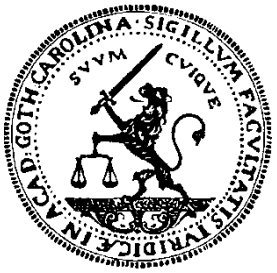

FACULTY OF LAW
Lund University

Aschtar Yakob

Blanket Retention of Electronic Communications Traffic Data and the Right to Respect for Private Life - Sweden in Focus

Master thesis
30 credits

Supervisor: Håkan Hydèn

Master´s Programme in International Human Rights Law

Spring 2011

Contents

Summary

This thesis concerns Directive 2006/46/EC and its compliance with the European Convention on Human Rights and Fundamental Freedoms. The thesis uses Sweden as an example, and mainly analyses the shortcomings in Swedish legislation on how traffic data may be accessed by law enforcement authorities, finding that the regulations under the Swedish Electronic Communications Act breaches Article 8 and 13 of the Convention. The author shares the opinion of several Swedish bodies that the changes suggested in SOU 2005:38 concerning the regulations on access to the retained data should be implemented, so that the access is regulated only under the Swedish Code of Judicial Procedure. The thesis also describes the triangular relationship between the EU, the Convention and the Member State, and the changes to this relationship which are brought about by the Lisbon Treaty. Furthermore, the scenario of blanket retention of traffic data of all European citizens is analyzed from a sociological point of view, where the thesis looks into the mechanisms behind state surveillance as social control and the detrimental effects it may have on the individual and the society as a whole. In this context there is also a conclusion from a legal point of view, where it is argued that the European Commission has failed to provide evidence of a certain quality and quantity on the necessity of blanket retention, raising doubts concerning the proportionality, and, in effect, the legality of the Directive. The final conclusion is that blanket retention of traffic data should be replaced with the so called ‘quick-freeze’ method which was already used prior to the Directive, and that the Directive should be repealed or amended so that the conditions for the access to the traffic data is regulated in a satisfactory manner.

Sammanfattning

Detta examensarbete rör direktiv 2006/46/EG och dess överensstämmelse med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Examensarbetet använder Sverige som ett exempel, och analyserar främst lagen (2003:389) om elektronisk kommunikation och dess tillkortakommanden vad gäller brottsbekämpande myndigheters tillgång till lagrade trafikuppgifter. Analysen utmynnar i att finna att Sverige bryter mot artikel 8 samt 13 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Författaren delar flera remissinstansers åsikter om att förändringarna som föreslås i SOU 2005:38 rörande regleringar kring tillgång till trafikuppgifter bör förändras på så sätt att de enbart skall regleras i rättegångsbalken. Uppsatsen går också bitvis in på den triangulära relationen mellan EU, Europeakonvention och en medlemsstat, samt de förändringar som kommer till stånd i och med Lissabonfördraget. Vidare ägnas stora delar av uppsatsen till att analysera automatisk lagring av trafikuppgifter från alla individers kommunikationer ur ett sociologiskt perspektiv, där mekanismerna bakom och konsekvensarna av statlig övervakning som social kontroll tas upp. Denna diskussion innehåller ändock juridiska slutsatser i det att direktivets legalitet ifrågasätts då europeiska kommissionen, enligt författaren, inte har presenterat tillfredställande bevis för att behovet av datalagring verkligen står i proportion till de konsekvenser sådan övervakning kan ha för individen och samhället i stort. Således dras slutsatsen att obligatorisk datalagring bör ersättas av s.k. ’quick-freeze’ metod samt att direktivet bör upphävas eller ändras så att tillgången till data regleras på ett tillfredställande sätt.

Preface

I decided on the topic for this thesis after noticing the media attention that the proposed Swedish implementation of the Directive gained, where the human rights perspective and the European Convention on Human Rights and Fundamental Freedoms received much attention. As a masters student in international human rights law, the media coverage naturally caught my interest. This thesis attempts to clarify the situation brought up by blanket retention of communications traffic data from a human rights perspective.

Thank you to my supervisor Håkan Hydén and my friend Anders Holmström for clarifying elements of this topic of which I previously had no understanding. Thank you also to Amin Parsa for your sharing your thoughts and ideas!

