European Law Journal, Vol. 11, No. 3, May 2005, pp. 365–375.

Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR

*Patrick Breyer**

In today's information-oriented society, more and more social interaction is taking place via telecommunications networks. Private and business life is increasingly conducted via the telephone, mobile phone, and Internet. Patients consult doctors by telephone, people who are in difficulty consult the crisis line or drug-counselling websites on the Internet. Businesses transmit confidential data via telecommunications networks daily. Mobile phones and the Internet have become ever more important elements of daily life. As a result, the landslide success of these new technologies has opened up formerly unanticipated potential for surveillance, the extent of which could make both the dreams of criminalists and (former) 'Big Brother' dystopias come true. Whatever a person does using a mobile phone or the Internet can be effortlessly centrally recorded. The retention of such 'traffic data'—as opposed to the actual content of telecommunications—allows whoever has access to it to establish who has communicated with whom and at what time. In the case of mobile phones, the geographical movements of the owner can be tracked as well. The analysis of traffic data may reveal details of a person's political, financial, sexual, religious stance, or other interests. Therefore, it is fully justified to describe blanket traffic data retention as a new dimension in surveillance, as compared to traditional police powers. Data retention does not only apply in specific cases. Instead, society is being pre-emptively engineered to enable blanket recording of the population's behaviour, when using telecommunications networks.

Demands for traffic data retention have been repeatedly voiced on the basis that access to traffic data is increasingly becoming the only means by which state authorities can fulfil their tasks. There is no doubt that access to telecommunications data and its content is one of the most commonly used ways of gathering information for criminal investigations and the activities of intelligence services. Traffic data is usually the only way to identify users of telecommunications networks. Therefore, the availability of such data is often crucial to the successful investigation of crimes committed by

* Dr. Jur. (Germany). This article is a summary of the findings of the author's thesis on data retention, *Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland* [Vorratsspeicherung, traffic data retention] (Rhombos, 2005). Available at <http://retention.breyers.de>.

means of telecommunications networks. Another reason why traffic data is widely used by state authorities is that it can be stored and accessed at hardly any cost to them.

Fear of crime and the subsequent demand for security are strongly established in modern Western society and impact on political policy. Political debate on new surveillance powers usually focuses on the citizens' security. The population often welcomes the introduction or extension of such powers. Partly incited by the media, an undercurrent of insecurity and fear has established itself. However, this does not correlate to an actual increase in crime rates, and is therefore objectively unjustified. The historically founded *Rechtsstaat* (state based on the rule of law) and particularly human rights instruments, have established limits beyond which citizens are not obliged to tolerate any interference with their rights. The mere potential surveillance powers may hold as a worthy way to protect citizens, does not in itself provide a universal justification for unlimited interference, no matter how great the threats facing us may be.

From a legal point of view, human rights are decisive in determining the legality of blanket traffic data retention. The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[1] is binding not only for individual states but also for the European Union (Article 6(2) TEU). This is relevant in regard to a proposal of several EU Member States to introduce a compulsory traffic data retention and exchange scheme by means of a Council framework decision (Article 34(2)(b) TEU).[2] Because of Article 2 TEU, framework decisions must be compatible with the ECHR and are subject to review, under this aspect, by the European Court of Justice (Articles 35(1), 35(6), and 35(7) TEU). Framework decisions are not directly effective but, similarly to directives, require transposition into national law (Article 34(2)(b) TEU). Since the ECHR is first and foremost applicable to its contracting parties, national measures transposing framework decisions as well as measures carried out on the basis of such legislation, must also comply with the ECHR. Thus, the ECHR cannot be circumvented by means of a European Union framework decision.

