types of data to be retained, purpose of retention) and does not address access to retained data at all.²⁴ Most importantly, in imposing a blanket and indiscriminate telecommunications data retention scheme on all Member States, the Directive does the opposite of protecting data from being processed without consent. If the purpose of the Directive truly were to protect human rights, it would ban national data retention laws or impose limits on pre-existing laws rather than itself mandating such blanket and indiscriminate telecommunications data retention.

²⁴ Recital 25 notes that “Issues of access to data retained pursuant to this Directive [...] fall outside the scope of Community law.”

3.1. Massive interference with civil liberties

→ **The fundamental rights to privacy, to the protection of personal data, to freedom of expression and to freedom of movement all need to be fully acknowledged and considered.**

The Advocate General assesses the validity of Directive 2006/24 “primarily from the perspective of interference with the right to privacy”. Concerning the freedom of expression, he argues:

“52. First of all, it is true that it must not be overlooked that the vague feeling of surveillance which implementation of Directive 2006/24 may cause is capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information and that an interference with the right guaranteed by Article 11 of the Charter therefore could well also be found to exist. It may be noted, however, that, quite apart from the fact that the Court does not have sufficient material to enable it to give a ruling in that regard, that effect would be merely a collateral consequence of interference with the right to privacy, which is the subject-matter of a very careful and detailed examination below.”

This assessment does not address the fact that blanket communications data retention makes it impossible for the average user to anonymously express or read opinions on the Internet. Since most commercial services record every user action by the users IP addresses (“clickstream logging”), the retention of IP address data under the Data Retention Directive allows authorities to identify the readers and publishers of potentially any on-line information. IP retention will also often prevent users from anonymously sending and receiving opinions via e-mail.

US courts have long held that the right to freedom of expression encompasses the right to receive and impart information and ideas anonymously.²⁵ Anonymity is often a precondition to discussing private matters and problems (e.g. self-help groups, helplines, legal advice) as well as to media research and political debate, reporting or activism. The Advocate General's opinion lacks a sufficient analysis of the severe implications of blanket data retention on the freedom of expression and information on-line.

The Advocate General's opinion states:

“53. In addition, the High Court does not provide the slightest explanation of its reasons for considering Article 21 TFEU (right of residence and movement of European citizens) and Article 41 of the Charter (right to good administration) relevant in assessing the validity of Directive 2006/24, or even the slightest indication of the impact which that directive could have on the free movement of citizens or on the principle of good administration, contrary to the requirements now laid down in Article 94 of the Rules of Procedure of the Court. Accordingly, the Court also has insufficient material to give any ruling in that regard.”

This assessment could valuably have analysed various situations in which blanket data retention restricts the freedom of movement. Some people are obliged to carry mobile telecommunications devices, for example for professional reasons (e.g. for employer, cus-

25 US Supreme Court, *Talley v. California*, 362 U.S. 60 (1960); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995); *NAACP v. Alabama ex. rel. Patterson*, 357 U.S. 449 (1958); Washington District Court, *Doe v. 2TheMart.com*, 140 F.Supp.2d 1088; see also High Court of Israel, 4447/07 of 25/03/2010, <http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.htm>, § 11; Crump, 56 Stanford Law Review (2003), <http://www.thefreelibrary.com/Data+retention%3A+privacy,+anonymity,+and+accountability+online.-a0110534145>; Larios, Rutgers Law Record, Vol. 37, p. 36, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1640133.

tomer or patient contacts) or for medical reasons (e.g. emergency buttons). Some vehicles carry built-in mobile telecommunications devices (e.g. toll systems) and this will grow, with the use of eCall systems. As mobile device users location is being recorded every time they receive a message, forced users can no longer move without being tracked. There are many situations in which people want to prevent disclosure of locations to anybody, be in for private reasons (e.g. related to health or sexuality) or for professional reasons (e.g. related to clients or negotiations). Blanket data retention limits citizens ability to move anonymously and, in certain situations, will prevent them from seeking places completely where they cannot risk being seen.

The Advocate General's opinion states:

“65. ... The issue which arises in such cases is not yet that of the guarantees relating to data processing but, at an earlier stage, that of the data as such, that is to say, the fact that it has been possible to record the circumstances of a person's private life in the form of data, data which can consequently be subject to information processing.”

This interpretation of “processing” is not in line with the one generally recognised in EU law. The collection and storage of personal data constitutes data processing (see Art. 2 (b) Data Protection Directive). Article 8 (2) of the Charter therefore provides that personal data must be collected and stored “fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”. It therefore needs to be examined whether the indiscriminate mass retention of communications data “just in case” it might be needed for a future investigation of serious crime constitutes a “specified purpose” or not. There is also a need to examine whether there is, or can be, a “legitimate basis laid down by law” for such a practice.

In summary, we criticize a deficient analysis by the Advocate General of the Charter's relevant provisions. All relevant fundamental rights (Articles 7, 8, 11 and 21 of the Charter) need to be fully analysed for compliance.

→ Blanket and indiscriminate telecommunications data retention has proven harmful to many sectors of society.

Indiscriminately and permanently capturing and storing information on the communications, locations and Internet access of all citizens is not a legitimate objective in a democratic society.

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. 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 has not been demonstrated that the ostensible legal reason (harmonisation) or actual reason (law enforcement) for the Directive has – or could – generate benefits that would render this proportionate.

Blanket retention has a major impact on consumers in that they can no longer use telecommunications in situations that legitimately require non-traceability.

- A poll²⁶ of 1,000 Germans in 2008 found that indiscriminate bulk data retention is acting as a serious deterrent to the use of telephones, mobile phones, e-mail and Internet. The survey conducted by research institute Forsa found that with communications data retention in place, one in two Germans would refrain from contacting a marriage counsellor, a psychotherapist or a drug abuse counsellor by telephone, mobile phone or e-mail if they needed their help. One in thirteen people said they had already refrained from using telephone, mobile phone or e-mail at least once because of data retention, which extrapolates to 6.5 million Germans in total. There can be no doubt that obstructing confidential access to help facilities poses a danger to the physical and mental health of people in need as well as of the people around them.
- The German Working Group on Data Retention has received ample reports on negative effects of data retention, which have been summarised in its response to the Commission's evaluation questionnaire.²⁷ The indiscriminate retention of all communications data has been shown to disrupt confidential communications in many areas, affecting victims of sexual abuse, political activists, journalists, accountants, lawyers, businessmen, psychotherapists, drugs advisers and crisis line operators.

