University of Dundee

The retention of communication data and fundamental human rights

With lessons from the United Kingdom and Norway

Matriculation nr: 110021992
14/08 2012

Word Count: 13 779

Table of Contents.

Acknowledgements:

I would like to thank Dundee Law School for giving me the opportunity to study there, and a special thanks to my supervisor Dr .Patrick Ford who helped and guided me in the process of writing my dissertation.

Abstract.

After an increasing development in the field of electronic communication, The European Union now imposes all Contracting States to retain communication data from every user of electronic communication services. This is done through directive 2006/24/EC, the so-called 'data retention directive'. The purpose with this directive is the investigation, detection and prosecution of serious crime. Also member states within the European Economic Community (EEC) will have to follow this directive as the European Court of Justice found it to be 'inner marked relevant'. Communication data is the opposite of communication content; it is data about the 'traffic' of electronic communication, but not its actual content.

This piece of work seeks to highlight if this mass retention of this type of data from entire populations with the purpose of future crime investigations is compatible with fundamental human rights enshrined in the European Convention of Human Rights, and especially the right of privacy which is enshrined in the Conventions article 8. The findings of this piece of work reveal a dangerous surveillance measure that can have negative impacts on not only privacy, but also democracy as we know it.

List of Statutes, Cases and other Legislative material:

I. Statutes:

EU/EEC legislation:

European Convention of Human Rights, Art 8

European Convention of Human Rights, Art 10

Treaty of the European Union, Article 6

Directive 2006/24/EC of the European Parliament and of the Council (the data retention directive)

United Kingdom legislation:

Data Retention (EC Directive) Regulations 2009/857

Data Retention (EC Directive) Regulations 2007 (SI/2199)

Crime and Security Act 2001 (ACTCA), Part 11.

Human Rights act 1998

Regulation of Investigatory Powers Act 2000

Regulation of investigatory powers (Communication data) Order 2010, SI 2010/480

Interception of Communications Act 1985, ss 1-10

Norwegian legislation:

Law of 22 May 1981 nr. 25 'Lov om rettergangsmåten i straffesaker' (Straffeprosessloven).

Law of 07 April 2003 nr 83 'Lov om elektronisk kommunikasjon' (Ekomloven).

Law of 15 April 2011 nr 11: 'Lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)' I

II. Cases:

European Court of Justice:

Ireland v European Parliament, Council of the European Union (Case C-301/06) Action for annulment - Directive 2006/24/EC - Retention of data generated or processed in connection with the provision of electronic communications services. Choice of legal basis. Judgment of the European Court of Justice (Grand Chamber) of 10 February 2009

National Courts:

Judgment of the German constitutional court (Bundesverfassungsgericht), Vorratsdatenspeicherung [Data retention] BverfG, 2 March 2010, 1 BvR 256/08

Decision no. 13627, Bulgarian Supreme Administrative Court.

Decision no.1258, Romanian Constitutional Court, 8 October 2009

Paton v Poole BC (2000) IPT/09/01/C

European Court of Human Rights:

Case of Copland v the United Kingdom App no. 62617/00 (03/04/2007)

Case of Klass and Others v Germany, App No. 5029/71 (ECtHR 06/09/1978)

Case of Leander v. Sweden (1987) 9 EHRR 433

Case of Liberty and Others v. The United Kingdom App no 58243/00 (ECtHR 01/07/2008)

Case of Malone v the United Kingdom (1985) 7 EHRR,

Case of S and Marper v the United Kingdom (2008) ECHR 1581

Case of Weber and Saravia v Germany App no. 54934/00 (ECtHR 29/06/2006)

III. Other legislative material:

European Council Declaration of Combating Terrorism (adopted on 25 march 2004)

Home Office: Explanatory memoarandum to the data retention (EC directive) Regulations 2009 No.859

Draft Communications Data Bill| Presented to Parliament| June 2012 |Cm 8359

Preparatory work for new legislation made by the Norwegian legislation:

NOU 2003: 18 'Mistankekravet for bruk av tvangsmidler'. (Norwegian legislation preparatory work, Suspicion requirement for the use of coercive measures)

Prop. 49 L (2010-2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomfoering av EU's datalagringsdirektiv i norsk rett.

Chapter 1: Introduction.

In the last two decades the world has gone through major changes. One trend in particular is that the world depends more and more on information and communication technology. The world has 'gone digital', and for most people new technology plays a crucial part in their daily lives from the use of a computer and having internet access at home or work, to texting or making calls on a mobile phone. Even if people do not make direct use of these technologies, they are surrounded by networks through which information constantly flows[1].

Information technologies are of value to investigators too, and in the wake of sophisticated terror-atrocities throughout the world, the needs for more effective tools for law enforcement were stressed by governments throughout the western world. Directive 2006/24/EC; the data retention directive, was adopted by the European Union (EU) on the 15 March 2006, requiring the retention of telecommunications data for a period of six months up to two years[2]. The data retention directive represents in many ways one of the most intrusive surveillance measures ever; societies dependence on digital technology now makes it possible to monitor every aspect of peoples lives, The opportunities for surveillance that technology gives might be a useful tool to fight criminality and terror, but on the other hand there are not just terrorists and criminals who get affected by it, but all of us. It is therefore important to discuss how far it is reasonable to stretch the possibilities that technology gives us in the struggle for a safer society[3].

Whatever a person does when using a mobile phone or the internet can be effortlessly centrally recorded[4]. Communication data, as opposed to the actual content of communication 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[5]. The analysis of traffic data may reveal details of a person's political, financial,

[1] The Office for National Statistics (ONS) Social Trends 41: e-Society. (2010) available at <http://www.ons.gov.uk/ons/search/index.html?pageSize=50&sortBy=none&sortDirection=none&newquery=social+trends+41> (accessed 9/8 2012)
[2] Directive 2006/24/EC of the European Parliament and of the council, Art 6.
[3] Jocahim Hammerlin: 'Terror & demokrati. Fra 11.september til 22' Juli. Forlaget manifest AS, Oslo (2011). 23.
[4] Patrick Breyer' Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. European law review, vol. 11 no.3, May 2005. 365
[5] ibid

religious stance, or other interests[6]. The question is if such retention of every citizen's communication data is consistent with the European Convention of Human Rights (ECHR) requirements for privacy and the right of private correspondence which after the Conventions art 8, which is also related to and overlap the freedom to hold opinions and receive and impart information and ideas without interference by public authority after ECHR art 10.

A number of civil society organisations wrote to the commission arguing that data retention is, in principle, an unnecessary restriction of individuals' right to privacy[7]. They consider the non-consensual 'blanket and indiscriminate' retention of individuals' telecommunication traffic, location and subscriber data to be an unlawful restriction of fundamental rights[8]. Also, the European Data Protection Supervisor expressed doubts about the necessity of the measure[9]. Furthermore, this seemingly straightforward directive has 'generated' quite an impressive number of court judgments[10]. They range from the European Court of justice[11] (ECJ) to the Constitutional Courts of some Member States[12]. While the ECJ ruling is concerned with the legal basis of the directive itself, the constitutional judgments in different member states subject the national implementation of the Directive in order to test concerns about the legality, the legitimate purpose and proportionality of the measures[13]. The Constitutional courts in Germany, Romania and Bulgaria have all found the implementation of the directive to be breaching their constitutions, with some different reasoning: The focus of the German constitutional court have been on access and use of retained data, it does not condemn data retention itself[14]. The Bulgarian constitutional aversion to centralized storage

[6] Ibid

[7] Report from the Commission to the council and the European Parliament – Evaluation report on the Data Retention Directive (Directive 2006/24/EC) Brussels 18.4.2011 29

[8] idem

[9] European Data Protection Supervisor Press release: 'Data Retention Directive fails to meet data protection requirements' (1 June, 2011) Available at: <http://www.edri.org/edrigram/number9.11/data-retention-directive-failure-edps>

[10] de Vries, Bellanova & de Hert, 'Proportionality overrides Unlimited Surveillance: The German Constitutional Court Judgment on Data Retention' (May 2010) CEPS 'Liberty and Security in Europe' p 1

[11] *Ireland v European Parliament, Council of the European Union* (Case C-301/06) Action for annulment - Directive 2006/24/EC - Retention of data generated or processed in connection with the provision of electronic communications services – Choice of legal basis. Judgment of the European Court of Justice (Grand Chamber) of 10 February 2009

[12] Germany, Romania and Bulgaria.

[13] de Vries, Bellanova & de Hert (n.10) p 7.

[14] *Judgment of the German constitutional court* (Bundesverfassungsgericht), Vorratsdatenspeicherung [Data retention] BverfG, 2 March 2010, 1 BvR 256/08. Available at:

and direct access with any court control is very similar to the reasoning found in the German judgment[15]. The Romanian court's approach on the other hand has been considering blanket retention of data disproportionate by nature as well as the legislation on access and use of retained data[16].

This illustrates that the directive rises a distinction; on one hand there is the directive itself, and on another hand there is the national implementation of the directive. This piece of work will deal with both the directive as a whole, and the national implementation when it comes to use and access of retained communication data, in the United Kingdom, and in Norway.

This piece of work will in chapter 2 give an introduction to Directive 2006/24/EC and also give an introduction to the human rights mechanisms within the EU, and Europe as a whole. Chapter 3 will give detailed human rights critique of the directive itself; it will analyse if Directive 2006/24/EC as a whole is an interference with the right to privacy as enshrined in ECHR art 8; if it is in accordance with the law, if it is necessary in a democratic society; which is a matter of proportionality. Chapter 4 will assess a human rights critique of the United Kingdom's implementation of the directive through Regulations 2009/857, where access and use of communication data is regulated through the Regulatory of Investigatory act 2000 (RIPA). Chapter 5 will focus on the Norwegian implementation of the directive, which is still not in force, and highlight the differences between the United Kingdom and the Norwegian approach of the implementation. This thesis will reveal a directive that is in itself disproportionate; and national implementations of this directive that in the United Kingdom breaches fundamental human rights, but doesn't affect Norway to the same extent.