I The Right to Respect for Private Life and Correspondence (Article 8 ECHR)

The principal provision providing the individual with protection from the processing of telecommunications traffic data is Article 8 ECHR. This article warrants, among others, the right to respect for a person's private life and correspondence. In its jurisprudence, the European Court of Human Rights has repeatedly held that the metering of traffic data without the consent of the subscriber constitutes an interference with the rights to respect for private life and correspondence.[3] This jurisprudence is based on traffic data being 'an integral element in the communications made'.[4]

---

[1] Dated 04/11/1950. Available at <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

[2] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, Council document 8958/04, dated 28/04/2004, available at <http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>.

[3] Court of Human Rights, *Malone v the United Kingdom* (1984), Publications A82, § 84; Court of Human Rights, *Valenzuela Contreras v Spain* (1998), Decisions and Reports 1998-V, § 47; Court of Human Rights, *P. G. and J. H. v. the United Kingdom* (2001), Decisions and Reports 2001-IX, § 42.

[4] Court of Human Rights, *op. cit.* note 3 *supra*.

Just as the metering of telecommunications by government officials, the state-imposed retention of traffic data by private telecommunications companies is an interference with Article 8 ECHR.[5] The fact that the state uses private companies for the execution of its retention programme does not affect this classification, given that authorities have the right to access retained traffic data at any time. Neither does the legal qualification of data retention legislation depend on whether or not telecommunications companies may access retained data for their own purposes as well. Lastly, it is an interference with Article 8 ECHR if the state grants telecommunications providers the right to voluntarily retain traffic data beyond the period necessary for their business purposes,[6] because state authorities in turn can assert the right to access such data for their own purposes.

Any interference with the rights guaranteed in Article 8 ECHR requires justification. According to Article 8(2) ECHR, any interference must be 'in accordance with the law'. According to the Court of Human Rights, this expression requires that the measure should have some basis in domestic law. It further refers to the quality of the law in question, requiring that it should be accessible to the person concerned, and formulated with sufficient precision in line with the seriousness of the interference.[7] Sufficient precision is necessary to enable the individual concerned to foresee the consequences of the law and adapt their conduct accordingly. Additionally, domestic law must provide effective legal protection against arbitrary or improper interference by public authorities.

It has been argued that traffic data retention is incompatible with the requirement of foreseeability because it fails to distinguish between different categories of people, and does not provide a citizen with an accurately foreseeable basis by which to regulate their conduct.[8] However, if a statute permits indiscriminate interference, the problem does not lie in the precision of the law. Data retention legislation allows everyone to foresee that all traffic data will be recorded and retained for a certain period of time. Provided that the relevant legislation satisfies the conditions mentioned above, data retention schemes do not violate the requirement of foreseeability. Instead, the concerns raised in relation to this question are problems of proportionality, and need to be examined as such.

The same applies to the argument that blanket retention of traffic data falls 'short of the requirements of: being authorised by the judiciary on a case-by-case basis and for a limited duration, distinguishing between categories of people who could be subject to surveillance, respecting confidentiality of protected communications (such as lawyer-client communications), and specifying the nature of the crimes or the circumstances that authorise such an interference'.[9]

---

[5] Covington & Burling, *Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights*, dated 10/10/2003, available at <http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf>, at 6.

[6] See Art 6 of the Directive 2002/58/EC on privacy and electronic communications.

[7] Court of Human Rights, *Sunday Times v the United Kingdom* (1979), Publications A30, § 49; Court of Human Rights, *Silver* et al. *v the United Kingdom* (1983), Publications A61, §§ 87 and 88; Court of Human Rights, *Lambert v. France* (1998), Decisions and Reports 1998-V, § 23.

[8] Covington & Burling, *Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights*, dated 10/10/2003, available at <http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf>, at 8 *et seq*.

[9] European Parliament resolution on the First Report on the implementation of the Data Protection Directive (95/46/EG), dated 09/03/2004, document reference P5-0104/2004, available at <http://www2.europarl.eu.int/omk/sipade2?SAME_LEVEL=1&LEVEL=5&NAV=S&LSTDOC=Y&DETAIL=&PUBREF=-//EP//TEXT+TA+P5-TA-2004-0141+0+DOC+XML+V0//EN>, § 18.