Citizens who refuse to use traceable communications channels act rationally as there have been concrete examples of abuse of communications data:

- In 2006, 17 million sets of mobile phone subscriber data were sold by employees of T-Mobile, among them secret telephone numbers of ministers, politicians, former German heads of state, economic leaders, billionaires and church officials.²⁸
- In Ireland, a detective sergeant in the Irish police's intelligence division is being investigated over claims that she used her position to check her former lover's phone records.²⁹
- In Germany an intelligence officer was charged in 2007 with having abused his powers to spy on his wife's lover.³⁰

Although these abuse cases cannot always be directly linked to the data retention directive, it is clear that the directive removes the only truly effective way to prevent such data abuse, which is not collecting such sensitive information in the first place.

More widespread than cases of abuse are cases of communications data falsely incriminating innocent persons of offences not committed by them or not committed at all. Communications data are particularly prone to errors as it is easy to make mistakes in the process of identifying a subscriber (e.g. transposed digits, mismatching time zones) and because communications data relate to a line or an account which can be shared

26 Forsa, Opinions of citizens on data retention, 2 June 2008, http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf or <http://www.webcitation.org/5sLeT8Goi>.

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

28 Deutsche Welle, Telekom Says Data From 17 Million Customers Was Stolen, 4 October 2008, <http://www.dw-world.de/dw/article/0,,3690132,00.html>.

29 <http://www.tjmcintyre.com/2011/02/judges-report-reveals-allegations-that.html>.

30 <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.berlinonline.de%2Fberliner-zeitung%2Farchiv%2F.bin%2Fdump.fcgi%2F2007%2F0831%2Fpolitik%2F0062%2Findex.html&date=2011-03-26>.

(e.g. public wifi hotspot). Communications data have time and again resulted in innocent citizens being put under surveillance, having their houses searched, being arrested or being publicly accused of abhorrent offences they had not committed. Also location data is often used to investigate a large number of law-abiding citizens simply for having been close to a scene of crime.

Blanket and indiscriminate telecommunications data retention undermines the protection of journalistic sources and thus compromises the freedom of the press, damaging preconditions of our open and democratic society:

- In a poll of 1,489 German journalists commissioned in 2008, one in fourteen journalists reported that the awareness of all communications data being retained had at least once had a negative effect on contacts with their sources.³¹ The inability to electronically receive information through untraceable channels with blanket data retention in place affects not only the press, but all watchdogs including government authorities.
- 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.³²
- 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.³³
- In the Netherlands, retained data was used to reveal anonymous sources of a journalist that had nothing to do with a criminal investigation. Also telecommunications data of non-suspects were accessed merely because people had the same first name as the suspect.³⁴

The Article 29 Group has stressed that risks of breaches of confidentiality are inherent in the storage of any traffic data.³⁵ 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.

3.2. Lack of necessity for law enforcement

→ Blanket and indiscriminate telecommunications data retention has proven superfluous for the detection, investigation and prosecution of serious crime.

It is unclear what evidential basis on which the Advocate General bases his view that blanket data retention is “necessary for achieving that ultimate objective” of enhancing

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

32 AK Vorrat, There is no such thing as secure data, http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

33 AK Vorrat, There is no such thing as secure data, http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

34 AK Vorrat, There is no such thing as secure data, http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

35 Article 29 Data Protection Working Party, Report 01/2010 (WP 172) of 13 July 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf, p. 2.

law enforcement (§ 136).

First of all, law enforcement interests cannot justify the Directive because its purpose is not facilitating law enforcement. According to the settled case-law of the EU Court of Justice, the interference with fundamental rights an EU measure ensues needs to be justified by the “objectives pursued by the measure chosen”.³⁶ The predominant objective of the Data Retention Directive is ensuring the functioning of the internal market (Articles 114 and 26 TFEU).³⁷ The EU has no competence 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.³⁸ 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.

If law enforcement purposes were to be considered, the following points would need to be examined:

3.2.1. Does the investigation, detection and prosecution of serious crime lack communications data in the absence of a blanket retention scheme?

A wealth of communications data is available for law enforcement purposes even where providers are in principle obliged to erase such data upon the termination of each communication (see Article 6 of directive 2002/58/EC). Law enforcement authorities can request 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 providers retain for billing purposes (e.g. telephone records). Law enforcement authorities can order providers to preserve data relating to future communications of suspects.

The evidence presented by the Commission to justify blanket retention mostly concerns situations where “useful” communications data was available in Member States that have transposed the Directive. 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 irrelevant because it fails to identify the reason for which “useful” communications data was 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 2004 Madrid bombings were available in the absence of a blanket retention scheme. Even where law enforcement authorities access data specifically retained in accordance with retention obligations, the same data may have been available in the absence of such obligations. 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

³⁶ ECJ, C-58/08, § 53; C-92/09, § 74.

³⁷ ECJ, C-301/06, [§§ 72 and 85](#).

³⁸ Advocate General, C-301/06, [§§ 99 and 100](#).

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.

The European Court of Human Rights has consistently held that mere usefulness does not satisfy the test of necessity.³⁹ In a case concerning the retention of biometric data, the European Court of Human Rights criticised data such as now presented by the Commission:

“It is true, as pointed out by the applicants, that the figures do not reveal the extent to which this 'link' with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons. Nor do they demonstrate that the high number of successful matches with crime-scene stains was only made possible through indefinite retention of DNA records of all such persons. [...] Yet such matches could have been made even in the absence of the present scheme [...].”⁴⁰

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 was 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.

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.⁴¹ The German Federal Crime Agency (BKA) counted only 381 criminal investigation procedures in which traffic data was lacking in 2005⁴² and 880 unsuccessful data requests in 2010⁴³. In view of the total of about 6 million criminal investigations per year in Germany, no more than 0.01% of criminal investigation procedures were potentially affected by a lack of traffic data.⁴⁴

Similarly a Dutch study of 65 case files found that requests for traffic data could “nearly always” be served even in the absence of compulsory data retention.⁴⁵ The cases studied were almost all solved or helped using traffic data that was available without compulsory data retention.⁴⁶

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

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

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

41 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.

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

43 BKA, Report of 17 September 2010, [p. 6](#).

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

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

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

3.2.2. To the prosecution of how many serious crimes does such extra communications data ultimately make a positive difference?