<http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html> (accessed at 29/05/2012)
cited in de Vries, Bellanova & de Hert (n.10) p 8

[15] *Decision no. 13627, Bulgarian Supreme Administrative Court* ('Върховния административен съд'), December 2008. Commentary in English: <http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention> (Accessed at 29/05/2012).
cited in de Vries, Bellanova & de Hert (n.10) p 8

[16] *Decision no.1258, Romanian Constitutional Court*, 8 October 2009. Published in the Romanian Official Monitor, no. 789, 23 November 2009. English translation (unofficial): <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf> (accessed at 29/05 2012)
cited in de Vries, Bellanova & de Hert (n.10) p 8

Chapter 2: Retention of communication data: an initial human rights critique.

2.1 The directive's background and content

The Madrid and London bombings, which together resulted in more than 250 deaths, revealed that Europe's counter terrorism strategy was far from adequate[17]. In 2004 the EU adopted a declaration[18] where the need to adopt common measures to retain data in combating terrorism was stressed. The European Council was asked by the commission to come up with ideas for the establishment of common EU rules for the retaining of electronic communication, which led to a proposal for a council decision about data-retention. This proposal was submitted by Sweden, the UK, France and Ireland in April 2004[19]. The proposal was rejected by the European Parliament in September 2005 on the basis that this was founded upon Articles 31 and 34 in the Treaty of the EU, which is the so-called 'third pillar' of the Union; Police and Judicial Co-operation in Criminal Matters. In 2005 the commission made a proposal for a directive, where they argued that the legal basis for data retention belongs in the scheme of the free market, rather than 'the pillar' of Police and Judicial Co-operation in Criminal Matters. The proposal from the Commission was changed in certain areas after negotiations with the EU Parliament and the Council [20] and after some further changes it was accepted. In March 2006 the Data retention directive was adopted by the EU.

Today the data retention directive imposes the Member States of the EU and the European Economic Community[21] (EEC) to retain data that can identify and trace the participants in a phone call and the type of phone which is used, the time for the communication, and the geographical location of the person participating in the communication, and which time the telecommunication took place[22]. Furthermore, the data retention directive also demands traffic data from internet usage to be stored. Data which is necessary to identify the user behind an

[17] Marie-Helen Maras: 'From targeted to mass surveillance: is the EU data retention directive a necessary measure or an unjustified threat to privacy' in 'New Directions in Surveillance and Privacy'. Willan Publishing (2009) 76.

[18] European Council Declaration of Combating Terrorism (adopted on 25 march 2004)

[19] Prop. 49 L (2010-2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomfoering av EU's datalagringsdirektiv i norsk rett. 11 Para 2.1
(Preparatory work for new legislation made by the Norwegian government)

[20] ibid

[21] Norway, Liechtenstein and Iceland

[22] Directive 2006/24/EC, Art 3.1 – Art 5.1

IP-address, in regard to both the use of and communication over the internet is retained[23]. The data is stored for a minimum period of six months and a maximum of two years[24]. The DRD does not obligate the states to retain the content of the correspondence such as for example which websites have been visited or the actual content of a text message or the content in an e-mail[25]. In other words, it is the so-called 'traffic data' or 'communication data' that is retained, and not the 'content data' or 'communication content'.

The purpose of the data retention is the investigation, detection and prosecution of serious crimes.[26] What is considered 'serious crime' is not defined by the directive, so it is up to each Member State to consider what is included within this definition of serious crimes in accordance with its national laws subject to the relevant provisions of EU law or public international law[27]. Also, what procedures are followed and the conditions required in order to gain access to the retained data is up to the Member States to decide[28].

2.2 Introduction to European Human Rights Law.

The three formal sources for European Union (EU) Human rights law are listed in Article 6 of the Treaty of the European Union (TEU). The first one is the EU Charter of Fundamental Rights which was proclaimed in 2000, and upgraded to the same binding legal status as the Treaties by Lisbon in 2009. The second is the European Convention of Human Rights (ECHR), which has long been treated by the European Court of Justice (ECJ) as a 'special source of inspiration'. The third is the 'general principles of EU law', a body of legal principles, including human rights, which have been articulated and developed by the ECJ for years, drawing from national constitutional traditions, the ECHR and other international treaties signed by the Member States. These three sources overlap, since many provisions of the EU charter are based on the ECHR, creating a certain amount of legal confusion[29].

[23] ibid
[24] Ibid, Art 6
[25] Ibid, Art 1.2
[26] Ibid, Art 1.1
[27] Ibid, Art 4
[28] ibid
[29] Paul Craig & Gráinne de Búrca. 'EU Law – text, cases and materials'. (2011) Oxford university press. 362-367

By treating the ECHR as a source of inspiration rather than a formally binding or fully binding agreement, the EU and the ECJ retained the freedom to 'go beyond' the Convention in recognizing or not recognize rights as part of EU law[30]. This means that, in theory, the ECJ can decide to deem directives that are in total breach of the rights such as those enshrined in the ECHR to still be compatible with EU law. In other words: the question about the legality of the directive itself is an ECJ question. The question if the implementation of the directive on a national level is compatible with human right standards is on the other hand a ECHR question relevant for the European Court of Human Right (ECtHR). However, it seems clear that the ECJ is willing to look closely at the relevant ECtHR case law for guidance[31].

It is implied in the directive that the EU presumes that this form of data retention is consistent with both the Union's Charter of Fundamental Right, and with the European Convention on Human Rights (ECHR). The European Union assumes that as long as the processing of retained data and the conditions for disclosure of this data to the police or prosecuting authorities is in accordance with the basic requirements of the rule of law and proportionality that the ECHR demands - the human right aspect will be safeguarded[32].

The next chapter will assess if the question of the storage and retention of data which is regulated by Directive 2006/24/EC fulfills the human rights standards set out in the convention, and then first and foremost Art.8

[30] ibid

[31] ibid

[32] Jon Wessel-Aas. 'Datalagringsdirektivet – er dets krav om lagring av trafikkdata forenelig med den europeiske menneskerettighetskonvensjonen?' (2010) Nordisk årbok i rettsinformatikk, 136. (Journal article on the data retention directives compability with the ECHR)

Chapter 3: Retention of communications data – a human rights critique.

In regard to the Human right aspects of the data retention directive, Human Right issues concerning the Contracting States implementation of the directive have not yet been up for the ECtHR. Cases that have been up for the ECtHR that concern privacy, have mostly been concerned around if the specific (targeted) measures have been proportionate, and if control mechanisms of the specific measures that have been used have been sufficient in line with the principles of the convention and the rule of law. What we see within the scheme of both the practice of the ECtHR and the constitutional courts judgments, such as the German Constitutional Courts judgment of the 2nd of march 2010[33] where it said 'no' to the German implementation laws of the directive, seem to indicate the emergence of a new important demarcation within data retention[34]. On one hand there is the question of the storage and retention of data, which is regulated by the data retention directive, and on the other hand there is the question of the use and access to these data, which falls under the competency of the individual member state[35].

However, some cases that in many ways raise the same issues as the directive have been up for the court and one case has concerned the principle of in-discriminatory mass retention of highly personal data of innocent and acquitted individuals[36]. Before looking at the specific cases, there will be necessary to evaluate if the directive constitutes an interference with ECHR art. 8:

"Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is 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."

[33] Supra (n 10)
[34] de Vries, Bellanova & Paul De Hert (n.10) 4.
[35] Ibid.
[36] *Case of S and Marper v the United Kingdom* (2008) ECHR 1581

If the directive is interfering with the right for private and family life, home and correspondence as stated in the first section, for the directive then to be accepted in spite of its infringing nature, it has to pass a legality, necessity and proportionality test after section two. It must be in 'accordance with the law' which means it has to have its basis in some domestic law. Furthermore, it has to be adequately accessible and must be formulated so that it is sufficiently foreseeable[37]. The second condition that has to be met is that it has to be 'necessary in a democratic society' in pursuit of one or more legitimate aims as prescribed in Art 8.2. Thirdly, it has to pass a proportionality test[38]. Proportionality requires that there is a rational connection between the objective a particular measure pursues, and the means the state has employed to achieve that objective[39].

3.1 Is the data retention directive an interference of ECHR Art.8.?

The question, whether this retaining of traffic data from phones and phone calls is considered to be an infringement according to ECHR Art 8, can be answered positively with the case of *Malone v the United Kingdom*[40]. The judgment concerned the laws and practices in England and Wales allowing interception of communications and "metering" of telephones by or on behalf of the police[41]. The Strasbourg court held that metering information, which includes information on numbers dialed is an 'integral element' in the communications made by telephone and the duration of the calls made, falls within the scope of 'private life' under ECHR Article 8(1).[42]

The case of *Copland v the United Kingdom*[43] shows that storage of traffic data when it comes to the use of internet and email also can be considered a breach of Art 8.1. In this case the

[37] Maras (n 17) 81
[38] Maras (n 17) 87
[39] Emmerson & Ashworth 'A Human Rights and Criminal justice' (2001) London: Swet and Maxwell p 93. Maras (n 17) 87
[40] *Case of Malone v United Kingdom* (1984) 7 EHRR 14
[41] Council of Europe report: 'Case law of the European Court of Human Rights concerning the protection of personal data' (DP 2009 Case law) Available at: <http://www.coe.int/c/document_library/get_file?uuid=ec21d8f2-46a9-4c6e-8184-dffd9d3e3e6b&groupId=10227> (accessed 12/08/2012) 14
[42] *Malone v United kingdom* (n 40) para. 84
Maras (n 17) 80
[43] *Case of Copland v the United Kingdom* App no. 62617/00 (03/04/2007)

Court considered that the employers collection and storage of personal information by the use of the telephone, e-mail and internet at the workplace interfered with the employees right to respect of private life and correspondence, Furthermore, in the case of *Leander v Sweden*[44] it was confirmed by the Strasbourg court that the retention of private information is a breach of Art 8 when it happens without the consent of the citizens concerned[45].

These cases combined show that the storage and retaining of traffic data both when it comes to communications by phone, via e-mail and internet will be an interference of Art 8; the right to privacy and correspondence, and therefore the retention of these types of data, which is the core of the data retention directive, needs to be justified by the criteria in Art 8.2 to be pursuant with the human rights standards enshrined in ECHR.