The Court of Human Rights established these requirements for surveillance undertaken on a case-by-case basis. The application of these conditions to blanket data retention schemes would effectively outlaw any such scheme. Therefore an in-depth analysis of these schemes' proportionality should be conducted before deciding whether to apply the Court of Human Rights requirements to blanket surveillance measures.

If an interference is in accordance with the law, Article 8(2) ECHR further requires the interference to be 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. Keeping in mind the importance of the human right being interfered with, such necessity for interference can be assumed only if the interference corresponds to a pressing social need, pursues a legitimate aim and is proportionate to that aim.[10] The Court of Human Rights has clearly stated that the aim pursued must be balanced against the seriousness of the interference, and that the social need must be sufficiently pressing to outweigh the human right in question.[11]

Some have interpreted the jurisprudence of the Court of Human Rights as outlawing any exploratory or general surveillance[12] not carried out on a case-by-case basis in the event of reasonable suspicion.[13] It is unclear whether the Court of Human Rights would indeed take such a stance. So far, it has not decided on the matter.[14] In its decision on the German G10 Act, the Court of Human Rights noted that the Act did not permit 'so-called exploratory or general surveillance',[15] but did not elaborate on the consequences this would entail. Therefore, this mention does not provide a sufficient basis for legal argument, instead, the compatibility of data retention with Article 8 ECHR is an issue of proportionality.

In examining the necessity of data retention, the first test is that of effectiveness. Data retention is not altogether ineffective because it can be assumed to support law enforcement in a certain number of cases. Furthermore, no less intrusive but equally effective alternatives are available.

The proportionality test finally requires the harm to civil rights to be proportionate to the aims of the legislation in question. Thus, the positive and the negative effects of the measure on individuals and society as a whole must be balanced against each other. This cannot be achieved by means of general considerations on the interests and rights in question, since it is impossible to establish an absolute order or ranking of

---

[10] Court of Human Rights, *Sunday Times v. the United Kingdom* (1979), Publications A30, § 62; Court of Human Rights, *Silver* et al. *v the United Kingdom* (1983), Publications A61, § 97; Court of Human Rights, *Foxley v the United Kingdom* (2000), available at <http://hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%2020062000e.doc>, § 43.

[11] Court of Human Rights, *Sunday Times v the United Kingdom* (1979), Publications A30, §§ 65 and 67; Court of Human Rights, *Leander v Sweden* (1987), Publications A116, § 59.

[12] Recommendation of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001/2070(COS)), dated 06/09/2001, document reference A5-0284/2001; Second Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, dated 24/10/2001, document reference A5-0374/2001, Amendment 4; Art. 29 Data Protection Working Party, Opinion 2/99, dated 03/05/1999, available at <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp18en.pdf>, at 5.

[13] R. Allitsch, 'Data Retention on the Internet', (2002) June *Computer Law Review International*, 167.

[14] European Commission, SEK(2002) 124 final, dated 05/02/2002, 3.

[15] Court of Human Rights, *Klass* et al. *v Germany* (1978), Publications A28, § 51: 'Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation'.

interests and rights. Instead, it is necessary to determine how useful the measure will actually be, and what harmful effects it will actually have.

It needs to be kept in mind that law enforcement is not an interest or a right in itself. Any other opinion would enable the state, having the power to make the laws that are to be enforced, to progressively erode human rights. Sanctions as a mere instrument of retribution for criminal acts committed in the past cannot legitimise restrictions on human rights. The same applies to other abstract aims, such as 'criminal justice' or 'the defence of innocent suspects'. Article 8(2) ECHR, while recognising the 'prevention of . . . crime' as a legitimate aim, does not mention the prosecution of crime. Therefore, the prosecution of crime can justify an interference only where it is effective in preventing crime. Criminal law is legitimate only as a means of protecting individual rights, that is, of preventing damage being inflicted upon them. The degree to which an interference with human rights is effective in furthering this aim needs to be evaluated, in order to protect civil liberties effectively. Thus, restrictions on human rights for the purpose of fighting crime cannot be accepted without examining the actual effectiveness of law enforcement.