Where otherwise unavailable communications data is accessed by law enforcement authorities under a blanket retention scheme, this data often makes no difference to the outcome of the criminal investigation. Often an investigation will be unsuccessful whether or not communications data is 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, a pre-paid mobile telephone card not correctly registered by the subscriber 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.⁴⁷ Moreover 72% of the investigations with fully successful requests for traffic data did still not result in an indictment.⁴⁸ All in all, blanket data retention would have made a difference to only 0.002% of criminal investigations.⁴⁹ This number does not change significantly when taking into account that in the absence of a blanket data retention scheme, less requests for data are made in the first place.⁵⁰

3.2.3. Is any such benefit offset by counter-productive side effects of blanket data retention?

It has been shown that blanket retention obligations may make a positive difference to the prosecution of a small fraction of all criminal offences. Even so, such obligations cannot be considered necessary for the prosecution of serious crime if 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 data without cause has counter-productive effects on the prosecution of serious crime in that it furthers the use of circumvention techniques and other communication channels (e.g. Internet cafés, public wire-

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

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

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

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

less Internet access points, anonymisation services, public telephones, unregistered mobile telephone cards, non-electronic communications channels). According to a representative poll after the implementation of the Directive in Germany, 24.6% of Germans declared that they use or intend to use public Internet caf  s, 59.8% said that they use or intend to use an Internet access provider that does not retain communications data without cause, and 46.4% of Germans declared that they use or intend to use Internet anonymisation technology.⁵¹

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

Also retained data is mostly used for prosecuting petty crime such as minor fraud or file sharing. By tying up law enforcement resources with the mass prosecution of petty crime, blanket retention can hamper the investigation of truly serious crime (e.g. organised crime).

3.2.4. All in all, does blanket and indiscriminate telecommunications data retention have a statistically significant impact on crime or the investigation of crime?

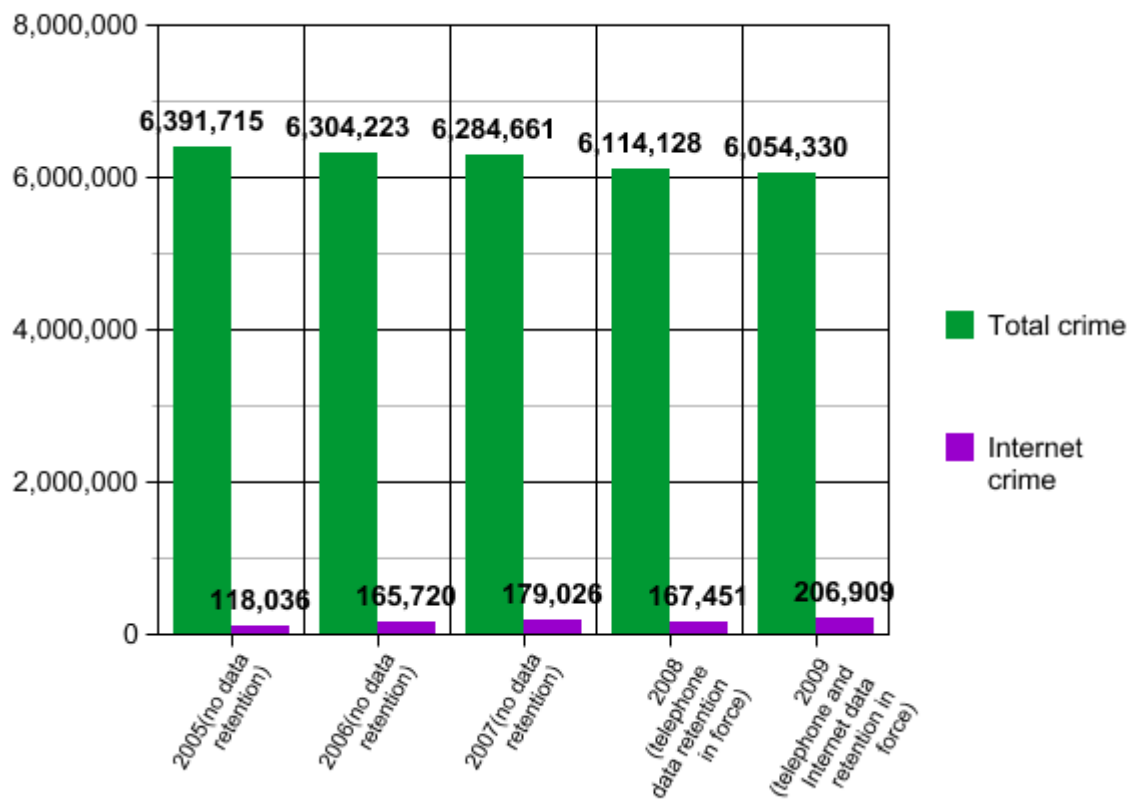
A meaningful assessment of net effectiveness of blanket retention schemes needs to look at whether, in a given country, serious crime as a whole is prosecuted more effectively under a blanket retention scheme than under a targeted investigation scheme. Has the introduction of a blanket retention scheme led to an increase in the number of condemnations, acquittals, the closure or discontinuation of cases, or the prevention of crimes? Did States operating with targeted instruments achieve a similar number of condemnations, acquittals, the closure or discontinuation of cases, and the prevention of crimes as States operating with blanket retention? 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.