3.2 Is the data retention directive 'In Accordance with the law'?

Having concluded in section 3.21 that the directive constitutes an interference of ECHR Art.8 for the directive then to be accepted in spite of being an interference of Art 8, it must be in 'accordance with the law'. This means it has to have its basis in some domestic law. Furthermore, it has to be adequately accessible and must be formulated so that it is sufficiently foreseeable[46].

The data retention laws stem from EU directive 2006/24/EC and are implemented in the contracting states through national legislation. This means it has legal basis in an EU directive which is made a part of domestic law, and hence is available and known for the public. The requirements of retention that the directive itself sets out are therefore in accordance with the law. However, the directive gives the states a margin of discretion how to implement the directive in its national laws, for example on which grounds authorities can acquire and obtain access to retained communication data. This national legislation will also have to meet the requirements to be foreseeable, accessible and formulated so it is sufficiently forseeable for the public. The ECtHR decision in *Liberty and others v. the United Kingdom*[47] points to that the law has to be precise, so that the authorities are not granted an unfettered discretion to perform general surveillance measures. The legality of the national legislation, such as the

[44] *Case of Leander v. Sweden* (1987) 9 EHRR 433
[45] Wessel-Aas (n 32) 137
[46] Maras (n 17) 81
[47] *Case of Liberty and Others v. The United Kingdom* App no 58243/00 (ECtHR 01/07/2008)

access and use of retained data will be taken in account as factors determining the proportionality of the directive. This will be done further down in chapter 4 and 5, focusing on the national implementation of the directive in the United Kingdom, and Norway. To sum up; the directive itself is in accordance with the law, but the national implementation of the directive, might or might not be in accordance with the law.

3.3 Is the data retention directive necessary in a 'democratic society'?

The second condition that has to be met if for the directive to be accepted in spite of being an interference with art 8, is that the measures in it has to be 'necessary in a democratic society' in pursuit of one or more legitimate aims as prescribed in Art 8(2). Recital 21 of the Directive reveals that this measure pursues a legitimate aim because its objective is to retain data for the 'purpose of the investigation, detection and prosecution of serious crime' where serious crime such as terrorism falls within the categories of the legitimate aims mentioned in Article 8(2)[48]. This gives the states certain discretion in what measures it might use to pursue this national interest.

The ECtHR has clearly stated that the social 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[49]. Some have interpreted the jurisprudence of the Court of Human Rights as outlawing any exploratory or general surveillance not carried out on a case-by-case basis in the event of reasonable suspicion. It is unclear whether the Court of Human Rights would indeed take such a stance[50]. So far, it has not decided on the matter[51].In its decision on the *Weber and Saravia v Germany*[52], the Court of Human Rights noted that the Act did not permit 'so-called exploratory or general surveillance but did not elaborate on the consequences this would enable[53]. Therefore, this mention does not provide a sufficient basis

[48] Maras (n 17) 85
[49] Breyer (n 4) 368
[50] ibid
[51] July 2012
[52] *Case of Weber and Saravia v Germany* App no. 54934/00 (ECtHR 29/06/2006)
[53] Breyer (n 4) 368

for legal argument; instead, the compatibility of data retention with Article 8 is an issue of proportionality[54].

3.4 Proportionality.

Proportionality requires that there is a rational connection between the objective a particular measure pursues and the means the state has employed to achieve that objective[55]. In other words: under the label 'necessity in a democratic society' a proportionality test has to be conducted. The interference must be proportionate to the legitimate aim of the restriction. The ECtHR affords to the State a margin of appreciation when deciding whether an interference with an Article 8 right is justified under paragraph 2 of that provision, this margin of appreciation as a factor determining proportionality will be dealt with for UK in chapter 4 and Norway in chapter 5.

3.41 Retention of communication data.

The Data retention directive represents a blanket approach to surveillance, where the majority of the populations that will be affected by it are bound not to be terrorists or criminals[56]. The nature of the directive differs from most of the cases that have been up for the ECtHR in regard to infringements of privacy where most cases have mainly revolved around individuals whose personal information have been retained and used for more or less targeted purposes; such as specific criminal cases under investigation, or to prevent terrorism or other serious crimes which threaten national security. The main elements in the ECtHR assessment have been to avoid that the infringements is arbitrary or disproportional towards the individual who is affected[57] and have not taken in account mass-surveillance.

The case of *S and Marper v the United Kingdom* however shows that the ECtHR can be willing to do a concrete evaluation of the proportionality of blanket data retention itself. In this case the ECHR found the retention of DNA from innocent or acquitted people to be a breach of Art.8.

[54] ibid
[55] Maras (n 17) 85
[56] Clive Walker: 'Terrorism and the Law' (2011) Oxford University Press 74
[57] Wessel-Aas, (n 32) 143

3.42 The judgment of *S and Marper v the United Kingdom*[58].

In this case the Court were not first and foremost interested in the guarantees and safeguards against misuse of retained information, but rather focused on the issues of blanket retention of innocent individuals as a principle. It is the only case for the Strasbourg Court which concerns mandatory mass retention of personal information of law abiding citizens, without other purposes than for use in future criminal cases[59].

S and Marper v UK concerned mass data retention, like the directive. More precisely it concerned the retention and use of information that was retained in DNA-registers. In this case, the complainants were two British citizens who both had their cases dropped. In both cases biometrical information and DNA samples had been retained for investigation, and when afterwards the complainants was acquitted and demanded that their fingerprints and DNA samples be destructed, the Police refused to do so. The background for this was the UK practice in the area. The UK started with DNA-registers in 1995 and today has the largest database of this kind of information in the world. In 2008 it contained around 5 million people, of which half million were children under the age of 16[60]. With an increase of around 700 000 per year it is estimated that the database today has at least 6 million profiles, ca 10% of the British population[61].

The reason for the massive increase in the information stored in this database can be traced back to 2003, when the British government started to register DNA of anyone arrested for any criminal felony[62]. This also included minor incidents, like being under the influence of alcohol in public, and the participation in illegal demonstrations[63]. It is estimated that at least one million were innocently registered[64]. The court considered the storage of fingerprints, cell-

[58] *Case of S and Marper v the United Kingdom* (2008) ECHR 1581
[59] Wessel-Aas (n 32) 146
[60] Report from the Human Genetics commission 2009. Available at: <http://www.hgc.gov.uk/Client/document.asp?DocId=226> (accessed 11/08 2012) 3, 4, 74
Hammerlin (n 3) 26-28; O' Hara, Kieron and Nigel Shadbolt: 'the spy in the coffee machine'(2008) Oxford: oneworld publications 107-108; Alex Deane. 'Big brother watch: the state of civil liberties in modern Britain. London (2010) Biteback Publishing. 47; John Kampfner 'Freedom for sale: How we made our money and lost our liberty'(2010) Pocket books 205; Dominic Raab: 'the assault on liberty: what went wrong with rights (2009) London: Fourth Estate 101-102.
[61] ibid
[62] ibid
[63] ibid
[64] ibid

prints and DNA-profiles of people who had been suspected but not sentenced, such as in this case, not to be based on a reasonable balancing between the competing public and private interests. Furthermore, the Court stated that it was especially worried about the risk of stigmatization of people in the complainants' situation; that is people who were not sentenced and who have a right to be considered innocent were to be treated the same way as people who have committed a felony[65].

One of the central points of this judgment is how the ECtHR addressed the nature of this retention: "*In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender"*[66] . The Government argument in this case was that the retaining of private information would not have any appreciable effect on the individuals because the information would only be used later if it could link the citizen to a criminal offence. The ECtHR addressed this with the following words: "*The Court is unable to accept this argument and reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data*."[67]

The ECtHR arguments on this case reflect the principle of the 'presumption of innocence'; those not charged or convicted with a crime and thus innocent, should not have their DNA, fingerprints or other profiles kept by the police[68]. Those who advocates against the directive argue that this principle should also apply for the data retention directive, and they advocate that the argumentation of the court could be used analogically; communication data of innocent people which reveal contact networks and movement patterns should not be kept by the government. Those who argue in favour of the directive point that the court's reasoning in this specific case must be taken in consideration as a whole. DNA was not retained generally for the population, but innocent and acquitted people had their DNA retained the same way as

[65] *Case of S and Marper v UK* (n 58) Para 116.
[66] *Case of S and Marper v UK* (n 58) Para 119
[67] *Case of S and Marper v UK* (n 58) Para 121
[68] Joint Committee Report on Human Rights. 'Enhancing Parliament's role in relation to human rights judgments' Great Britain Parliament: 15th report of 2009-2010 33

DNA from convicts, something that would lead to stigmatization of people in the complainants' situation, who were not sentenced and who have a right to be considered innocent. The reasoning here is that because the directive makes sure that the information of every citizen is retained, everybody gets the same treatment, hence there is no discrimination[69]. Furthermore in *S and Marper v the United Kingdom*, the complainants had limited possibilities to have data removed. If we compare this to the data retention directive, data is kept by the public communication provider 'just' for a period between six months and two years from the date of the communication in question[70].

However, the case of *S and Marper v the United Kingdom* shows that the ECHR clearly have on a principal level condemned the blanket retention of personal information of innocent or acquitted individuals, without other purposes than for use in future criminal cases.

3.43 Broader factors determining proportionality

There are also other factors that can be taken in regard when considering if the directive is a proportionate measure. These factors are not strictly juridical factors, but represent nevertheless important arguments in when considering the overall proportionality of the mass retention of communication data. Evasion of the directive is easy, and the possibilities for evasion might have negative consequences on the fight against crime. The directive will have economic impacts, and cost the society and communication service providers money. The intention with the directive is good; the government wants to be ahead of the criminals and tries to prevent offences from being committed. Databases which cover the entire populations' network, contacts and movement patterns are created in case this information should be valuable for investigating future offences[71]. It is in other words a form of pre-emptive evidence handing. This can however also lead to an undermining of rule of law and what we consider liberal democratic values and the concept of the mass retention of communication data is in conflict with the presumption of innocence[72]. To answer the question if the directive constitutes is disproportionate it will be necessary to have a look on what broader consequences the mass retention of communication data might have on society as a whole.