Abbreviations

BRU	*Beredning för Rättsväsendets Utredningar*. It is a Commission of Inquiry, which has as its object to investigate the possibilities to make judiciary processes in Sweden more effective and of higher quality. Has written several Reports, among them Report 2005:38 *"Tillgång till elektronisk kommunikation i brottsutredningar m.m"* .
ECHR	European Court of Human Rights
EU	European Union
FRA	The Swedish National Defence Radio Establishemnt (*Försvarets Radioanstalt*)
IPRED	The Intellectual Property Rights Enforcement Directive
IPT	The Investigatory Powers Tribunal
ISP	Internet Service Provider
ISSJ	International Social Science Journal
MLR	Modern Law Review
OJ	Official Journal of the European Union
PTA	The Swedish Post and Telecom Agency (*Post- och telestyrelsen*)
SOU	Swedish Government Official Reports (A Report is made by a Commission of Inquiry subsequent to a demand from the Swedish Government)
TEU	Treaty on the European Union

TFEU	Treaty on the Functioning of the European Union

1 Introduction

'We must move forward, not backward. Upward, not forward!
And always twirling - twirling, twirling towards freedom.'
-
Kodos impersonating President Bill Clinton in an attempt to rule mankind
The Simpsons S08E01

1.1 Thesis Question

The overall question this thesis will attempt to answer is: Does the retention of electronic communications traffic data pursuant to Directive 2006/24/EC sufficiently respect the private life of European Citizens? This has been done by examining the retention's compliance with the right to private life under Article 8 and the right to an effective remedy under Article 13 of the European Convention on Human Rights ('The Convention' alt 'the ECHR'). In order to illustrate it in a more concrete way, I have chosen to look closely at the Swedish implementation of the Directive and examine its compliance with the Convention Rights.[1] When reading this thesis one will find that it seems as though the implementation can be divided in two parts: firstly the legality of the actual storing of specific data, and secondly the legality on the accessing of the data. Furthermore, one will find that for the first part, the Member States have had little discretion on how to implement the Directive; the guidelines are clear and rather detailed. For the second part, the Member States were given full discretion by the Directive, meaning that the Member State would have complete power over when and how the data may be accessed by its law enforcement authorities.

When I started writing, I realized that the thesis would fall flat if it entailed no attempt to examine underlying mechanisms behind surveillance. What inspires States to monitor their citizens? What indications are there in the area of legislation on surveillance in Sweden; is there an increased political will to surveil, and if so is there a focus or a vast array of simultaneous committee inquiries?

1.2 Methodology and Material

This thesis mainly uses a traditional legal method to investigate Sweden's compliance with the Convention. The sources I have used are legislation from the EU and domestic level. As always when investigating a legal

[1] The author is aware of the court judgments regarding data retention in Germany, Romania and Czech Republic have claimed their national implementations of the directive to be un-constitutional. I will not discuss this matter in my thesis, since my topic is narrowed down to the implementation in Sweden. While the foreign cases may have some good points, I am not knowledgeable enough in the language, law or the constitution to justify a discussion regarding the case in this thesis. This is not a comparative study.

situation in Sweden, there is much emphasis on the *travaux préparatoires* to the various Swedish legislation which this thesis brings up. As regards the Swedish legislation, the *travaux préparatoires* is an important source when analyzing the law. The other major source has been case law from the Court of Justice and the European Court of Human Rights ('the Court'). Furthermore the thesis looks at the critique from EU institutions as well as Swedish bodies of referrals, which are later used to add authority to the analysis which appears in chapter 10. Scholarly books and articles have been used to deepen the knowledge on the rights under the Convention.

Chapter 3 and 9 does not contain the regular discussions one would find in a legal thesis. The methodology used here is a social science method. The sources here are exclusively books and articles.

1.3 Outline

In Chapter 2, I have presented definitions of some key words which might be difficult to understand as a novice in the area. Chapter 3 attempts to present the idea of privacy and how scholars have attempted to define it. Chapter 4 deals with the actual legal protections the individual enjoys to safeguard her privacy in Sweden. One will see that the protection for the Swedish citizen is the same as for any European, due to the close relationship with the Convention and the EU in the matter but also because of the new status of the Charter of Fundamental Rights of the European Union. In Chapter 5, the Directive is presented. The regulation is accounted for, and critique from the most influential bodies is presented. In Chapter 6 I goes on to present how Sweden has proposed to implement the Directive. Yet again, critique from influential bodies is presented, as well as the government's response. Chapter 7 can be seen as a continuation of chapter 6. This chapter compares the two different regulations through which the Swedish law enforcement authorities may gain access to the data which is retained. Here the reader will find that one of the regulations is lacking in quality, something which has been pointed out for years by various Swedish bodies. In chapter 8 we finally get to go into the Convention and the standards it sets out for surveillance measures under Article 8 and the right to respect for private life through the case law of the Court. Article 13, *i.e.* the right to effective remedy, is also accounted for. There is a brief presentation of the freedom of expression under Article 10 of the convention; there will be no analysis of the compliance with this right. Rather, it is presented as part of the overall effect that the increasing surveillance may have on the individual and, in effect, the democratic society. Chapter 9 attempts to explain the mechanism behind state surveillance. There is a general account here, as well as a Swedish focus which aims to present the increase of surveillance in Sweden through some examples, as well as pointing to the disarray of legislation in the field of surveillance and privacy. Chapter 10 contains the analysis on traffic data retention pursuant to the Directive and Sweden's compliance with the Convention rights under Article 8 and 13, and lastly some final words on what could, and, in the author's opinion, should, happen with the Directive.