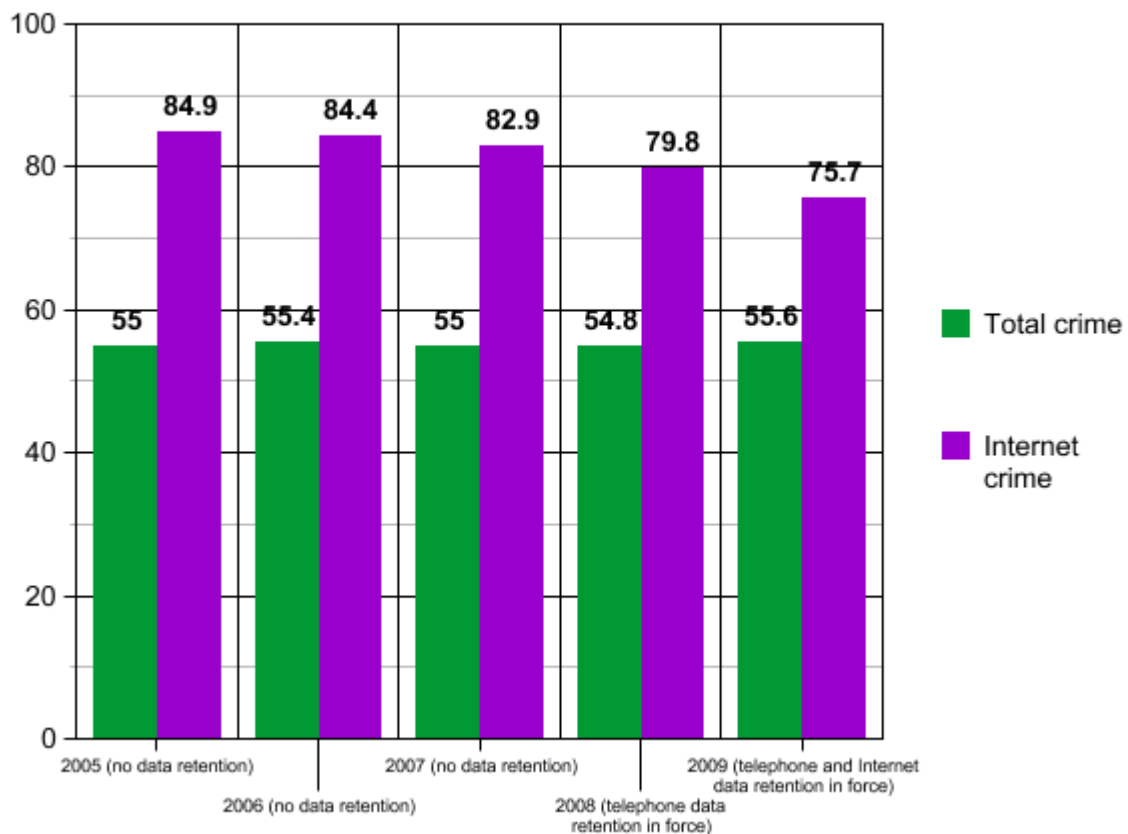
This is exemplified by statistics published by the German Federal Crime Agency (BKA):

51 infas institute poll, <http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf>.