[69] Ingvild Bruce: 'Datalagringsdirektivet – en menneskerettskrenkelse eller –forpliktelse' (2010) Lov og Rett 2010-6 22 (Journal article on the data retention directive)
[70] Directive 2006/24/EC, Art.6
[71] Hammerlin (n 3) 80-81
[72] ibid

3.431. Evasion

One argument that points in the direction that the directive is disproportionate is the argument that evasion of it is relatively simple. Detection difficulties can be multiplied by using a public internet terminal, the use of more sophisticated anonymised web browsing systems, and the use of foreign-based information society service providers[73]. One example of how easy a terrorist suspect can avoid to getting caught by the mechanisms imposed by the data retention directive is Zacarias Moussaoui, who was charged as a conspirator in the September 11 attacks. The FBI only discovered that Moussaoui had utilized three Hotmail accounts through his written court pleadings[74]. If the directive had been into force at the time and in the relevant area where he operated, it would therefore not make any difference for the prevention of terrorism.

3.432 Effect on investigations

An analysis of the German Federal Crime Agency (BKA) statistics, published by the German privacy rights group AK Vorrat, suggests the loss of data retention will make little practical difference to police[75], and it is stated in the report that because of easy evasion, blanket data retention can actually have a negative effect on the investigation of criminal acts[76]. In order to avoid the recording of sensitive personal information under a blanket data retention scheme, people who of some reason wants to avoid the attention from the authorities will increasingly resort to Internet cafés, wireless Internet access points, anonymisation services, public telephones, unregistered mobile telephone cards, non-electronic communications channels and such like[77]. This avoidance behaviour can not only render retained data meaningless but even frustrate targeted investigation techniques (e.g. wiretaps) that would possibly have been of use to law enforcement in the absence of data retention[78]. Because of this counterproductive effect, the usefulness of retained communications data in some investigation procedures does not imply that data retention makes the prosecution of serious

[73] Walker (n 56) 77
[74] ibid
[75] Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics: available at: <http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf> (accessed 01/08 2012)
[76] Ibid
[77] ibid
[78] ibid

crime more effective overall. There might be reasons blanket data retention can actually be detrimental to the investigation of serious crime, facilitating some investigations, but frustrating others[79].

3.433 Leaks

The directive constitutes a faith in the authorities' ability to secure this type of information which in many cases will be very sensitive[80]. Stored information is never 100% safe, and there are many examples of information getting lost. One of the first political crises that Gordon Brown had to face as prime minister was when private information of 25 million British citizens was lost (almost half of the British population!). Information such as bank numbers, social security information was lost in the mail in November 2007[81]. In 2008 a person within the British ministry of defence lost a laptop that contained personal information of 900 000 people[82]. According to a research made by the privacy group 'big brother watch' data has been lost by or stolen from UK local councils more than 1,000 times since 2008[83]. Importantly, Computer systems will always be at risk of break-ins or leaks. Just one example of this happened in 2011 when Sony lost private information of 77 million PlayStation users, possible including card details[84]. Another potential risk is the risk of disloyal system servants. One example of this is the American soldier Bradley Manning who downloaded large amounts of information from American intelligence, and gave it to the website wikileaks[85]. Even though many would argue that Manning represents the more heroic examples of 'disloyal servants', one could imagine situations where we have a 'Manning' with another political and personal agenda[86].

---

[79] ibid

[80] Hammerlin (n3) 75

[81] 'Brown apologises for records loss'< http://news.bbc.co.uk/1/hi/uk_politics/7104945.stm#graphic> (BBC, 21 November 2007) accessed 01/08/2012
Hammerlin (n 3) 75

[82] 'Personnel records stolen from MoD' <http://news.bbc.co.uk/1/hi/england/gloucestershire/7639006.stm> (BBC, 27 September 2008) accessed 12/08/2012

[83] Tom Espiner, 'Local councils report only 55 of 1,035 data losses' (ZDnet November 23, 2011) <http://www.zdnet.com/local-councils-report-only-55-of-1035-data-losses-3040094491> accessed 12/08 2012

[84] Charles Arthur & Keith Stuart ,' PlayStation Network users fear identity theft after major data leak' (the Guardian, 27 April 2011) <http://www.guardian.co.uk/technology/2011/apr/27/playstation-users-identity-theft-data-leak?INTCMP=SRCH> accessed 12/08/2012

[85] Hammerlin (n3)p 76-77.

[86] ibid

3.434 Costs.

One factor determining if the data retention directive is proportionate is the economic impact of the directive. If more money are invested in data retention this means that less will be available for other initiatives because of the finite number of resources available for competing activities[87], since there is an infinite number of risks and only a limit of resources to spend on counter terrorism, priority should be given to those which provide the highest expected benefit at a low cost[88].

The direct costs of the directive includes the cost of storage and support infrastructures, system technology for the processing and storage of data, changes in design systems, more powerful and sophisticated platforms, security of archived data, costs for searching and retrieving archived data (making data available for law enforcement authorities) and human resources to handle that data[89]. The indirect consequences of the implementation of the directive is factors such as its impact on economic growth and competitiveness, impacts on the potential for innovation and technological development and its resulting increases or decreases in consumer prices[90].

A study carried out before the transposition of the Directive estimated the cost of setting up a system for retaining data for an internet service provider serving half a million customers to be around €375 240 in the first year and €9 870 in operational costs per month thereafter, and the costs of setting up a data retrieval system to be €131 190, with operational costs of €28 960 per month[91]. The home office calculates in the impact assessment for the proposed changes to the UK implementation of the directive that the total economic costs over 10 years starting from 2011/12 are estimated to be £1.8 billion. The additional costs to the private sector relate to the investment in capabilities required by Communication service Providers to implement suitable systems to capture, retain and transmit data are estimated at £859m over

[87] Marie-Helen Maras: 'The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?' (2012) 33 European Journal of Law & Economics 449
[88] ibid
[89] Maras (n 87) 451
[90] ibid
[91] Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC) 26

ten years[92]. The home office also calculates in the impact assessment with benefits, calculating the benefits of the implementation of the directive in a 10 year period to be expected benefits from addressing the decline in the proportion of communications data available to the police and others are estimated to be £5.0 – £6.2 billion.

The assessment takes into account an analysis of criminal behaviours by the Serious and Organized Crime Agency and an analysis of the future communications. The largest categories of benefits are direct financial benefits arising mainly from preventing revenue loss through tax fraud and facilitating the seizure of criminal assets[93]. However, the different estimates provided by governments and service providers have caused uncertainty as to which cost are truly reflective of the financial impact of this measure. Criminals are rational agents who will adapt their behavior after what government measures are taken to fight crime[94], and hence an analysis of what economic benefits crime fighting measure like the data retention directive would lead to would therefore be difficult to predict. Furthermore the governments cost analysis on the direct costs of the directive has been significantly lower than those provided by the telecommunication and electronic communications industry[95]. The LSE suggests that the real cost may be closer to £12 billion[96].

Furthermore, Additional costs will be the indirect economic costs. The directives will lead to an inconsistency in the marked because the contracting states can choose, or choose not to compensate the service providers. This can have to a negative impact of competition between communication service providers in Europe. More expensive communication-services may furthermore lead customers to use international webmail services (that is non-EU providers) and new marked participants to take their business elsewhere. In conclusion; the economic disadvantages of the data retention directive therefore outweigh the economic advantages[97]. One thing is certain; the directive is going to be a costly affair.

---

[92] Home office impact assessment on communications data legislation IA No: HO 0073. Available at: <http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-ia?view=Binary> (accessed 24/07 2012)
[93] Ibid.
[94] Maras (n 87) 449
[95] Maras (n 87) 451-452
[96] Adam Gersch: 'Covert surveillance – a snoopers' charter' (2012) 5th Archbold Review 8
[97] Maras (n 87) 469

3.435 Chilling effect

People might change their behaviour if they know there is a possibility they are being watched, this is what is called the 'chilling effect'. A poll of 1,000 Germans found in 2008 that indiscriminate blanket communication data retention is acting as a serious deterrent to the use of telephones, mobile phones, e-mail and the Internet[98]. The survey conducted by the 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[99]. There can be no doubt that obstructing confidential access to help facilities poses a danger to the physical and mental health of people in need as well as to the safety of the people around them[100].

If an entire population knows that there is a possibility they might be snooped on, and that information stored about them might get out of hand, this will possibly change society as a whole, and lead to a 'chilling effect 'of the entire society. Knowing that we might be watched, would we start to behave differently[101]? How many might think twice about participating in political markings if they know that this can trigger interests from the American embassy[102]? How many will refrain from participating in public debates because they do not find it is worth the burden it might cause? In what way will this influence the exchange of views which is the backbone of democracy?[103] The fear of knowing that information about you might get out of hand, or that you are being watched will lead the population to restrain themselves, and

[98]Poll on data retention (in German): <http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf> accessed 12/08/2012
[99] Digital Rights Ireland, 'Press Release on German Data Retention Decision' (March 3rd, 2010) <http://www.digitalrights.ie/2010/03/03/press-release-on-german-data-retention-decision> accessed 12/08/2012
[100] Dr Breyer and Arbeitskreis Vorratsdatenspeicherung (Working group on Data retention), 'Civil society letter to MEPs on mandatory data retention' Available at: <http://www.statewatch.org/news/2010/dec/eu-mandatory-data-retention-civil-society-letter-10.pdf> accessed 12/08/2012
[101] Hammerlin (n 3) 87-88
[102] ibid
[103] ibid

it will have a 'chilling effect' on the people's will to participate in public life and hence democracy[104].

3.5 Summary and Concluding remarks.

The data retention directive, Directive 2006/24/EC is an interference of privacy after ECHR Art.8 and will therefore have to be justified with the requirements of the second paragraph of the same article. The directive is a question of proportionality, and the ECtHR judgment of *S and Marper v the United Kingdom* shows that the blanket mass retention of ordinary citizens' personal information independently of any concrete investigation will have big problems by passing the ECtHR normal requirements what is considered proportionate[105]. Other factors that indicates that the directive is disproportionate is because evasion is relatively simple by using for example a public internet terminal, the use of more sophisticated anonynmized web browsing systems, and the use of foreign-based information society service providers[106]. Furthermore, it is questionable how much the mass retention of communication data really matters for police investigations, and it might even have a negative effect on it. This because criminals are rational agents whose behaviour is best understood as an optimal response to incentives set by the government through expenditures on law enforcement[107]. The costs are also high, and it is difficult to tell how much the directive really costs, and even harder to say how much economic benefits it leads to. All these factors point in the direction that the nature of blanket mass retention of communication data itself represents a disproportioned measure, and this point in the direction that is not 'necessary in democratic society' as required by Art.8. The blanket mass retention of communication data might have many different consequences; but the disturbing effect it can have on society as a whole leads to the conclusion that while it is doubtful that data retention directive is 'necessary in a democratic society' it can rather lead to harmful effects on democracy itself.