Traffic data retention can, in principle, be useful in preventing infringements on any right. As far as cyber-crime (i.e. crime committed by means of telecommunications networks) is concerned, however, it is mostly the monetary interests of individuals that are affected. Cyber-crime hardly ever poses a threat to society as a whole, or to the physical safety of individuals.

The benefit of retaining traffic data lies mostly in the investigation of criminal acts committed in the past, whereas its effectiveness in preventing damage is marginal. An analysis of relevant empirical studies shows that strengthening law enforcement does not have any apparent effect on the decision-making process of potential offenders. The investigation and prosecution of crime has preventive effects only insofar as prison sentences prevent offenders from committing offences out of prison during their prison term, and where proceedings result in the restoration or compensation of damage suffered by victims of crime. It is not known how many cases traffic data retention would be of use in, in this regard. However, what is clear from general practical experience is that strengthening law enforcement does not have any apparent effect on crime levels.

The existence of various ways of communicating anonymously, the use of which is likely to increase as a reaction to traffic data retention, raise fundamental doubts as to the benefit of data retention. There is a range of methods for preventing either the generation of traffic data or access to it by European authorities. For example, it is easy for criminal offenders to use mobile-phone cards that have been registered in the name of another person or even bought in a country that does not require registration. Only if the world community cooperated closely would it be possible to prevent anonymous telecommunication from taking place. Realistically, however, such cooperation is not to be expected. In any case, criminal offenders cannot be expected to observe laws banning the use of anonymous telecommunications. Therefore, traffic data retention cannot stop more experienced criminals from preventing the generation of incriminating traffic data.[16]

In summary, data retention can be expected to support the protection of individual rights only in a few, and generally less important, cases. A permanent, negative effect on crime levels, even in the field of cyber-crime, is not to be expected. The potential

[16] C. Bowden, 'Closed circuit television for inside your head: Blanket traffic data retention and the emergency anti-terrorism legislation', (2002) *Computer and Telecommunications Law Review*.

use of data retention in fighting organised crime and in preventing terrorist attacks is marginal or non-existent.

In determining the proportionality of data retention, its negative effects need also to be taken into account. Generally, the seriousness of an interference with human rights is to be judged according to the preconditions of powers granted, the number and nature of individuals affected and the intensity of negative effects. In doing so, the harmful effects that are certain to happen are not the only ones that need to be taken into account. Serious risks (such as abuse of power) need to be considered as well.

Regardless of the details of data retention schemes, they gravely interfere with the rights to respect for private life and correspondence guaranteed in Article 8 ECHR. Not only specified individuals but everybody is subjected to having their telecommunications usage recorded. In many situations, people cannot reasonably avoid using telecommunications. Therefore, there is often no escape from having the details of one's telecommunications recorded, even where communications are confidential (e.g. lawyer–client communications).

Under a data retention scheme, every use of fixed-line or mobile telephones, fax, text messaging, e-mail, the Internet, and so on, is recorded as to the identity of the individuals involved, the time and place of communications, and other details. Unmonitored telecommunications would practically cease to exist. Data retention not only affects communications taking place in public or business premises but for a large part also affects communications in private homes, despite the fact that monitoring a citizen's behaviour in their home is generally permissible only in exceptional circumstances. Traffic data is not being registered anonymously or for statistical purposes, but its purpose is being directed towards enforcement measures against individuals. Therefore, the retention of traffic data can have most serious consequences for individuals, ranging from embarrassing interrogation or observation procedures, right up to life prison sentences—possibly as a result of wrong presumptions. Furthermore, access to retained traffic data is not costly for authorities, which eliminates another traditional logistical restriction on the use of surveillance powers.