2 Terminology

Here are the definitions of certain terms as understood from Swedish law:

"Electronic messages" is defined as all information which is exchanged or transferred between a limited amount of parties through a publically accessible electronic communication service, except information which is transferred as part broadcasts of radio- or TV-programs directed towards the public through an electronic communications network if the information cannot be connected with the individual subscriber or user of the information.

"Handling or processing of messages" means the exchange or transfer of an electronic message.

"Traffic data" is defined as a piece of information processed in order to transport a communication through an electronic communications network or for invoicing for used services.

"Retention" means the collecting of the data. "Blanket retention" means that the data is collected from the communications of all citizens, indiscriminately.

Throughout this thesis, one will find the words propositions and SOU. These two are the most important elements of *travaux préparatoires* in Sweden. According to the Swedish legal system, *travaux préparatoires* enjoy a high status when interpreting the law - if something needs an explanation, one must first go to the *travaux préparatoires*. Propositions are shortened as 'prop.', and are the final propositions for new legislation. SOU is short for *Statens Offentliga Utredningar*, meaning Swedish Government Official Report. I will use the Swedish abbreviation of SOU throughout the thesis, with one exception: the SOU 2007:76 *Lagring av Trafikuppgifter för brottsbekämpning* will be called the Traffic Data Inquiry. It is my translation of *Trafikuppgiftsutredningen* which is the name it has been given when discussing it in Sweden. SOUs are made by commissions of inquiry upon requests by the Swedish government when it needs an inquiry on a specific issue. When the reports are made for investigating possibilities for new legislation, the final report will be referred to public bodies, NGOs, and other bodies, for consideration, in order to obtain critique regarding the legislation that had been suggested by the investigator. After this procedure, a refined proposal for a new legislation will be handed over to the Swedish Legal Council (*Lagrådet*) in in order to obtain their observations. After this part of the legislation process, the government hand over the final proposition to the Swedish Parliament (the *Riksdag*).

N.B.: The thesis concerns the retention of traffic data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks. This is referred through at the thesis as the “retention of data”, “retention of traffic data”, “traffic data retention”, “data retention”, “blanket retention of traffic data”, etc., interchangeably.

3 Personal Integrity

While in Sweden the discussion concerns *personlig integritet*, or translated "personal integrity", the international discussion would be labelled as one concerning "privacy". There are some differences, but this thesis will use the words interchangeably. I believe that there is no real difference "legally" when one speaks of safeguarding personal integrity or safeguarding privacy. The discussion will, in the end, be one and the same.

Defining personal integrity, or privacy, is a tricky quest. When we speak privacy in terms of rights or obligations between actors, the question we really discuss is whose and what interests are we safeguarding and against what.[2] One finds that the idea of personal integrity is a highly subjective notion. What one person feel is a violation to her integrity might be nothing peculiar to the other. Furthermore, as this chapter will show, there are few positive definitions of personal integrity. Instead, attempts for a definition will ultimately resort to a negative definition, i.e. the notion of personal integrity is defined by the acts which are considered an intrusion of it.

In Sweden, the term "personal integrity" has been central ever since the 1960's with the emergence of the discussion on computer technology from a societal perspective.[3] At the dawn of this discussion the centre of interest was the risk for totalitarian regimes, the so-called Big Brother. As time has passed, it has become clear that the problem of Big Brother may arise even when the use of surveillance technology has a good cause.[4] An example is the use the example of surveillance cameras - they create a feeling of security but they are also potential infringements on personal integrity.[5]

In everyday speech one may hear somebody being described as a person with integrity – this would allude to the character of said person.[6] Personal integrity is however a right everyone has, regardless of your personal traits.[7] It can be said that there are three principles protecting an individual's personal integrity. The first principle is the limitation of State interference[8] – data retention and monitoring of peoples activities are two ways in which a State is in danger of stepping outside of its competence. Another principle is the protection of personal data.[9] For example, an individual's medical file may not be read by anyone unauthorized. Lastly there is the idea of protection of private zones, meaning that information shall not be gathered