[104] ibid
[105] Prop. 49 L (n 19) 3.1
[106] Walker (n 56) 77
[107] Maras (n 87) 458

Chapter 4: United Kingdoms' implementation of the Directive.

In the United Kingdom the data retention directive, 2006/24/EC is implemented through the Data Retention (EC Directive) Regulations 2009/857.These regulations relate to internet access, internet e-mail and internet telephony as well as mobile and fixed line telephony[108]. They revoke and supersede the Data Retention (EC Directive) Regulations 2007 (SI/2199) which transposed the parts of Directive 2006/24 /EC relating to mobile and fixed telephony[109].A standard period of 12 months applies across the board meaning that internet communications data will have to be retained by notified public communication providers[110]. Part 11 of the Anti-terrorism, Crime and Security Act 2001 (ACTCA) already provided a legal basis for the retention of communications data in the UK for certain purposes. These regulations made the retention of communications data mandatory rather than voluntarily for the service providers[111].

4.1 The margin of appreciation.

A factor in determining if the measures imposed by the data retention directive are proportionate is the national implementation of the directive where the states are given a certain competency and a margin of appreciation. The contracting state has the competency to decide what grounds stipulates the access to data, which authorities are allowed to access the information, and how the authorization to retained data is given[112]. In the United Kingdom this is regulated through the Regulation of Investigatory Powers Act of 2000 (RIPA).The Human Rights act of 1998 Art.2 determines that a court or a tribunal must take in to account any judgment, decision, declaration or advisory opinion of the European Court of Human Rights[113], and Art 3 of the same act requires the court to interpret the primary legislation and subordinate legislation in a way which is compatible with the Convention rights[114]. Therefore when considering the proportionality of the data retention directive as a whole, it is important

[108] Home Office: Explanatory memoarandum to the data retention (EC directive) Regulations 2009 No.859. 1
[109] ibid
[110] Walker (n 56) 75
[111] idem (n 108)
[112] Directive 2006/24/EC, Art.4.
[113] Human Rights act 1998,s 2. (1)(a)
[114] Human Rights act 1998,s 3(1)

to see if the UK legislation is within the boundaries of the margin of appreciation that the ECtHR have traditionally granted the contracting states.

The ECtHR affords to the State a margin of appreciation when deciding whether an interference with an Article 8 right is justified under paragraph 2 of that provision. The margin of appreciation afforded to competent national authorities will vary according to the circumstances, the subject matter and its background[115]. Factors in determining if the measure is necessary in a democratic society will include the scope of the margin of appreciation traditionally given to the contracting states in regard to judgment by the ECtHR concerning access and use of data obtained from individuals by surveillance measures by the authorities.

In the judgment of *Klass and Others v Germany*[116], which concerned phone-tapping, The ECtHR agreed for the first time that the development within espionage and terrorism could legitimate that the states could use intrusive means such as secret surveillance of communication[117].In regard to the margin of appreciation of the state, the Court stated that: "*As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field (…) Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measure they deem appropriate*[118]*".*

Klass and Others v Germany implies that the states do have a certain margin of appreciation when it comes to what privacy infringing measures the government may use to pursue its national interests, but this margin of appreciation is not unlimited, there has to be a balance between the democratic values and core Human Rights principles. In the following, these

[115] Ursula Kilkelly, 'Handbook No. 1: The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights'(2001) Directorate General of Human Rights 32

[116] *Case of Klass and Others v Germany*, App No. 5029/71 (ECtHR 06/09/1978)

[117] Bruce (n 69) 17

[118] *Klass v Others* (n 116) para 49

principles will be assessed an further clarified using cases that have come up in the ECtHR. The case of *Liberty and Others v the United Kingdom*[119] emphasizes that the grounds for conducts have to be very precise and clear and that it does not give government officials a total discretion[120]. The judgment in *Weber and Saravia v Germany*[121] and the judgment of *Leander v Sweden*[122] shows there have to be proper safeguards in place; judicial control with the measure, monitoring measures, oversight and supervision as well as the destruction of data when it is not needed anymore[123].

4.2 Regulation of Investigatory Powers Act of 2000 (RIPA)

The access and use of retained communication data is in the UK regulated by the Regulation of Investigatory Powers Act of 2000 or RIPA. RIPA regulates five different types of surveillance: (i) interception of communications: telephone calls or contents of emails, (ii) intrusive surveillance: covert surveillance in residential premises or private vehicles, (iii) directed surveillance: covert surveillance in public place (iv) Covert Human Intelligent sources: informants and undercover agents and (v) communications data: any record of the communication but not the actual content of the communication[124]. The last mentioned is what this chapter will concentrate on. Communication is dealt with in Part (i) chapter 2 of RIPA. Section 22 set out the conducts for accessing the record of telephone calls and electronic communications. Section 25 lists which authorities that can access these records. In addition, part IV of the act lists the 'independent oversight', the control mechanisms; which is the 'communication commissioner', and the 'Investigatory Powers Tribunal'.

4.21 Grounds for granting access to communication data.

Section 22(2) of the RIPA act stipulates under which grounds the access to communication data might be given. The grounds for accessing retained communication data goes over a wide span from 'interests of national security', to the 'purpose of protecting public health'. The provision does not give any further elaborations about the content of the terms, but provides

[119] *Case of Liberty and Others v. The United Kingdom* App no 58243/00 (ECtHR 01/07/2008)
[120] Ibid para 80
[121] *Weber & Saravia* (n 52) para 115
[122] *Leander v Sweden* (n 42) para 65
[123] Bus, Crompton, Hildebrandt, Matakides: 'Digital Enlightenment Yearbook' (2012) IOV Press BV 28-29
[124] Gersch (n 96) 6

that obtaining communications data may be necessary for the purpose of preventing disorder, protecting public health, assessing or collecting tax or other charges payable to the government, or for the purpose of preventing, or mitigating (where applicable) death, injury or damage to a person's physical or mental health in an emergency; in the interests of public safety; or for any purpose which the Secretary of State specifies by order[125].

The terms used in RIPA is very broad and gives a big scope of discretion. The question is therefore if this can be said to be in 'accordance with the law' as required by ECHR art.8.

In the case of *Liberty and Others v The United Kingdom*[126] the ECtHR made it clear it was not prepared to accept terms such as 'State security' as a legal basis for the monitoring of large amount of communication traffic[127].

The background of the case was the 'troubles' in Northern Ireland, and British anti-terror measures which involved what the court described as 'generalized strategic monitoring or blanket monitoring of communications traffic, as opposed to the targeting of specific individuals[128]' .The United Kingdom had systems in place such as 'catch words' which would trigger the surveillance. Between 1990 and 1997 it was alleged that British authorities intercepted all telephone, facsimile and e-mail communications carried on microwave radio between two British Telecom radio stations in Wales and Cheshire. These links carried much of Ireland's telecommunications traffic. The court in its judgment found that this blanket monitoring granted to the executive 'unfettered discretion' as in theory everybody who received or sent communications within this time could have had their communications intercepted[129]; *"In their observations to the Court, the Government accepted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication*

[125] Clive Gringras: 'Legislative Comment: There is nothing new under the sun, or in the cloud' (2012) European Intellectual Property Review 73-74
[126] *Liberty* (n 119) para 64
[127] John Barry, 'The criminal justice(surveillance) Act 2009: An examination of the compatibility of the new act with article 8 of the European Convention on Human Rights' (2010) 2, COLR; Cork Online Law Review < http://corkonlinelawreview.com/editions/2010/CRIMINAL%20JUSTICE-BARRY.pdf > accessed 11/08 2012
[128] ibid
[129] ibid

intercepted (…)The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered[130]*".*

The court found that the British interception of communication act of 1985 was not specific as to what captured material was listened to or read, terms such as 'national security' and 'preventing and detecting serious crime' were too general[131] : "*In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law"*[132].

In conclusion the Court found that the relevant British laws were a breach of ECHR Art 8(1). The measure was not 'in accordance with the law'. This shows that the laws have to be precise enough, to give conduct to examine communications.

Liberty and others v the United Kingdom represented a blanket approach on surveillance, where telecommunications; communication data, was 'trawled' and surveillance of the content of these communications was triggered if certain words where used in the correspondence. The retention of communication data may work in a similar fashion. The directive imposes the entire populations' network, contacts and movement to be retained in databases, but rather than trigger words, the communication data itself may be the trigger mechanism. Communication data provides a detailed picture of the telecommunications, social environment, and movements of individuals[133]. The information value of traffic data can be, depending on the circumstances, equal to or exceed that of communication contents[134], in fact, because section 17 of RIPA makes evidence derived by 'communication content' inadmissible in court, communication data is mainly what law enforcement are interested in. It can therefore not be said that traffic data is typically less sensitive than content data, and it

[130] Idem (n 126)
[131] ibid (n 126) & Barry (n 127):
[132] *Liberty* (n 119) Para 69
[133] Breyer (n 4) 371
[134] ibid

is not justified to apply a lower level of legal protection to traffic data than to content data[135]. The definitions set out in RIPA of what is necessary grounds of accessing and using retained communication data is very similar to the terms that the ECtHR in *liberty* found too broad and vague to be 'in accordance with the law[136]'. Hence, there is reason to believe that the grounds for accessing traffic data in RIPA 22(2) are not in accordance with the law either. The directive combined with the broad terms in RIPA with the tool for accessing and using this data give the authorities a wide discretion to examine all forms for electronic communication.

4.22 Accessing communication data.

When an access to communication data is requested; an applicant in the public authority sets out an application for the requirement for communication data with an assessment of why the request is necessary and proportionate[137]. RIPA section 22(3) sets out that a 'designated person might grant authorization to grant access to retained communication data. The designated person is the senior officer in the public authority, which has the responsibility to assess the necessity and proportionality evaluation of the application, and authorize or refuse to authorize the acquisition of communication data[138]. The whole process is overseen by a senior responsible officer who is held accountable for the integrity of the process[139]. Once approved, the application goes to the technicians called 'the single point of contact' which acquires the data and passes it to the applicant[140].