As opposed to other powers granted for the collection of personal data in democratic societies, blanket data retention does not only affect data for which there is an expressed likely use in the future. Citizens are monitored purely for unsubstantiated reasons of precaution. Of the innumerable telecommunications taking place every minute, the probability of a random communication needing to be re-visited and established as fact by law enforcement is minuscule. Although powers are known in democratic societies that are not subject to reasonable suspicion, blanket retention of all telecommunications traffic data is of a new quality, even compared to those powers. In other fields, measures against non-suspects are permissible only in specific cases or situations. Data retention, on the other hand, constitutes a permanent, general recording of citizens' behaviour. The users of telecommunications services are neither responsible for creating a source of danger, nor do telecommunications take place in an unusually dangerous area.

Contrary to popular opinion, access to traffic data cannot be considered less privacy-invasive than the surveillance of the content of telecommunications. The information value and usability of traffic data is extremely high and at least equals that of telecommunications content. First, traffic data can be processed much more effectively than content data. Traffic data can be analysed automatically, combined with other data, searched for specific patterns, and sorted according to certain criteria, all of which

cannot be done with content data. Second, authorities often are, at least initially, interested in obtaining traffic data only. An interest purely in the contents of telecommunications does not occur in practice. Traffic data provides a detailed picture of the telecommunications, social environment, and movements of individuals. The information value of traffic data can, depending on the circumstances, be equal to or exceed that of communications contents. It can therefore not be said that traffic data is typically less sensitive than content data, and it is not justified to apply a lower level of legal protection to traffic data than to content data.

One of the harmful effects of data retention is an increase in the likelihood of erroneous decisions in criminal investigations and court procedures. In view of the difficulties in determining a user's identity for a given telecommunications service, at a given time, and the fact that access to traffic data often affects a multitude of individuals simultaneously, this instrument bears the specific risk of leading to erroneous incriminations or suspicions. Furthermore, retaining traffic data creates potential risks of abuse by state agencies. Traffic data can be extremely useful for political control, for example, by intelligence agencies. Experience shows that the risk of powers being abused, especially where they are exercised in secret, must not be underestimated, even in Europe. Furthermore, where the government prevents the effective protection of personal data because of its appetite for surveillance, it opens up the gates for misuse of the data by third parties. Innumerable facts about the private life of prominent members of the public could be obtained by analysing traffic data. In the event of unauthorised access to retained traffic data, politicians could be forced to resign and officials could be blackmailed. Last but not least, traffic data is useful in gathering economical intelligence by foreign states.

Where data retention takes place, citizens constantly need to fear that their communications data may at some point lead to false incrimination, or governmental or private abuse of the data. Because of this, traffic data retention endangers open communication in the whole of society. Individuals who have reasons to fear that their communications could be used against them in the future will endeavour to behave as unsuspiciously as possible or, in some cases, choose to abstain from communicating altogether. Such behaviour is detrimental to a democratic state that is based on the active and unprejudiced involvement of citizens. This chilling effect is especially harmful in cases that attract abuses of power, namely in the case of organisations and individuals who are critical of the government or even the political system. Blanket traffic data retention can ultimately lead to restricted political activity, bringing about damage to the operation of our democratic states and thus to society.

Traffic data retention also causes increased efforts in the development of countermeasures such as technologies of anonymisation. Where the state indirectly encourages anonymous communications in its pursuit of surveillance, it will ultimately damage its power to intercept telecommunications even in cases of great danger.

Neither the positive nor the negative effects of traffic data retention can be determined with certainty. This is because of the lack of empirical knowledge available on the subject at present. In such situations of uncertainty, democratically elected parliaments have a certain margin of appreciation as far as the facts in question are concerned. However, where political decisions have a significant impact on human rights, parliaments are required to make use of all information available to determine the relevant facts as well as possible, and to make a rational decision on that basis. Furthermore, for as long as the relevant facts have not been established, irreversible restrictions on human rights cannot be considered necessary in a democratic society, with an

exception being justified only if a measure is indispensable to protect important rights from grave threats.