[2] Westregård, *Integritetsfrågor i arbetslivet* (Juristförlaget i Lund, Lund, 2002) , p 43
[3] Olsson, *Efter 11 september 2001: Kan storebror hejdas?* (Teledok & Vinnova, Stockholm, 2006), p 11
[4] Olsson, *ibid.*
[5] Olsson, *ibid.*
[6] Hansson, *Teknik och Etik* (KTHs filosofienhet, Stockholm, 2002), p.47; Westregård *supra* note 2, p.43
[7] Hansson, *ibid.*
[8] Hansson, *ibid.*
[9] Hansson, *ibid.*

from a person's home or any place which is otherwise private even if the information is not of a delicate nature.[10] As anyone can tell, these principles are not absolute. House warrants are approved by courts and data is retained by law enforcement authorities. We should view them more as ideas, from which we do not diverge unless necessary.

Personal integrity is the idea of a personal sphere, which should be protected from intrusion.[11] In short, it is about controlling the conditions for living your life and interacting with others.[12] You maintain your dignity by protecting your private life. The Swedish notion of personal integrity is used for various aspects of integrity.[13] It is used to mean physical as well as psychological aspects of integrity and it is sometimes referred to as something you have a right to and other times as a right in itself. The starting point, in both Swedish and international discussions, is often the 1967 resolution adopted by the International Commission of Jurists. This resolution used the formulation "right to privacy" The definition is a negative, precising which concrete measures would constitute infringements on someone's personal integrity, or privacy.[14] The resolution listed plenty examples of violations, such as phone tapping, search of the person, intrusion on a person's private sphere through bugging, espionage etc. These various violations were divided into three categories: intrusion, both physical or in any other sense, on a person's private affairs; gathering of information concerning a person's private affairs; publication or other exploitation performed by public authorities as well as individuals.

An intrusion on an individual's personal integrity could e.g. result in personal or monetary damage.[15] An example of this could be the exposure of a person's sexual orientation or political views, resulting in harassment. Another possible negative consequence is a weakened autonomy and freedom, for example: an individual's approach to their life choices, commitment and preferences are shaped more independently if the individual can feel assured that there is no transparency.

Göran Collste, a Swedish professor in applied ethics at Linköping University, wrote a piece on integrity for the commission of inquiry in their report SOU 1997:39 on integrity, information technology and public access.[16] He writes about the idea of privacy as a sphere.[17] There is an infringement on personal integrity when there is an intrusion in an individual's private life, or, in other words, when the person loses control over his or hers personal sphere. Collste states that it is easier to define

[10] Hansson, *ibid.*
[11] Hansson, *ibid.*
[12] *Olsson, supra* note 3, p. 11
[13] Westregård *supra* note 2, p.47
[14] *Conclusions of the Nordic Conference on the Right to Privacy*, International Commission of Jurists (1967) Geneva, p. 2, 3.
[15] Hansson, *supra* note 6, p.48
[16] Collste, 'Personlig Integritet'; SOU 1997:39 Integritet – Offentlighet – Informationsteknik , bilaga 4, s 785-807
[17] Collste, *ibid.*, p. 793

infringements on personal integrity, rather than defining personal integrity itself.[18] He holds that personal integrity is violated when there is an intrusion on the personal sphere and/or data about the individual, which there is reasonable cause to suspect are sensitive, are spread. The information may be about the person's qualities, perceptions or actions. Collste also discussed the matter of opposing interests, but he speaks of a conflict of values.[19] When a registry of personal data is established, a conflict of values will arise between the value of establishing the registry and the risk of integrity infringements that arises. The data might leak, for example. What kind of processing of data may threaten personal integrity? Collste gives some guideline, *inter alia* [20] Open v Closed systems – *i.e.* access for everyone or access for qualified persons only. Collste writes that while it is easy to assume that a system where only authorized personnel has access to the data would be the solution, experience show that such is not the case. There will be events of negligence with security routines, mistakes and even intended intrusion, whereby closed systems are not exclusive anymore. He concludes that since no system is absolutely closed, personal integrity must be discussed when establishing closed systems too. Another guideline was that of Intentions v Results – while the intention may be one, the results might be another. For example, while the intention of the data retention as per the Directive is to fight crime, the result may be violations of individuals' privacy. A third guideline was Identification v De-identification – registries where the data is de-identified constitutes no threat to personal integrity, according to Collste.