This means that access to communication data is not given by a judicial authorization, but on basis of the discretion of the senior officer of the 'relevant authority'. In *Klass* it is implied that a judicial authorization is desirable, and "*The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper*

[135] ibid
[136] *Interception of Communications Act 1985, s 1-10*
[137] Regulation of Investigatory Powers Act 2000, s 22(3)
[138] Ibid, s 22(5)
Home Office, 'Draft Communications Data Bill, Privacy Impact Assessment', 'Existing safeguards - Regulation of Investigatory Powers Act 2000' 10-11
Available at: < http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-privacy-ia?view=Binary > (accessed 26/07 2012) 10
[139] ibid
[140] ibid

procedure"[141]. The current legislation in RIPA breaks with this principle, and hence it lacks guarantees to secure an independent, impartially and a proper procedure.

Anecdotal experience from criminal practitioners is that it is unusual to find cases where RIPA authorization is refused; prosecutions by benefits agencies and local authorities regularly make use of covert surveillance in routine cases[142]. Access to communication data is often requested. If we included the investigation of crimes, 500,000 official requests to access phone and email records were made in 2008 – the equivalent of one in 78 adults coming under some form of surveillance by the authorities in the United Kingdom[143]. No judicial control to access communication data will lower the threshold for people working in public authorities to requests access. This can lead to arbitrariness which not can be in 'accordance with the law' because it is not accessible or foreseeable what individuals working within authorities may put in the concept of proportionality. No judicial authorization, combined with the broad terms in section 22(2) that are the grounds for accessing communication data, give the people within the authorities an 'unfettered discretion' which can not be lawful in regard to ECHR art.8.

4.23 Delegated legislation.

The relevant public authorities that can access retained communications data is set out section 25(1) of the RIPA act. This includes the police and secret services, but also 'other relevant authorities' may also acquire access[144]. RIPA contains controversial provisions enabling delegated legislation[145] and paragraph (g) of the definition of 'relevant public authority' in section 25(1) permits the Secretary of State to add further public authorities to this list[146]. The list[147] that contains additional 'relevant authorities' which is granted access to communication

[141] *Case of Klass v Germany* (n 116) Para 56
[142] Gersch (n 96) 7
[143] Henry Porter and Afua Hirsch, 'The dangers of state surveillance' The Guardian (1 February 2010) <http://www.guardian.co.uk/commentisfree/henryporter/2010/feb/01/ripa-act-surveillance-authorities> accessed 17/07 2012
[144]Regulation of Investigatory Powers Act 2000, s 25(G)
[145] Gerch (n 96) 6
[146] Explanatory memorandum on the Regulation of Investigatory Powers (Communication Data) Order 2003 available at: < http://www.statewatch.org/news/2003/sep/RIP-memo-1.pdf> Accessed 03/08 2012.
[147] See further: Regulation of investigatory powers (Communication data) Order 2010, SI 2010/480. Available at < http://www.legislation.gov.uk/uksi/2010/480/pdfs/uksi_20100480_en.pdf >Accessed 11/08 2012

data is long and organizations that use RIPA for access to communication data is long; the count in July 2008 was 792 organizations, including 474 councils[148].

Organizations as diverse as the Royal Pharmaceutical Society and the Milk Marketing Board have been given powers to conduct covert surveillance[149]. This suggests that the development of RIPA has turned into a 'mission creep' where data is being used for other purposes than those for which they were originally collected, which is as a measure to fight serious crime and terrorism[150]. Complaints from the subjects of covert surveillance have included a nursery suspected of selling pot plants unlawfully, a family suspected of lying in a school application[151] and paperboys suspected of wrong paperwork[152].

4.24 Oversight & supervision.

In the case of *Weber and Savaria v Germany*, the ECtHR has accepted a far-reaching strategic surveillance of communication as long as the systems are subject to sufficient control[153]. Independent supervision empowered with substantial power has to be established in relation to all stages of interception and the establishment of reporting duties[154]. In *Leander v. Sweden* the safeguards contained in the Swedish personnel control system were found to be sufficient to fulfill the requirements Article 8, Para. 2. The Court attached much importance to the fact that the supervision of the proper implementation of the system was entrusted both to Parliament and independent institutions[155].

In RIPA, There are two bodies of 'independent oversight' that controls the process of requesting, authorizing and obtaining access to communication data. These are the Communications Commissioner[156] who oversees the interception of communication and

[148] Gerch (n 96) 6.
[149] Ibid 7
[150] Directive 2006/24/EC, Art.1
[151] Gersch (n 96) ; *Paton v Poole BC* (2000) IPT/09/01/C where the IPT ruled that this was not a proper purpose for surveillance and breached the family's right to privacy. (The IPT is the judicial body established to determine ECHR and HRA based claims against the conduct of the agencies and public authorities with RIPA powers.)
[152] Gersch (n 96) 6
[153] *Case of Weber & Saravia* (n 52) Para 115
[154] Ibid & Bus, Crompton, Hildebrant, Matakides (n 123)
[155] Leander v Sweden (n 42) Para 65 , Kilkelly (n 115) 37
[156] Regulation of Investigatory Powers Act 2000, s 57

produces a detailed report[157], which is presented to the House of Commons annually. Also, the Investigatory Powers Tribunal (IPT) was set up by RIPA to provide for review by a judicial body of public authorities under RIPA. This tribunal has the power to investigate complaints and if they are upheld, it can quash authorizations, order the destruction of records and award financial compensation and do therefore have some substantial power[158]. The Communication commissioners do give some oversight entrusted to the parliament. However, According to the commissioners' report 494,078requests for communication data were made in 2010 and only noted 895 errors during the reporting year[159]. The Investigatory Powers Tribunal received the same year 164 complaints[160]. The massive number of requests for communication data and the small number of complaints and errors indicates either that system and legislation that gives access and disclosure to communication data works smoothly, and that the access and disclosure of communication data is very seldom being abused. It might on the other hand indicate a system, where the nature of this systematic mass retention of data makes the oversight and supervision mechanism of the system insufficient considering the enormous amount of requests for traffic data where hundred thousands of requests are made annually. Meaningful supervision and compliance is difficult to achieve when more resources are put into monitoring of data than its regulation. Unless it is fully resourced, any regulator cannot do more than scratch the surface to ensure compliance with the rules[161].

4.3 New legislation

The UK government are now to introduce new laws in this field. The Queen's speech on the 9th of May 2012 included the following: 'My government intends to bring forward measures to maintain the ability of the law enforcement and intelligence agencies to access vital

[157]See: report of the Interception of Communications publisher 2011. Presented to the United Kingdom parliament pursuant to s 58(6) of the Regulation of the Investagory Powers Act 2000.
Available at: < http://www.intelligencecommissioners.com/docs/0496.pdf > accessed 11/08 2012
[158] Home office, 'Draft Communications Data Bill. Privacy Impact Assesment, Existing safeguards' (2012) Regulation of Investigatory Powers Act 2000 (RIPA). p 11.
Available at: < http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-privacy-ia?view=Binary >(accessed 26/07 2012)
[159] Report of the Interception of Communications (2012) Presented to the United Kingdom parliament pursuant to s 58(6) of the Regulation of the Investigatory Powers Act 2000.
Available at: <http://www.intelligencecommissioners.com/docs/0496.pdf> (accessed 12/08/2012) 28,30
[160] Interception of Communications Commissioner, Annual Report of (2010) Available at: <http://www.ipt-uk.com/docs/Interception_of_Communications_2406.pdf> (accessed 03/08 2012) 54.
[161] Gersch (n 96) 8

communications data under strict safeguards to protect the public, subject to scrutiny of draft clauses[162],

A draft bill was published on Thursday, 14th June[163] and a joint committee will report on the bill by the end of November 2012. It will also be looked at by two other committees. The bill is expected to be ready after 7th Jan 2013. It is expected to be announced in the Queen's Speech in May 2013 and debated in the 2013-14 parliamentary session[164]. As stated in Under Part 1 of the Bill, individual Communication Service providers' may be given a notice by the Secretary of State to obtain, process and retain communications data they would not ordinarily hold for their own business purposes e.g. data relating to new or innovative communications services[165]. In practice the new law will be allowing police and security services to extend their monitoring of the public's email and social media communications, the Home Office has confirmed[166]. Examples of information that the UK government now wants the communication service providers to store for a period of 12 months in addition to what is already retained is: who communicates with each other on social mediums like Facebook and Twitter, who you have contact with on online games, and which websites you visit[167].

The purpose of this is to make it more difficult for people to evade the directive, and to close the gaps between uptake in the use of new communication services like webmail, social networking and gaming services, which are almost entirely provided by companies located

[162] Queens speech: available at http://www.cabinetoffice.gov.uk/queens-speech-2012

[163] Draft Communications Data Bill| Presented to Parliament| June 2012 |Cm 8359
Available at: <http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf> (accessed 28/07 2012)

[164] The open rights group, 'Draft publication and next steps'
http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill#cite_note-0 (Accessed 12/08 2012)

[165] Home Office, 'communications data legislation impact assessment' (11/05 2012)
Available at: http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-ia?view=Binary accessed 28/07 2012

[166]Robert Booth, 'Government plans increased email and social network surveillance' (the Guardian, 1 April 2012) Available at: <http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance> accessed: 28/07 2012

[167] Nicholas Watt and Rajeev Syal, 'Nick Clegg pledges open hearings over web surveillance plans' (the Guardian, 3 April) Available at: <http://www.guardian.co.uk/politics/2012/apr/03/nick-clegg-open-hearings-surveillance?intcmp=239> accessed 12/08/2012

Alan Travis, 'Online privacy: Home Office to write blank cheque for 'snoopers' charter' (The Guardian) <http://www.guardian.co.uk/world/2012/jun/13/online-privacy-legislation-internet-phone-data> accessed 12/08 2012

overseas[168]. Whether this will help fighting crime and making the society safer is yet to be seen, but it will impose further infringement of individuals' privacy.