On this basis, blanket traffic data retention, being a measure with a significant impact on human rights and civil liberties, may not be instituted before having established its effects. The immediate introduction of data retention is not indispensable for the protection of important rights from grave threats. Determining the effects of data retention is possible without actually introducing such a scheme. Since data retention merely brings about a quantitative extension of the amount of traffic data available, evaluating traditional powers of access to traffic data can provide important information on the prospective effects of data retention. Furthermore, for as long as traffic data retention schemes are operated by some EU states, their effects can be studied first hand, both by comparing national data over time, and by comparing data with states without retention schemes. Such evaluations would reveal whether traffic data retention is actually useful to agencies, in how many and which cases of crime prevention and prosecution data retention has ultimately made a difference, whether data retention is effective in fighting serious organised crime, and whether it has resulted in a decrease in crime levels or not.

Weighing the conflicting rights and interests on the basis of what present knowledge is available, demonstrates a significant disparity between the likely benefit of blanket traffic data retention and its negative effects, both on individuals and on society as a whole. Data retention is a disproportionate restriction of rights under Article 8 ECHR.[17] While it threatens to inflict great damage on society, its potential benefit appears, overall, to be little. Data retention can support the protection of individual rights only in few and generally less important cases. A permanent, negative effect on crime levels is not to be expected. On the basis of present knowledge, it would not be rational to assume otherwise. Consequently, parliaments that still enact data retention legislation exceed their margin of appreciation under Article 8 ECHR. As a result, blanket traffic data retention is incompatible with Article 8 ECHR.

Legislation that allows telecommunications providers to voluntarily retain traffic data is less intrusive on human rights than compulsory schemes if less data is retained as a result. However, voluntary schemes have important disadvantages, the most significant of which is that companies can choose not to retain traffic data. This has a detrimental effect on the potential benefit of data retention, since every serious criminal will take great care to use companies that have opted out of data retention. Therefore, all considered, voluntary data retention schemes are just as disproportionate as compulsory schemes.

---

[17] Article 29 Data Protection Working Party, Opinion 5/2002, available at: <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_en.pdf> and Opinion 9/2004, <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_en.pdf>; Covington & Burling, *Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights*, dated 10/10/2003, available at <http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf>, at 3; Recommendation of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001/2070(COS)), dated 06/09/2001, document reference A5-0284/2001; Statement of the European Data Protection Commissioners, dated 11/09/2002, <http://www.fipr.org/press/020911DataCommissioners.html>. See also European Parliament resolution on the First Report on the implementation of the Data Protection Directive (95/46/EG), dated 09/03/2004, document reference P5-0104/2004, available at: <http://www2.europarl.eu.int/omk/sipade2?SAME_LEVEL=1&LEVEL=5&NAV=S&LSTDOC=Y&DETAIL=&PUBREF=-//EP//TEXT+TA+P5-TA-2004-0141+0+DOC+XML+V0//EN>, § 18.

On the other hand, providing authorities with the power to order the logging and disclosure of traffic data in regard to specified communications (data preservation) is compatible with the ECHR, provided that the power is subject to sufficient conditions, and the cost to the telecommunications providers is borne by the government. Although the Council of Europe's Convention on Cybercrime[18] provides for such data preservation powers to be enacted, other provisions of the convention are incompatible with the ECHR—the convention provides for an extensive exchange of data among signatory states without guaranteeing that the minimum human rights standards afforded by the ECHR are maintained in states that are not party to the ECHR.

II Freedom of Expression (Article 10 ECHR)

Article 10 ECHR guarantees the right to freedom of expression, including the freedom to hold opinions, and to receive and impart information and ideas without interference by public authorities. Both facts and opinions fall within the scope of Article 10 ECHR.[19] It is irrelevant which technical means are used to exercise the rights under Article 8 ECHR.[20] Thus, the use of telecommunications networks is covered by the provision. It is also without relevance whether communications are of a private or a public nature and whether they are individual or mass communications.[21] Although the protection afforded by Article 10 ECHR is partly identical to that of Article 8 ECHR, both rights have different purposes and are therefore to be applied independently of each other.