Collste also makes a distinction between subjective and objective infringements.[21] He uses Parents when defining what personal data is, who said that private data are "facts about a person which most individuals in a given society at a given time do not want widely known about themselves".[22] Is it possible, when legislating, to take into consideration what most individuals in society would not want widely known about themselves? Collste uses the example of a short adult who would not want his height publically proclaimed.[23] Here we get to the issue of subjective and objective infringements. This is a matter of feeling violated *contra* having been violated. The legislation must be based on the notion of what is reasonable to consider an infringement and what is unreasonably considered so. Collste alludes to the quote by Parent, saying that an infringement on integrity exists when data, which the majority would not want to be made public were the data about themselves, is made public.[24] He also considers individual experiences of violations to possibly be actual infringements if there is a reasonable cause for such experience, e.g. something you are ashamed of and thusly do not want anyone to know.

---

[18] Collste, *supra* note 16, p. 796
[19] Collste, *ibid.*, p. 803
[20] Collste, *ibid.*, p. 802-803
[21] Collste, *ibid.*, p. 794
[22] Parent, 'Privacy, Morality and the Law', (1983) 12 PPA 267, 270
[23] Collste, *supra* note 16, p. 792
[24] Collste, *ibid.*, p. 794

Hermerén, a Swedish professor of philosophy, writes that the idea of a right to private life means that everyone has the right to decide what information about the individual may be shared to whom, for what purpose this information may be used, and what type of information may be communicated to themselves.[25] He discussed the notion of privacy as the distinction between public and private spaces.[26] He notes, however, that simply because a person is located in a public space, does not mean she should be subject to surveillance. He also noticed the option of defining privacy through the notion of a private sphere, but is not satisfied with the notion.[27] He writes that the two latter constructions are built on the idea that there are certain types of data or areas which are private and therefore should be protected. He presents a different notion, which is the thought that what should be prevented is that an individual or the authorities acquire complete knowledge regarding another individual, regardless of how private data and areas are possibly defined. This means that it is of importance to regard the kind and amount of data being stored concerning an individual. It is perhaps possible, he writes, to completely map out a person's life by coordinating data which in and of themselves are trivial.[28] Hermerén links the definition of integrity with the idea of a set of rights for a person with the corresponding obligations of others. We define these rights and obligations by looking at the opposing interests of actors, thus making this way of defining personal integrity as a *prima facie* right, not an absolute right.

Defining integrity has thus proved to be tricky and ultimately most effectively defined by using a negative approach, *i.e.* from concluding what actions would constitute violations of privacy. From a human rights law perspective it thus becomes interesting to see what legal regulations there are protecting the individuals from violations on their privacy.

[25] Hermerén, Kunskapens pris. Forskningsetiska problem och principer I humaniora och samhällsvetenskap (HSFR, Stockholm, 1996), p.143
[26] Hermerén, *ibid.*, p.148
[27] Hermerén, *ibid.*, p.149
[28] Hermerén, *ibid.*

4 Legal Protection for the Individual

This thesis concerns the Swedish implementation's compliance with the right to respect for private life. Therefore, a presentation is needed on the various ways the individual will have her privacy protected by national legislation, the Convention and under EU law. The chapter ends with a presentation of the relationship between the EU and the ECHR. For clarity's sake, I will refer to the European Convention on Human Rights as the ECHR in this chapter, and the European Court of Human Rights will be referred to as the ECtHR.

4.1 Protection for the Swedish Citizen

Sweden has three main legal provisions protecting the individuals from infringements on their human rights: the Instrument of Government (*Regeringsformen*), [29] the ECHR and the Charter of Fundamental Rights of the European Union.

The protection of personal integrity, or privacy, in Sweden is regulated in the Swedish fundamental laws ('*grundlagen*') which constitutes what could be dubbed the constitution of Sweden. This is a collection of fundamental laws, of which the Instrument of Government is part. In Article 6 of the second chapter of the Instrument of Government, there are regulations on the protection of the individual's relations with the public institutions against physical violation, body searches, house searches and other invasions of privacy.[30] The individual is also protected against examinations of her correspondence, eaves-dropping and recording of phone conversations or other confidential communication. Until 2011 this was all the privacy protection that the fundamental laws afforded. This meant that only the content of correspondence would be protected from arbitrary intrusions, which in turn meant that the proposed legislation or data retention would not have been covered by the privacy protection in Swedish fundamental laws. However, changes to the Instrument of Government were passed by the Parliament and as of 1 January 2011, the fundamental laws of Sweden also protects the individual against significant invasions by public authorities on her personal privacy if it occurs without her consent and involves the surveillance or systematic monitoring of the individual's personal circumstances.[31]