4.4 Summary and Concluding remarks.

The European Court of Human Rights have traditionally given the States a broad margin of appreciation when it comes to the national discretion of implementation of measures to protect the national security and defend criminality; however this limit is not unlimited and have to be balanced with democratic values and human right principles. The terms set out in RIPA are incompatible with these values and principles. The reasons authorities might access communications data retained from communication service providers is vague and general, and this gives the relevant authority an unfettered discretion to decide when to request access for communication data; the case of *Liberty and others v the United Kingdom* shows that the ECtHR demands precise and clear legislation.

There is no juridical control on accessing traffic data; the authorization to access retained communication data is given by senior officer of a relevant authority, based on this persons discretion of what is considered proportionate. These factors combined with the delegated legislation that gives hundreds of different councils and agencies access to communication data, and insufficient control and overview leads to a state of arbitrariness that is not 'in accordance with the law' nor 'necessary in a democratic society'.

The British laws on access and use of retained communication data are already going further than what the directive imposes the contracting states to do, and goes outside of the States margin of appreciation. However, The United Kingdom is now reconciling the legislation. When the existing laws in RIPA are already dubious in regard to civil liberties and privacy, the new proposals takes this a step further. Some time ago, Richard Thomas, the Information Commissioner, expressed concern that the UK was "sleep-walking into a surveillance society". More recently, he said he "is worried that we are in fact sprinting towards a surveillance society"[169]. There are reasons to believe that this is in fact what is happening. The

[168]Home Office (n 165) 5

[169] House of Commons, Home Affairs Committee, 'A Surveillance Society? Oral and written evidence'. Fifth report of Session 2007-08,186.

forthcoming Communication Data bill will represent the most significant piece of legislation of covert surveillance that the United Kingdom has ever seen[170].

The United Kingdom have been one of the states that have lobbied the hardest to get the European Union to adopt the directive[171], and is a nation that have implemented this directive in a way that breaches fundamental rights and even want to take this even further, with putting further surveillance measures in force. It can be said that it is ironic that the United Kingdom, who historically have been a lantern of liberty when continental Europe have been gloomy and under oppressing regimes, have taken this direction, when the Constitutional Courts in nations who have had historical ties to totalitarian regimes have found the directive to be incompatible with their respective constitutions. Maybe it is when one first has experienced to live in suppression that one understands the value of defending the political framework democracy is built on. [172]

[170] Gersch (n 96) 9
[171] Walker (n3) 75.
[172] Hammerlin (n3) 92

Chapter 5: Norwegian implementation of the directive.

The directive applies both to Norway and the United Kingdom. Because the directive imposes the same minimum requirements for the States to retain communication data, the basics requirements when it comes to data retention are the same in Norway as in the United Kingdom. However there are some differences lying in the national implementation where the states have discretion. The United Kingdom have mainly a different approach to Norway on what procedures are to (i) be followed in order for the authorities to gain access and the use of the retained data, and (ii) the length of time the communication service providers are obligated to store the data.

5.1. Background

After the judgment in ECJ of Ireland v European Parliament and Council of the European Union[173] when an application for annulment of the Directive was rejected on the basis that the Directive properly sought to limit national disparities which might either affect fundamental freedoms or market competition[174], it was clear once and for all that the directive was relevant for the European Economic Community, and therefore would also apply to Norway who is not a member of the European Union.

In Norway the data retention directive have created a lot of discussions, and after a period of heated public debate the plans to implement the data retention directive in Norwegian law was approved with the slightest of margins in the parliament on the 4 April 2011 with 89 votes in favor of the implementation of the directive and 80 against. According to plan it was to go into force on the 1 of April 2012, but this was postponed until the 1 of July. The directive was then further postponed until January 2013[175] and it is still uncertain if this deadline will be met[176]. In a report made on behalf of the Norwegian Department of Communication (Samferdselsdepartementet) it was made clear that the government have no idea how much the directive is going to cost, nor how to resolve the issues on who will bear the expenditures

[173] *Ireland v European Parliament, Council of the European Union* (n 11)
[174] Walker (n 56) 75 para 2.75
[175] Arild Færaas, 'IKT-bransjen vil utsette datalagringsdirektivet i tre år' ("The Communication Service providers wish to postpone the data retention directive for 3 years") (Aftenposten, 18 April) available at <http://www.aftenposten.no/nyheter/iriks/IKT-bransjen-vil-utsette-datalagringsdirektivet-i-tre-ar-6808486.html> accessed 12/08/2012
[176] ibid

of the directive[177]. Many private Norwegian organizations are deeply concerned about the impact the directive has on privacy, and a group lead by the former director of the Norwegian data inspectorate have started fundraising to bring the directive to the Norwegian Supreme Court (Høyesterett) and if necessary all the way to the ECtHR in Strasbourg[178]

5.2. Changes in Norwegian legislation.

The implementation of the data retention directive in Norway will be done through changes in existing national legislation[179]. The major changes in Norwegian legislation to implement the directive will be done through the "law relating to legal procedure in criminal cases" (Straffeprossessloven[180]) and through the "law relating to electronic communications" (Ekomloven)[181]. The changed provisions in 'Straffeprossessloven' will concern the legal procedures for access and use of retained data. While the obligations for the communication service providers to store communication data is regulated through 'Ekomloven'.

The new legislation will require the communication service providers to retain communication data for a period of 6 months for: 'The investigation, detection and prosecution of serious criminal offences'. Those are offences that qualify for a specified number of years of imprisonment. Disclosure of communication data can only be given by the court, if it must be assumed that the information given is of vital importance for a criminal investigation[182].

[177] Report from committee appointed by the Norwegian Justice department, and Communication department 'available at:
<http://www.regjeringen.no/Upload/SD/Vedlegg/rapporter_og_planer/2012/rapportkostnadsfordelingsutvalgetdld.pdf> (accessed 7/8 2012)

[178] Sverre Steen, 'Motstandere av datalagringsdirektivet vil ta saken til Høyesterett og Strasbourg' ("Opponents of the Data Retention Directive will take the case to the Supreme Court and the Strasbourg") (Nationen 02 April 2012) available at:
<http://www.nationen.no/2012/02/02/nyheter/datalagringsdirektivet/dld/georg_apenes/anders_brenna/7226281> Accessed 07/08 2012

[179] Lov 2011-04-15 nr 11: Lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) Part. I

[180] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (Straffeprosessloven).

[181] Lov-2003-07-04-83 Lov om elektronisk kommunikasjon (ekomloven).

[182] Ibid (n 180) (n 181)

5.3 Differences between UK and Norwegian approach on the directive.

5.31. Retention time.

The retention period is shorter in Norway than in the United Kingdom. In Norway communication data is retained for a period of 6 months while in the UK it is 12. The UK government justifies this retention period by reference to a two-week survey undertaken on behalf of ACPO in 2005 which showed there had been 231 requests for data aged between six and twelve months, with 60 percent of the cases relating to murder or terrorism[183]. In Norway, the consideration to privacy has weighed more than the consideration to the value it has on investigation. A study which was included in the impact assessment to which the European Commission as well as the Presidency of the European Council, attached importance, demonstrated that overall, traffic data of up to 1 year was required by law enforcement agencies. Longer retention periods were found to provide little or no added value to law enforcement authorities[184]. Accordingly, any retention period greater than 1 year was considered disproportionate[185]. This means that the Norwegian retention period is more proportionate than that of the UK.

5.32. Access and disclosure to data.

As explained in chapter 4, the United Kingdom's implementation of the directive, needs no judicial authorization, and there is no specifications of the offence that grants the authorities access, just terms such as 'national security'. There is delegated legislation and hundreds of different councils that can request and access communication data. In the Norwegian legislation, certain specified types of criminality are listed, and they might qualify for certain penal consequences which might give the law enforcement authorities access to retained data if there is 'reasonable grounds to suspect' (Skjellig grunn til mistake) a criminal offence. In this lies a probability assessment. 'Reasonable grounds for suspicion' means that it is a higher probability that the suspect have committed the offence, than that he has not[186]. This

[183] Home Office, 'Transposition of Directive 2006/24/EC' (London, 2008) para 5.5
Walker (n 56) 75 para 2.77
[184] Maras (n 87) 358
[185] ibid
[186] NOU 2003: 18 'Mistankekravet for bruk av tvangsmidler'. (Norwegian legislation preparatory work, Suspicion requirement for the use of coercive measures) available at:

consideration of probability is done by a court which issues a warrant to the law enforcement authorities if it finds the requirements to be met. Hence, there is no delegated legislation for the Norwegian implementation of the directive, as there is Court control and access can only be given to the police if there is reasonable grounds for suspicion.

5.4 Summary and Concluding remarks.

It is clear that in the Norwegian government's approach when implementing the directive, consideration of individuals' privacy have weighed heavier than the principle has done in the United Kingdom, where the efficiency-principle weights heavier. The advantage of the Norwegian approach is that it protects the citizens from arbitrariness of the authorities. The advantage of the British approach is that easy access to the data retained will make the directive a more efficient tool for law enforcement than in Norway, as a court order is a process that takes time. In Norway there is no delegated legislation, which lowers the chances of a 'mission creep' whereas in the United Kingdom we see that retained communication data is already being used for other purposes than solely fighting serious crime. In conclusion the Norwegian laws for accessing and using the retained data are compatible with the fundamental human rights enshrined in Art.8, while the British approach is not.

<http://www.regjeringen.no/nb/dep/jd/dok/nouer/2003/nou-2003-18/9/3/1.html?id=371125> accessed 12/08 2012

Chapter 6: Conclusions.

We have seen that the data retention directive impose problems with regard to the fundamental human rights which is enshrined in the European Convention of Human Rights Article 8; the right to respect for private life. The blanket mass retention of communication data is an interference with the individuals' right to privacy and needs to be justified. However, this piece of work has showed that what the data retention directive imposes is a disproportionate measure and hence is not justified.