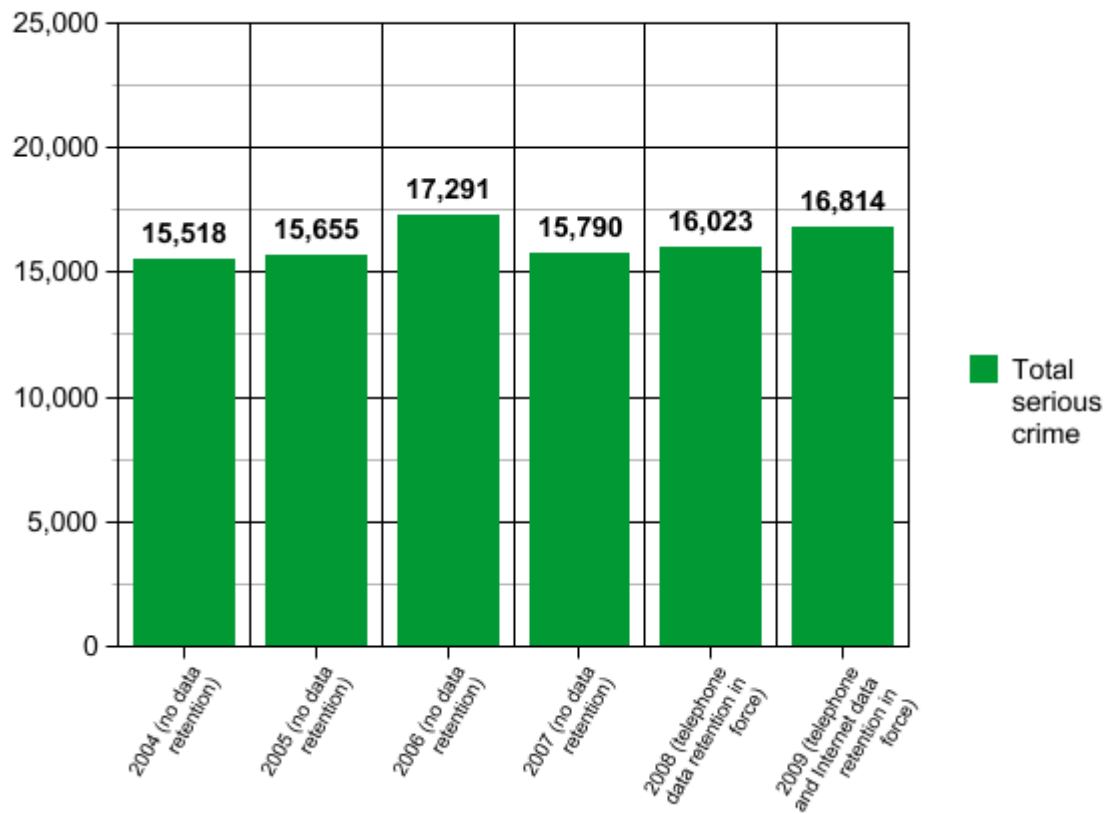
Registered crime in Germany



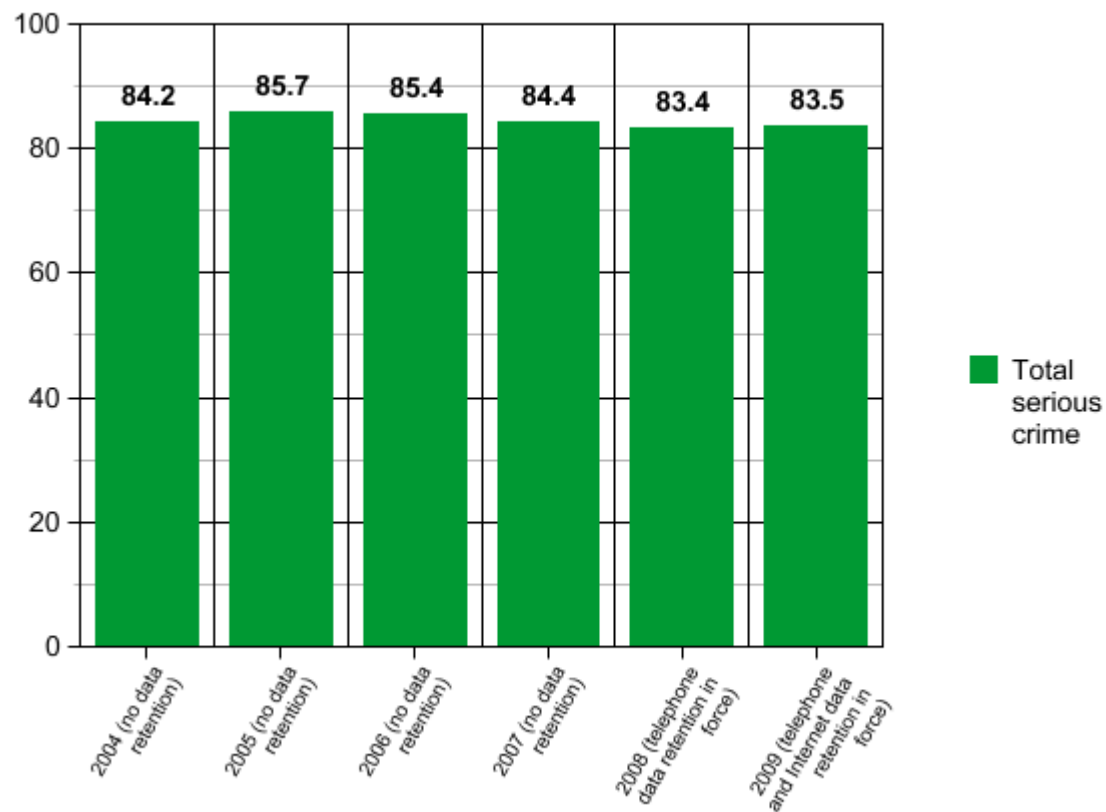
Crime clearance rate in Germany



Registered serious crime in Germany



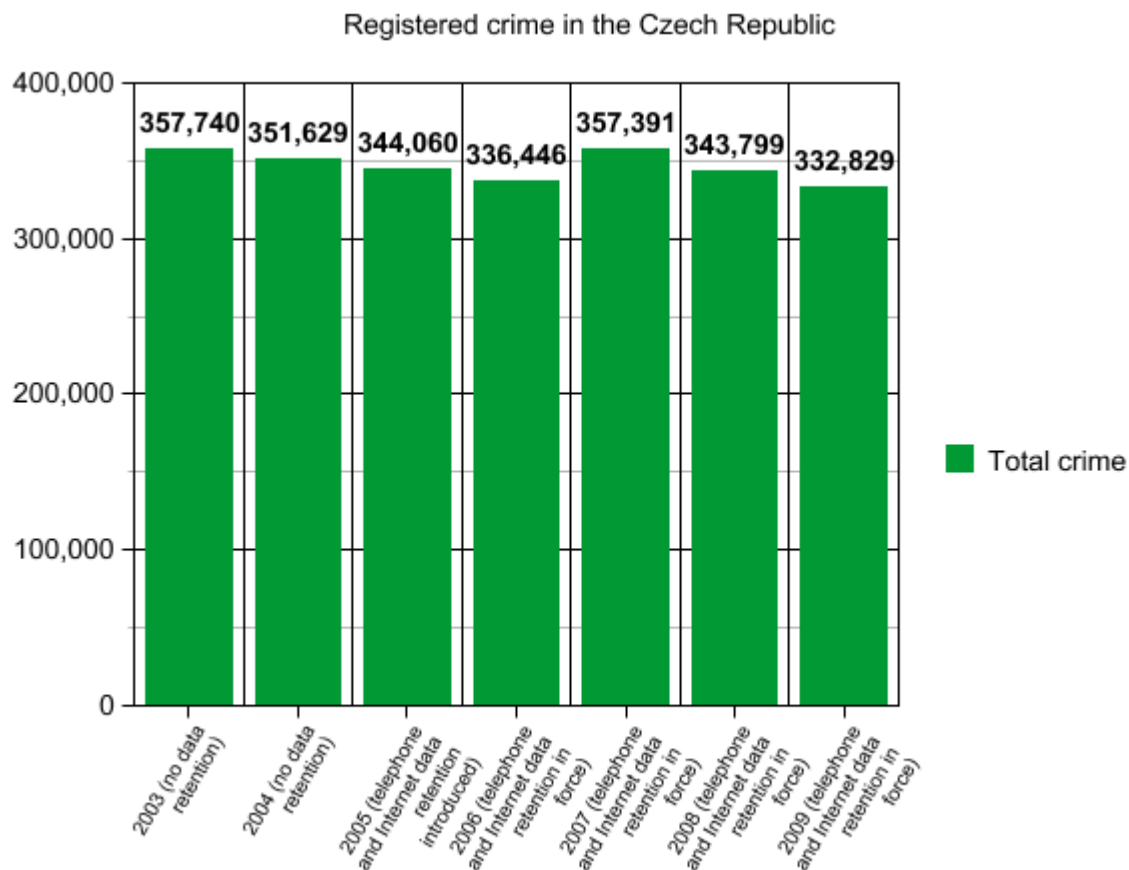
Serious crime clearance rate in Germany



With data retention in effect, more serious criminal acts (2009: 16,814) were registered by German police than before (2007: 15,790), and a smaller proportion were cleared up (2009: 83.5%) than before the introduction of blanket retention of communications data (2007: 84.4%). Likewise, after the additional retention of Internet data began in 2009, the number of registered Internet offences surged from 167,451 in 2008 to 206,909 in 2009, while the clear-up rate for Internet crime dropped (2008: 79.8%, 2009: 75.7%).⁵²

In the absence of a blanket traffic data retention regime, German law enforcement agencies have consistently cleared more than 60% of all reported Internet offences, significantly outperforming the average crime clearance rate of about 50%. The coming into force of data retention legislation did not have any statistically significant effect on crime rates or crime clearance rates. After data retention was discontinued in Germany following the Constitutional Court ruling, Internet crime continued to be cleared more often than offline crime.⁵³