The Instrument of Government allows restrictions to the scope of Article 6; Article 20 of the same chapter permits that several of the rights and

[29] Instrument of Government – SFS 1974:152, *Regeringsformen*
[30] Chapter 2, Article 6(1), Instrument of Government
[31] Chapter 2, Article 6(2), Instrument of Government

freedoms in the Instrument of Government may be limited by law, including the rights and freedoms of article 6.[32] The limitations may be imposed only when they satisfy a purpose acceptable in a democratic society and a limitation may not go beyond what is necessary with regard to the purpose which occasioned it.[33] Furthermore, the limitations may not be so far-reaching that they pose a threat to the free formation of opinion as one of the fundaments of democracy. Much of these formulation we recognize from the Articles of the ECHR, presented in Chapter 8.

Swedish citizens are also protected by the European Convention on Human Rights. Sweden is a high contracting party to the ECHR and it was first implemented into Sweden by way of incorporating fully is as national legislation. This simply means that the entire text of the convention was implemented as an act of itself,[34] an act which is regularly updated pursuant to the Council of Europe's adoption of new Protocols. After this implementation, the status of the Convention was that of any act in Sweden. This caused a situation where it was unclear what the relationship was between the Convention rights and another act which would breach those rights. The solution to this dilemma was to add an Article to the Instrument of Government, which stipulated that no act of law or other provision may be adopted if it does not comply with Sweden's undertakings under the ECHR.[35]

The Charter of Fundamental Rights of the European Union was not a legally binding treaty until the entry into force of the Lisbon Treaty in December 2009. Article 51 of the Charter states that "the provisions of the Charter are addressed to the institutions, bodies, offices and agencies" of the EU, meaning that they must comply with the charter when they legislate and otherwise act.[36] The Member State must observe the Charter only when they are implementing Union law. The European institutions must comply with the Charter and are subject to the jurisdiction of the European Court of Justice ('Court of Justice').[37] On a national level, one will find protection of privacy in the national constitutions, which are applicable to the national institutions and under the judicial scrutiny of national courts.

With the transformation of the Charter into a legally binding treaty, Mock and Demuro holds that we will now also find that "[u]nion protection may penetrate the national system, at least insofar as national bodies act in the implementation of union law".[38]

---

[32] Instrument of Government, Chapter 2, Article 20
[33] Instrument of Government, Chapter 2, Article 21
[34] Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
[35] See the Instrument of Government, Chapter 2, Articles 20-22 and 25
[36] TFEU, Article 51
[37] Mock and Demuro, Human Rights in Europe – Commentary on the Charter of Fundamental Rights of the European Union (Carolina Academic Press, Durham, 2010), p.319
[38] Mock and Demuro, *ibid.*

The individual may thus challenge the national implementation of EU law on grounds of interference with her Charter rights in her national court, which also in turn may refer a case to the Court of Justice when it is unclear what the approach should be. The individual may furthermore complain to the European Ombudsman, regarding how an EU institution has acted. The individual may also question the legality of an EU measure in front of the General Court, *i.e.* the first instance court of the Court of Justice, on grounds of a breach of her Charter rights. However, the possibilities for an individual to bring a case to the Court of Justice are limited. When challenging an act, the individual is afforded *locus standi* only when she is directly and individually concerned by an EU institutions actions or by a regulatory act.[39] Although Article 263 of the Treaty makes no express provision regarding the admissibility of actions brought by legal persons for annulment of a directive, it is clear from the case-law of the Court of Justice that the mere fact that the contested measure is a directive is not sufficient to render such an action inadmissible. In that respect, it must be observed that the Community institutions cannot, merely through their choice of legal instrument, deprive individuals of the judicial protection offered by that provision of the Treaty.[40]

What does it mean to be directly and individually concerned? The starting point is the *Plaumann* case, which has determined the tone in the discussion. In this case, regarding an importer of goods, the Court of Justice set strict requirements and held that in order for a person to challenge a measure which is not directly addressed towards them, the person must show that the decision "affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are differentiated from all other persons and by virtue of these factors distinguished them individually".[41] The Court of Justice pointed out that the defendant in the case was affected by the EU measure as an importer of goods and as such was not distinguished in relation to the measure since imports could be practiced by any person at any time. Thus it seems that the chances for an individual to claim that she is individually concerned by a Directive are extremely narrow.