For Article 10 ECHR to afford effective protection, indirect obstructions to the freedom of expression must fall within its scope where they typically and clearly hinder the free exchange of opinions and facts. Data retention has this effect. First, retaining all traffic data on the population's communications would have a disturbing effect on the free expression of information and ideas as described above. Second, if the state does not fully compensate telecommunications companies affected, prices for their services will rise significantly and formerly free services will partly cease to be offered, thus decreasing the amount of information people can afford to circulate. Therefore, data retention legislation interferes with the freedom of expression.

Article 10(2) ECHR states that the exercise of freedoms under Article 10(1) ECHR can be subjected to restrictions where it is necessary in the interests of, among others, national security, public safety, or for the prevention of crime. However, such legislation must fulfil the same conditions as described above in relation to Article 8 ECHR, most of all, the proportionality test.

Data retention legislation does not meet this requirement: The free exchange of information is of paramount importance in a democratic society. Traffic data retention has the effect of allowing communications to be revisited at will, thus deterring both providers and recipients of sensitive information. Particularly information that is critical of governments is subjected to this effect. In comparison to the marginal benefits of traffic data retention, its negative effects on the freedom of expression are major.

---

[18] Dated 23/11/2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[19] J. Frowein and W. Peukert, *EMRK-Kommentar* (Engel, 1996), Art. 10, § 5; D. Kugelmann, 'Der Schutz privater Individualkommunikation nach der EMRK', (2003) 30 *Europäische Grundrechte-Zeitschrift* 1–3, 20 with further references.

[20] Frowein and Peukert, *op. cit.* note 19 *supra;* Kugelmann, *op. cit.* note 19 *supra*, at 19.

[21] Frowein and Peukert, *op. cit.* note 19 *supra*, §§ 15 *et seq*.

Therefore, blanket data retention requirements are disproportionate and incompatible with Article 10 ECHR.

III The Protection of Property (Article 1 PECHR)

Article 1 of the first protocol to the ECHR (PECHR)[22] guarantees the protection of property. Article 1 PECHR applies to property that has been acquired rather than to future income or earnings.[23] Therefore, the fact that compulsory data retention would impose financial burdens on service providers and result in a loss of profits does not constitute an interference with Article 1 PECHR.

The jurisprudence of the Court of Human Rights recognises the customer basis of a company as property protected by Article 1 PECHR.[24] A state measure that results in a loss of customers to companies therefore interferes with their property rights.[25] Data retention requirements affect all telecommunications and Internet service providers in a similar fashion and are therefore unlikely to affect the customer basis of individual companies. Thus, their property rights are not interfered with in this regard.

The Court of Human Rights also recognises that an unintended, state-induced *de facto* deprivation of property is covered by the second sentence of Article 1(1) PECHR[26] if its effects are equal to those of formal dispossession. This is the case if possessions cannot be enjoyed in any purposeful way as a result of the measure.[27] A measure of that kind can only be deemed proportionate if the law provides for reasonable compensation.[28]

The machines and devices used by telecommunications service providers to operate their businesses are the property of those companies and thus protected by Article 1 PECHR. Compulsory data retention results in a *de facto* deprivation of service providers of that property if devices previously used to provide services cannot be upgraded or adapted to allow for traffic data retention and, as a result, become practically worthless. The second sentence of Article 1(1) PECHR consequently requires adequate compensation to service providers who suffer such losses where they are inevitable.

Apart from these extreme cases, data retention legislation could be manifested as laws controlling the use of property within the meaning of the second paragraph of Article 1 PECHR. A decision by the European Commission on Human Rights, on a German statute requiring employers to assist in the taxation of employees,[29] demonstrates that state-imposed obligations can be qualified as an interference with Article 1 PECHR. Although the Commission did not have to decide on the question because of

---

[22] Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, dated 20/03/1952, as amended by Protocol No. 11, dated 11/05/1994, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/009.htm>.