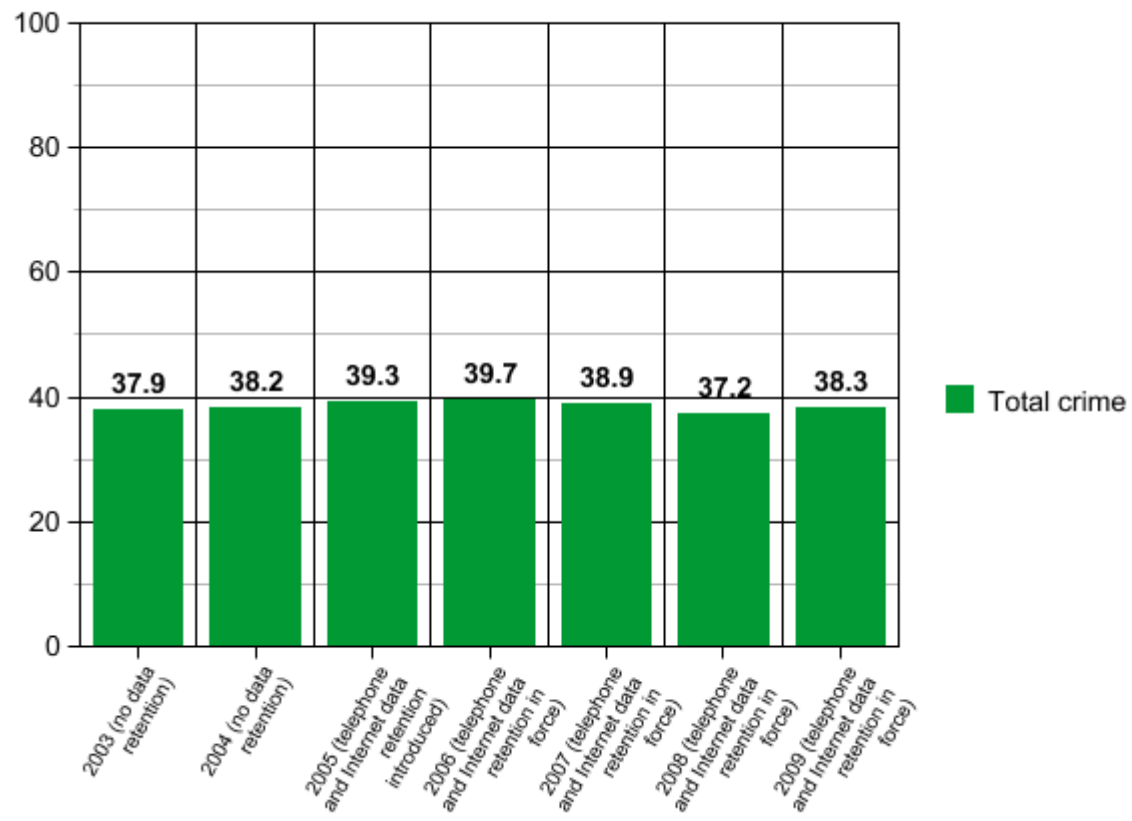
This picture is confirmed by statistics published by the Ministry of the Interior of the Czech Republic and by the Police of the Czech Republic:



⁵² Arbeitskreis Vorratsdatenspeicherung analysis, http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf.

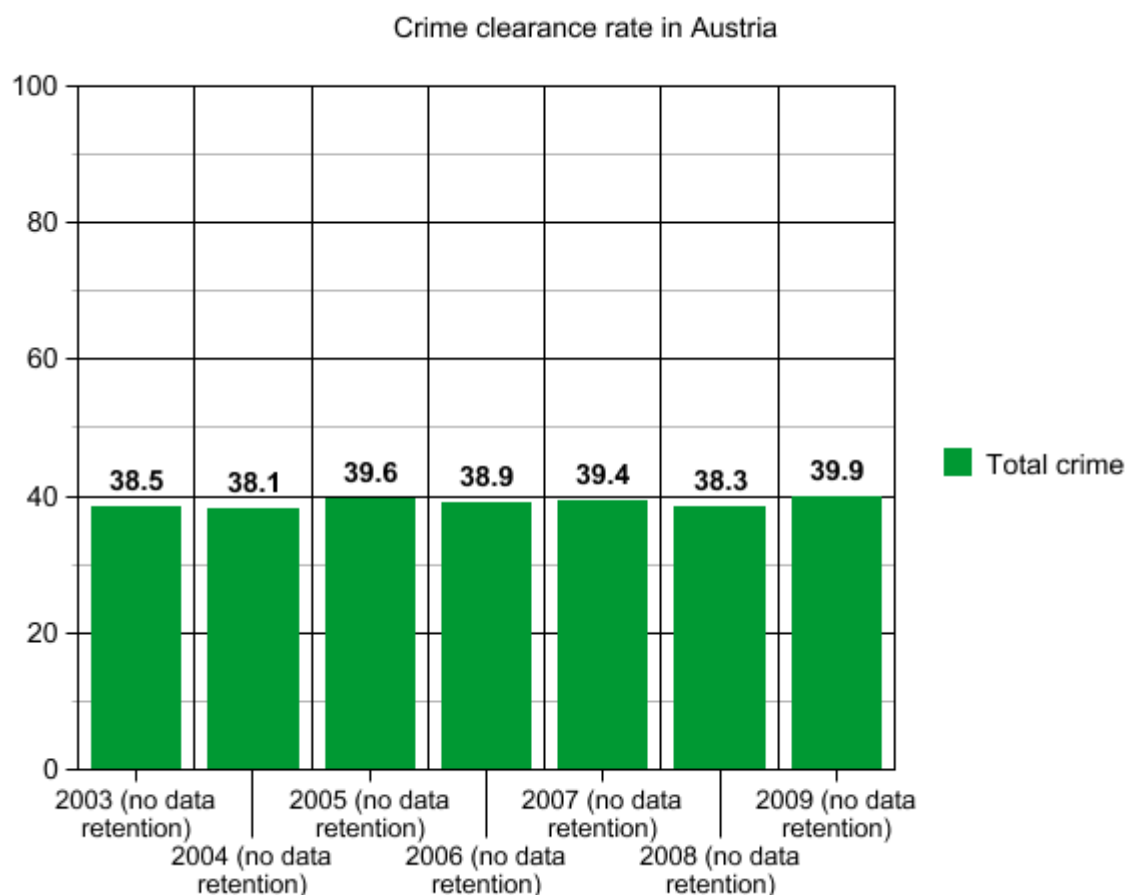
⁵³ Arbeitskreis Vorratsdatenspeicherung, <http://www.vorratsdatenspeicherung.de/content/view/435/79/lang,en/>.

Crime clearance rate in Czech Republic



Statistics published by the Austrian Ministry of the Interior show that the absence of blanket data retention legislation does not result in a rise in crime or a drop in crime clearance:





The Scientific Services of the German Parliament have analysed “The practical effects of data retention on crime clearance rates in EU Member States”. The report compared crime clearance rates throughout the EU and concluded as follows:

“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.”⁵⁴

Notwithstanding the comprehensive evidence presented above, we would like to recall that it is not the applicant's task to prove blanket data retention superfluous. It is rather the proponents of this measure who bear the onus of proof regarding the alleged necessity of blanket data retention.