In his opinion to a case from 2002, General Avocat Jacobs argued for a wider interpretation of the requirements. He proposed that the provision might be in need of a reconsideration, and in his opinion an individual should be considered directly affected by a generally applicable EU measure when "by reason of his particular circumstances, the measure has, or is liable to have, a substantial adverse effect on his interests."[42]
In a case from 2002, the General Court (formerly the Court of First Instance) seemed inspired by the General Avocat's approach in his

[39] TFEU, Article 263 (4)
[40] Case T-135/96 *UEAPME v. Council* [1998] ECR II-2335, para 63
[41] Case 25/62 *Plaumann v. Commission* [1963] ECR 95, para 107
[42] Opinion of General Avocat Jacobs, ECJ C-50/00 P – *Unión de Pequeños Agricultores* v *Council* [2002] ECR I-3357, Para 102 subparagraph 4

opinion.[43] In this case a fishing company sought annulment of a Community regulation, where the General Court reconsidered the notion of being directly concerned to meaning that "a natural or legal person is to be regarded as individually concerned by a Community measure of general application that concerns him directly, if the measure in question affects his legal position, in a manner which is both definite and immediate",[44] meaning that it would not be required that the individual shows that her particular situation differentiates her from all other. However, the Court of Justice dismissed this approach in its decision in the case, reaffirming the narrow possibilities for individuals to contest an EU measure.[45]

While having read this chapter, one might wonder why the Charter and the Court of Justice is of interest in a thesis concerning rights under the ECHR. Chapter 4.2 will explain the relationship between the EU and the ECHR, and how the Charter makes it possible for the ECHR to affect the workings of the EU institutions.

4.2 The EU and the ECHR

4.2.1 Today

The European Union is presently not a party to the ECHR. The Community as such is only indirectly affected by the ECHR due to the fact that all Member States to the EU are bound by the ECHR; however, the EU cannot itself be held responsible for any breaches of the rights imposed by the ECHR.[46] Member States are naturally bound by both. A Member State is thusly obliges to implement a Community Directive, but it is also obliged to comply with the ECHR when doing so.[47] In the *Matthews* case, the ECtHR observed that "acts of the [EU] cannot as such be challenged before the Court because the [EU] is not a contracting party" and that Member States of the Convention are free to transfer competences to an international organization so long as rights under the ECHR continue to be "secured",[48] *i.e.* the State continues to be responsible for infringements on ECHR rights even after the transfer of powers to the EU. In the *Bosphorus* case the ruling concerned Ireland's responsibility under the Convention for the execution of an EU regulation, *i.e.* secondary law which a directive also is, the ECtHR noted that in the one hand the ECHR does not prohibit the State from transferring sovereign power to international organizations such as the EU.[49] On the other hand, the State is still responsible under the ECHR "for all acts

[43] CFI T-177/01 – *Jégo-Quéré and Cie SA* v *Commission* [2002] ECR II-2365
[44] *Jégo-Quéré* case, *ibid.*, para 51
[45] ECJ C-263/02 *P Commission v. Jégo Quéré SA* [2004] ECR I –3452
[46] Lock, **'**The ECJ and the ECtHR: The Future Relationship between the Two European Courts' (2009) The Law and Practice of International Courts and Tribunals 8, p. 376
[47] Lock, *ibid.*
[48] *Matthews v United Kingdom*, (App. 24833/94) 18 February 1999 [GC], (1999) 28 EHRR 361, ECHR 1999-I, para 33
[49] *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v Ireland*, (App. 45036/98) 30 June 2005 [GC], (2006) 42 EHRR 1, ECHR 2005-VI, para 152

and omissions of its organs regardless of whether the act or omission in question was a consequence of domestic law or of necessity to comply with international legal obligations".[50] How would the ECtHR reconcile the two opposites? To what extent can a State's actions can be justified by its compliance with obligations arising from a membership of an organization to which sovereign power has been transferred? The ECtHR recognized that it would be incompatible with the purpose and object of the ECHR to absolve a State from its Convention obligations in the areas covered by such a transfer.[51] The ECtHR stated that State action which had been taken in compliance with such legal obligations is justified as long as the organization is considered to protect fundamental human rights in a manner which is equivalent to, i.e. comparable with, to the protection which the ECHR provides.[52] If the organization is considered to provide comparable protection, the presumption will be that the State has not violated ECHR rights when it implements legal obligations arising from its membership to said organization.[53] The State would still be fully responsible for acts falling outside strict international legal obligations.[54] The ECtHR reviewed the ways in which the EU guaranteed fundamental rights and the means of controlling any interference with these rights, and remained satisfied that the protection of fundamental human rights by the law of the EU is "equivalent to that of the Convention system".[55] The presumption only operates where the concerned community law can be challenged before the Court of Justice (being 'comparable' to the ECtHR), which means the presumption does not operate regarding issues of EU primary law, since primary law cannot be contested through the Court of Justice. It therefore seems as though the ECtHR "privileges" secondary community law as such,[56] *inter alia* a directive such as the Data Retention Directive.