The combination of the case of *S and Marper v the United Kingdom* and ECtHR judgments concerning surveillance measures shows that the directive will have big problems passing a proportionality assessment in the Strasbourg court. Furthermore, it is not effective because criminals know how to evade it and this can actually have a negative effect on police investigation, there is the risk of leaks of data, the directive is an expensive affair, and what it does is putting an entire population under suspicion which may have a negative impact on society and democracy as a whole. Blanket mass retention of data represents itself a disproportionate measure, but the United Kingdom's laws of accessing and using retained data represents a further violation of human rights. The terms used in the legislation to access data is too broad to be in accordance with the law, there is no juridical control and it is totally based on the discretion of the senior officers in the relevant authorities. Furthermore, the scope of the mass retention of communication makes the supervision of the system insufficient. The delegated legislation in the UK laws represents a further danger in the fact that it can lead to a 'mission creep' where the retained data is used more and more for other purposes than preventing crime and terrorism. Even though the directive itself represents a disproportionate measure that breaches the human right of privacy, in Norway there is at least the juridical safeguard that a court will control and decide when access to data should be granted. The United Kingdom should be considering changing its legislation in the same direction because the way the system works today is based on arbitrariness and state officials have way too broad discretion to snoop on anyone. However, the major problem between the directive and Human Rights lies with the principle of mass retention as a whole.

Bibliography:

I. Books:

Jocahim Hammerlin: 'Terror & demokrati. Fra 11.september til 22' Juli. Oslo (2011).Forlaget manifest AS

Ursula Kilkelly : 'Handbook No. 1: The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights'(2001) Directorate General of Human Rights

Bus, Crompton, Hildebrandt, Matakides: 'Digital Enlightenment Yearbook' (2012) IOV Press BV

Paul Craig & Gráinne de Búrca. 'EU Law – text, cases and materials'. (2011) Oxford university press

Clive Walker: 'Terrorism and the Law' (2011) Oxford University Press

Emmerson & Ashworth 'A Human Rights and Criminal justice' London (2001) Swet and Maxwell,

O' Hara, Kieron and Nigel Shadbolt: 'the spy in the coffee machine'(2008) Oxford: oneworld publications

Alex Deane. 'Big brother watch: the state of civil liberties in modern Britain. London (2010) Biteback Publishing

John Kampfner 'Freedom for sale: How we made our money and lost our liberty' (2010) Pocket books

Dominic Raab: 'the assault on liberty: what went wrong with rights (2009) London: Fourth Estate

II. Journal articles:

Patrick Breyer' Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. European law review, vol. 11 no.3, May 2005

de Vries, Bellanova & de Hert, 'Proportionality overrides Unlimited Surveillance: The German Constitutional Court Judgment on Data Retention' (May 2010) CEPS 'Liberty and Security in Europe

Marie-Helen Maras: 'From targeted to mass surveillance: is the EU data retention directive a necessary measure or an unjustified threat to privacy' in 'New Directions in Surveillance and Privacy'. Willan Publishing (2009)

Jon Wessel-Aas. 'Datalagringsdirektivet – er dets krav om lagring av trafikkdata forenelig med den europeiske menneskerettighetskonvensjonen?' (2010) Nordisk årbok i rettsinformatikk, 136. (Journal article on the data retention directives compability with the ECHR)

Ingvild Bruce: 'Datalagringsdirektivet – en menneskerettskrenkelse eller –forpliktelse' (2010) Lov og Rett 2010-6 22 (Journal article on the data retention directive)

Marie-Helen Maras: 'The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?' (2012) 33 European Journal of Law & Economics 449

Adam Gersch: 'Covert surveillance – a snoopers' charter' (2012) 5th Archbold Review

Clive Gringras: 'Legislative Comment: There is nothing new under the sun, or in the cloud' (2012) European Intellectual Property Review

John Barry, 'The criminal justice(surveillance) Act 2009: An examination of the compatibility of the new act with article 8 of the European Convention on Human Rights' (2010) 2, COLR; Cork Online Law Review Available at: <http://corkonlinelawreview.com/editions/2010/CRIMINAL%20JUSTICE-BARRY.pdf > accessed 11/08 2012

III. Reports:

The Office for National Statistics (ONS) Social Trends 41: e-Society. Available at: <http://www.ons.gov.uk/ons/search/index.html?pageSize=50&sortBy=none&sortDirection=none&newquery=social+trends+41> (accessed 9/8 2012)

Report from the Commission to the council and the European Parliament – Evaluation report on the Data Retention Directive (Directive 2006/24/EC) Brussels 18.4.2011

Council of Europe report: 'Case law of the European Court of Human Rights concerning the protection of personal data' (DP 2009 Case law)

Available at: <http://www.coe.int/c/document_library/get_file?uuid=ec21d8f2-46a9-4c6e-8184-dffd9d3e3e6b&groupId=10227> (accessed 12/08/2012) 14

Report from the Human Genetics commission 2009. Available at: <http://www.hgc.gov.uk/Client/document.asp?DocId=226> (accessed 11/08 2012)

Joint Committee Report on Human Rights. 'Enhancing Parliament's role in relation to human rights judgments' Great Britain Parliament: 15th report of 2009-2010

Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics: available at:

<http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf> (accessed 01/08 2012

Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)

Home Office, 'Draft Communications Data Bill, Privacy Impact Assessment', 'Existing safeguards - Regulation of Investigatory Powers Act 2000'

Report of the Interception of Communications publisher 2011. Presented to the United Kingdom parliament pursuant to s 58(6) of the Regulation of the Investagory Powers Act 2000.
Available at: < http://www.intelligencecommissioners.com/docs/0496.pdf > accessed 11/08 2012

Home office, 'Draft Communications Data Bill. Privacy Impact Assesment, Existing safeguards' (2012) Regulation of Investigatory Powers Act 2000 (RIPA). p 11.

Report of the Interception of Communications (2012) Presented to the United Kingdom parliament pursuant to s 58(6) of the Regulation of the Investigatory Powers Act 2000.
Available at: <http://www.intelligencecommissioners.com/docs/0496.pdf> (accessed 12/08/2012) 28,30

Interception of Communications Commissioner, Annual Report of (2010) Available at: <http://www.ipt-uk.com/docs/Interception_of_Communications_2406.pdf> (accessed 03/08 2012)

Home Office, 'communications data legislation impact assessment' (11/05 2012)
Available at: http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-ia?view=Binary accessed 28/07 2012

House of Commons, Home Affairs Committee, 'A Surveillance Society? Oral and written evidence'. Fifth report of Session 2007-08,186

Report from committee appointed by the Norwegian Justice department, and Communication department 'available at:
<http://www.regjeringen.no/Upload/SD/Vedlegg/rapporter_og_planer/2012/rapportkostnadsfordelingsutvalgetdld.pdf> (accessed 7/8 2012)

IV. News articles

Henry Porter and Afua Hirsch, 'The dangers of state surveillance' The Guardian (1 February 2010) <http://www.guardian.co.uk/commentisfree/henryporter/2010/feb/01/ripa-act-surveillance-authorities> accessed 17/07 2012

Robert Booth, 'Government plans increased email and social network surveillance' (the Guardian, 1 April 2012) Available at: <http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance> accessed: 28/07 2012

Nicholas Watt and Rajeev Syal, 'Nick Clegg pledges open hearings over web surveillance plans' (the Guardian, 3 April) Available at: <http://www.guardian.co.uk/politics/2012/apr/03/nick-clegg-open-hearings-surveillance?intcmp=239> accessed 12/08/2012

Alan Travis, 'Online privacy: Home Office to write blank cheque for 'snoopers' charter' (The Guardian) <http://www.guardian.co.uk/world/2012/jun/13/online-privacy-legislation-internet-phone-data> accessed 12/08 2012

Arild Færaas, 'IKT-bransjen vil utsette datalagringsdirektivet i tre år' ("The Communication Service providers wish to postpone the data retention directive for 3 years") (Aftenposten, 18 April) available at <http://www.aftenposten.no/nyheter/iriks/IKT-bransjen-vil-utsette-datalagringsdirektivet-i-tre-ar-6808486.html> accessed 12/08/2012

Sverre Steen, 'Motstandere av datalagringsdirektivet vil ta saken til Høyesterett og Strasbourg' ("Opponents of the Data Retention Directive will take the case to the Supreme Court and the Strasbourg") (Nationen 02 April 2012) available at: <http://www.nationen.no/2012/02/02/nyheter/datalagringsdirektivet/dld/georg_apenes/anders_brenna/7226281> Accessed 07/08 2012

'Brown apologises for records loss'< http://news.bbc.co.uk/1/hi/uk_politics/7104945.stm#graphic> (BBC, 21 November 2007) accessed 01/08/2012

'Personnel records stolen from MoD' <http://news.bbc.co.uk/1/hi/england/gloucestershire/7639006.stm> (BBC, 27 September 2008) accessed 12/08/2012

Tom Espiner, 'Local councils report only 55 of 1,035 data losses' (ZDnet November 23, 2011) <http://www.zdnet.com/local-councils-report-only-55-of-1035-data-losses-3040094491> accessed 12/08 2012

Charles Arthur & Keith Stuart ,' PlayStation Network users fear identity theft after major data leak' (the Guardian, 27 April 2011) <http://www.guardian.co.uk/technology/2011/apr/27/playstation-users-identity-theft-data-leak?INTCMP=SRCH> accessed 12/08/2012

Digital Rights Ireland, 'Press Release on German Data Retention Decision' (March 3rd, 2010) <http://www.digitalrights.ie/2010/03/03/press-release-on-german-data-retention-decision> accessed 12/08/2012

V. Other material

Her Majesty the Queens speech: available at http://www.cabinetoffice.gov.uk/queens-speech-2012

The open rights group, 'Draft publication and next steps' http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill#cite_note-0 (Accessed 12/08 2012)

Dr Breyer and Arbeitskreis Vorratsdatenspeicherung (Working group on Data retention), 'Civil society letter to MEPs on mandatory data retention' Available at: <http://www.statewatch.org/news/2010/dec/eu-mandatory-data-retention-civil-society-letter-10.pdf> accessed 12/08/2012

European Data Protection Supervisor Press release: 'Data Retention Directive fails to meet data protection requirements' (1 June, 2011)
Available at: <http://www.edri.org/edrigram/number9.11/data-retention-directive-failure-edps>

Explanatory memorandum on the Regulation of Investigatory Powers (Communication Data) Order 2003

available at: < http://www.statewatch.org/news/2003/sep/RIP-memo-1.pdf> Accessed 03/08 2012.

Poll on data retention (in German): <http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf> accessed 12/08/2012