[23] Court of Human Rights, *Wendenburg* et al. *v Germany* (2003), available at: <http://hudoc.echr.coe.int/Hudoc2doc2/HEDEC/200308/71630_01_di_chb3_06_02_2003.doc>.

[24] *Wendenburg* et al. *v. Germany*, *op. cit.* note 24 *supra.*

[25] *Wendenburg* et al. *v. Germany*, *op. cit.* note 24 *supra*.

[26] References in Frowein and Peukert, *op. cit.* note 19 *supra*, Art 1 PECHR, § 25; C, Grabenwarter, *Europäische Menschenrechtskonvention* (Beck, 2003), at 417.

[27] Grabenwarter, *op. cit.* note 26 *supra* 417.

[28] Court of Human Rights, *James* et al. *v the United Kingdom* (1986), Publications A98, § 54; J. Meyer-Ladewig, *Konvention zum Schutz der Menschenrechte und Grundfreiheiten* (Nomos, 2003), Art 1 PECHR, § 29 with further references.

[29] European Commission on Human Rights, E 7427/76, Decisions and Reports 7, 148.

its irrelevance with regard to the case at hand, it examined whether the statute would be justified if it were an interference with property rights. This is an indication that the Commission would have qualified the law as an interference with the right of property if it had had to decide on the question.

In principle, any legislation imposing or prohibiting specific uses of property, controls the use of property within the meaning of Article 1(2) PECHR.[30] However, not every law that may require making use of one's property can be considered would be excessive to consider any law the compliance with that requires making use an interference with Article 1 PECHR. An indirect interference with the right of property should be recognised only where a law typically and clearly results in an encroachment on the right of peaceful enjoyment of property.

An obligation to retain traffic data would force telecommunications service providers to use their property in order to comply with the law. Presumably, some devices would even need to be used exclusively to retain traffic data, without serving another purpose. Therefore, data retention laws would clearly control the use of the service provider's property and thus interfere with their rights under Article 1 PECHR.

According to Article 1(2) PECHR, an interference can be justified in the general interest. In this regard, the contracting parties enjoy a wide margin of appreciation.[31] However, any interference must be proportionate.[32] In the case of data retention requirements, it has been shown above that the benefit of data retention is very limited. On the other hand, the financial burden on the companies compelled to retain data is substantial. The cost of retaining traffic data is by far exceeded by the cost resulting from the ensuing obligations to administer, search, and transmit retained data to authorities requesting it. The total cost of data retention is high and has been estimated to be in the United Kingdom alone, industry-wide £100 million (€150 million) at the least.[33] In view of its marginal benefit, data retention legislation can be deemed proportionate under Article 1 PECHR only if telecommunications companies are fully compensated for costs they incur for compliance. Whether such compensation is warranted for is for parliament to investigate before the introduction of such legislation.

Conclusion

In conclusion, blanket traffic data retention legislation is incompatible with Article 8 and Article 10 ECHR because its harmful effects on citizens by far outweigh its benefits. Furthermore, data retention laws are also an improper invasion in the rights of the telecommunications companies guaranteed under Article 1 PECHR if the government does not compensate their costs.

---

[30] Grabenwarter, *op. cit.* note 26 *supra*, 418; see also European Commission on Human Rights, E 5593/72, Collection of Decisions 45, 113, qualifying a law which required owners of tenanted buildings to maintain them as an interference with the right of property.

[31] Court of Human Rights, *Tre Traktörer Aktiebolag v. Sweden* (1989), Publications A159, § 62.

[32] *Tre Traktörer Aktiebolag v Sweden op. cit.* note 31 *supra*, § 59.

[33] APIG, All Party Parliamentary Internet Group (UK): *Communications Data, Report of an Inquiry*, January 2003, available at: <http://www.apig.org.uk/APIGreport.pdf>, at 24.