3.2.5. Conclusion

Usefulness to law enforcement is not necessity. Access statistics and anecdotal evidence such as presented in the Commission's evaluation report do not demonstrate a need for blanket data retention. Successful requests for traffic data retained under directive 2006/24/EC do not prove that data would otherwise have been lacking, despite the commercial billing data stored under directive 2002/58/EC and extra data stored in compliance with specific judicial orders. Even where extra data is disclosed under data retention schemes, it often has no influence on the outcome of investigation procedures or benefits are offset by avoidance behaviour among citizens. The quota of criminal investiga-

⁵⁴ Scientific Services of the German Parliament, Report WD 7 – 3000 – 036/11, http://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.docx.

tions the outcome of which depends specifically on blanket communications data retention is exceedingly small (about 0.01%) and apparently at least offset by the counter-productive effects that blanket retention has on the 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 for years proven to be superfluous in many states across Europe, such as Austria, Belgium (for Internet data), the Czech Republic, Germany, Romania and Sweden. These states prosecuted crime just as effectively using targeted instruments, such as the data preservation regime agreed in the Council of Europe Convention on Cybercrime.

Besides, facilitating the prosecution of crime is not identical to safety. The prevalence of serious crimes is no lower in states where communications data are being retained indiscriminately. There is no indication that telecommunications data retention provides for better protection against crime.

3.3. Assessment of proportionality and relevant jurisprudence

→ Blanket and indiscriminate telecommunications data retention has proven to violate fundamental rights and unable to stand its ground against court challenges.

Contrary to the Advocate General's opinion (§ 135), the proportionality of the indiscriminate retention of data imposed by Directive 2006/24 requires a particularly detailed in-depth examination, considering the fundamental, vast consequences of blanket communications data retention on a democratic society. It is unclear to us on what basis the Advocate general makes his assertions in § 135

The Directive claims in recital 22 that it respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. However in view of the Directive's at questionable and unproven benefits and the widespread harm caused by it, systematically retaining communications data on the entire population cannot be considered a strictly necessary and proportionate measure in a democratic society:

Democratic states in Europe and beyond prosecute crime effectively without indiscriminate blanket retention. After all, offline crime can be prosecuted without lists of the people's past communications or whereabouts, too. Blanket retention appears to have no statistically significant impact on the crime clearance rate.

Enhancing the prosecution of crime is not identical to safety. There is no evidence that less crime was being committed in states that have implemented a policy of indiscriminate communications data retention than in other states. In chasing a small and unquantified number of criminal offenders who can be prosecuted on the basis of blanket retention only, the proponents of indiscriminate data retention lose sight of the fact that confidential and untraceable communications protect the lives, health and liberty of far more innocent persons, for example where counselling services can convince violent family fathers or paedophiles to take up therapy. The willingness to communicate with counselors and seek help often depends on the availability of untraceable communications channels. For example, a German helpline could convince a young man to give up plans

for a raid on his school in 2007. Had communications data been retained, the student may never have called and may have carried out his plan.

At any rate, 97% of all citizens whose communications are being recorded under blanket retention schemes in a given year are not even suspected of a criminal offence⁵⁵ and use their telephones, mobile phones and the Internet for entirely legal and legitimate purposes. Even if blanket and indiscriminate retention of communications data did contribute to the detection, investigation and prosecution of serious crime, it fails to strike a fair balance between the competing public and private interests, constituting a disproportionate interference with the EU citizens' right to respect for their private life. The EU Court of Justice should follow the Constitutional Court of Romania as well as the European Court of Human Rights's *Marper* judgement and annul the Directive for violating the EU Charter of Fundamental Rights.

In 2009, the Romanian Constitutional Court ruled that data retention per se breached Article 8 of the European Convention on Human Rights. 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 penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. Law 298/2008 applies practically to all physical and legal users of electronic communication services or public communication networks, so it cannot be considered to be in agreement with the provisions in the Constitution and 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.”⁵⁶ 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.

In 2010, the Federal Constitutional Court of Germany annulled the German data retention requirements for violating the right to secrecy of telecommunications.⁵⁷ 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”.

In 2011, the Constitutional Court of the Czech Republic annulled the Czech data retention provisions for violating the rule of law as well as the rights to data protection and informational self-determination.⁵⁸ In the reasons given for the judgement, the Constitu-

⁵⁵ In 2012, 2,094,118 of 80,521,000 inhabitants in Germany were suspected of a criminal offence: Federal Crime Agency, <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2012/pks2012Jahrbuch.templateId=raw.property=publicationFile.pdf//pks2012Jahrbuch.pdf>, p. 9.

⁵⁶ 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>.

⁵⁷ Federal Constitutional Court of Germany, decision of 2 March 2010, <http://www.bverfg.de/en/press/bvg10-011en.html>.

⁵⁸ Constitutional Court of the Czech Republic, decision of 31 March 2011,

tional Court expressed fundamental doubts “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 committed serious crimes”.

There are further complaints pending before the Hungarian Constitutional Court⁵⁹, the Irish High Court and the Austrian Constitutional Court. In 2010, the Irish High Court found that data retention had the potential to be of “importance to the whole nature of our society”. “[I]t is clear that where surveillance is undertaken it must be justified and generally should be targeted”. The Austrian Constitutional Court noted that data retention “almost exclusively affects persons who do not give cause for their data being stored” and that there was “a heightened risk of abuse”. It concluded that the interference in question “appears disproportionate, not least because of prevailing doubts as to its suitability for reaching the intended purpose”.⁶⁰

The Grand Chamber of the European Court of Human Rights found in 2008 that the retention of biometrics on mere suspects breached Article 8 of the European Convention on Human Rights:

“In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. 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.”⁶¹

This assessment of the collection of identification data on 5 million citizens⁶² 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 offences were being retained indiscriminately, as is the case with Directive 2006/24.

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 the EU act “while at the same time

<http://www.concourt.cz/clanek/GetFile?id=5075>.

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

60 Constitutional Court of Austria, decision of 28 November 2012, http://www.vfgh.gv.at/cms/vfgh-site/attachments/1/4/5/CH0007/CMS1363699922389/vorlage_vorratsdatenspeicherung_english.pdf.

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

62 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.

causing less interference with [the citizen's] right to respect for their private life”.⁶³ It has been shown that in the case of Directive 2006/24/EC, alternatives to 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 far less interference with the citizen's right to respect for their private life.

→ Blanket data retention transforms the exception from fundamental rights into an absolute rule and thus makes the essence of the rights disappear.

The Advocate General's opinion states:

“144. It should, in that regard, be pointed out in the first place that an accumulation of data at indeterminate locations in cyberspace such as the accumulation at issue, which always concerns actual and particular persons, tends, whatever its duration, to be perceived as an anomaly. In principle, such a state of ‘retention’ of data relating to the private lives of individuals, even if it remains just that, should never exist and, where it does, should exist only having regard to other requirements of society. Such a situation can only be exceptional and therefore cannot extend in time beyond the period necessary.”

It is correct that the storage of data relating to the private lives of individuals can be permitted only in exceptional circumstances in a democratic society. This is exactly why the permanent and indiscriminate retention of communications data, i.e. the routine collection of information concerning the everyday behaviour of the entire population, is manifestly disproportionate:

“The legal obligation that foresees the continuous retention of personal data transforms though the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule. The right appears as being regulated in a negative manner, its positive role losing its prevailing role. ... Therefore, 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. ... However, law 298/2008 imposes the obligation of a continuous retention of traffic data... without considering the necessity for the cessation of the limitation once the determinant cause has disappeared.”⁶⁴

In order to preserve the right to privacy and confidentiality of communications in an information society, blanket and indiscriminate telecommunications data retention requirements must be suppressed in favour of expedited preservation and targeted collection of traffic data that is needed for a specific investigation. A targeted and proportionate system as agreed in the Council of Europe's Convention on Cybercrime should be established, targeting suspects of serious crime instead of placing all 500 million EU citizens under general suspicion.

⁶³ ECJ, C-92/09 and C-93/09, § 81.

⁶⁴ Constitutional Court of Romania, decision of 8 October 2009, <http://www.asktheeu.org/de/request/21/response/153/attach/5/Wissenbach%20Annex%202.pdf>.

4. No suspension of judgement

→ **Staying the finding of invalidity of the Data Retention Directive would create a dangerous precedent and undermine the effectiveness of fundamental rights.**

The Advocate General's opinion states:

“158. It is appropriate, in those circumstances, to suspend the effects of the finding that Directive 2006/24 is invalid pending adoption by the European Union legislature of the measures necessary to remedy the invalidity found to exist, but such measures must be adopted within a reasonable period.”

We strongly disagree. It is our assertion that the finding of invalidity should not be suspended. Finding the directive invalid will allow the legislature, for the first time, to make a full and proper assessment of all options, including the option of targeted data preservation, having regard to all findings concerning the effects of data retention, as well as other current developments (i.e. international spying scandals).

The Court may consider definitive effects of an act which it has declared void only exceptionally where it is justified by overriding considerations of legal certainty. Declaring the Data Retention Directive void does not raise any issues of legal certainty. The effects of such judgement are very clear, and are the same as if the illegal Directive had not been adopted in the first place. Member States remain free to adopt legislative measures to restrict the obligation to erase communications data when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society (Art. 15 of Directive 2002/58).

By referring to “overriding considerations of legal certainty”, the Court means “the calling into question of the charging or payment of sums of money effected on the basis of that measure in respect of the period prior to the date of the judgement”.⁶⁵ In the case of *Société Régie Networks v Direction de contrôle fiscal Rhône-Alpes Bourgogne*, C-333/07, the French government feared that recovering sums for years past might put the finances and very existence of local radio stations in jeopardy and the plurality of the media could be threatened. Annuling Directive 2006/24 clearly does not call into question any transaction effected in the past.

The mere alleged “relevance and even urgency of the ultimate objectives” of an act at issue have never in the past led the Court to uphold a severe violation of fundamental rights. In the case of *European Parliament v Council*, C-317/04, the Court saw no reason to stay its decision. Nor did it in the *Schecke* case. There is no good reason why, in the case of the most grave violation of fundamental rights of all, the Court should deviate from its jurisprudence. Such deviation would create a dangerous precedent and undermine the effectiveness of our fundamental rights.

It should be noted that none of the national constitutional courts that found data retention laws in violation of fundamental rights saw a reason to stay their decision.

⁶⁵ ECJ, [C-228/99](#), § 36.

5. Conclusion

→ The EU must no longer force blanket and indiscriminate telecommunications data retention on its Member States but prohibit such laws in favour of expedited preservation and targeted collection of traffic data that is needed for a specific investigation.

Considering legal developments since 2005, the scale of the damage done to fundamental rights by the Directive, the dangers generated by the mere existence of unnecessary databases of extremely sensitive personal data, the unproven effectiveness of data retention for prosecuting serious crime and the existence of less invasive alternatives, such as targeted collection of traffic data as agreed in the Council of Europe's Convention on Cybercrime, the EU Court of Justice should prohibit national blanket data retention laws. Such an approach would target suspects of serious crime instead of placing all 500 million EU citizens under general suspicion. According to the EU Court of Justice, the EU is competent to harmonise whether or not telecommunications providers retain communications data for law enforcement purposes. The EU therefore has the power to harmonise the internal market by outlawing national blanket retention requirements. This would be broadly analogous to the harmonisation effected by EU legislation on tobacco advertising, for example.

According to its evaluation report, the Commission intends to pursue the aim of harmonisation by placing law-abiding citizens under general suspicion throughout the EU. This approach has not only failed by its own standards but is costing millions of Euros, 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. We believe that such invasive surveillance of the entire population as comes with blanket and indiscriminate telecommunications data retention is unacceptable. Representatives of the citizens, the media, professionals and industry collectively reject this policy. The EU must look beyond re-using the existing failed approach. Conclusions must be drawn from the experiences of countries that have not implemented the Directive. The EU needs to abandon the failed data retention experiment and embrace targeted, fundamental rights-compliant investigation methods. We urge the EU Court of Justice to protect our fundamental rights by finding the principle of indiscriminate communications data retention in violation with these guarantees.

Revised version of 16 March 2014

Arbeitskreis Vorratsdatenspeicherung (German Working Group on Data Retention)

The Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) is a Germany-wide organisation which campaigns against extensive surveillance in general and the blanket logging of telecommunications data in particular.

Homepage and contact details: <http://www.vorratsdatenspeicherung.de/?lang=en>