On the note of the Court of Justice and means of control, the ECtHR admitted that the possibilities for an individual to bring a case before the Court of Justice are limited, as described above in chapter 4.1. The ECtHR was nevertheless satisfied that the actions initiated before the Court of Justice by EU institutions or a Member State constitutes important control of compliance with EU norms which indirectly benefits the individuals.[57] The ECtHR noted that it is primarily through national courts that the EU system provides a remedy to individuals against a Member State or another individual for a breach of EU law. The Court of Justice remains control through the manner in which it will respond to the interpretative or validity questions referred to it by the domestic courts.[58]

[50] *Boshporus* case, *ibid.*, para 153
[51] *Boshporus* case, *ibid.*, para 154
[52] *Boshporus* case, *ibid.*, para 155
[53] *Boshporus* case, *ibid.*, para 156
[54] *Boshporus* case, *ibid.*, para 157
[55] *Boshporus* case, *ibid.*, para 161-165
[56] Lock, *supra* note 47, p. 379
[57] *Bosphorus* case, *supra* note 50, para 163
[58] *Boshporus* case, *ibid.*, para 164

The Charter of Fundamental Rights of European Union ('The Charter') has become legally binding as an EU treaty as of the entry in to force of the Treaty of Lisbon in 2009. This means that the States are obligated to comply with the Charter when implementing EU law.[59] It also means that the EU itself may not legislate in a way which is incompatible with the Charter. Article 52(3) of the Charter states that when there are corresponding rights in the ECHR, the protection afforded by the Charter shall be *at least* the same as by said Convention. Thusly it is prevented that the human rights standard afforded by the Charter becomes lower than that of the ECHR.[60] Such corresponding rights are, e.g., Articles 8 and 10. Article 13 does not have an equivalent. There are official explanations on Article 52(3) of the Charter, which *inter alia* states that "[t]he meaning and scope of the guaranteed rights are determined not only by the text of those instruments, but also by the case law of the European Court of Human Rights".[61] Lock notes that a general argument against an assumption that the ECHR's case law should be binding for the EU is that "such a duty would be alien to European Union Law"; court decisions under EU law can only become binding *inter partes*.[62] Lock writes that were the Court of Justice to be bound by the ECtHR's case law, it would mean that the court of one legal order would be bound by a court of an entirely different legal order. The doctrine of *stare decisis*, meaning the obligation for a court to abide by precedent rulings only makes sense when there is a clear hierarchy of the courts with the possibility to appeal an inferior ruling.[63] It is obvious that this is not the relationship between the Court of Justice and the ECtHR. Had there been a wish to make case law of the ECtHR binding for EU institutions, it would most likely have been blankly stated in the Charter. [64] One may note that the legal world is ever on the move, which means that future Court of Justice case law could render the ECtHR's case law binding to some extent to the Court of Justice but as of today no such situation can be claimed to exist. As for now, ECtHR's case law is merely a source among others when interpreting the Charter.[65]

4.2.2 Upcoming Changes

Article 6(2) of the Lisbon Treaty requires the European Union's accession to the ECHR. New Protocol 14 to the ECHR amends Article 59 of the ECHR, adding a second paragraph stating that "[t]he European Union may accede to this Convention".[66] The background of the accession is the situation of two separate legal orders where the ECHR and its judicial examinations are not applicable to EU acts. The Council of Europe sees this as a problem due the fact that EU law cannot, as of yet, be contested under

[59] The Charter of Fundamental Rights of the European Union, Article 51
[60] Lock, *supra* note 47,p. 382
[61] 'Explanations Relating to the Charter of Fundamental Rights' [2007] OJ C303/02, p.17
[62] Lock, *supra* note 47,p. 385
[63] Lock, *ibid.*,p. 385
[64] Lock, *ibid.*,p. 386
[65]The Charter of Fundamental Rights of the European Union, Preamble, 5th recital.
[66] Protocol 14 Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention, Article 17

the ECHR; meanwhile, the Member States must comply with the ECHR when they apply or implement EU law.[67] This discrepancy will be amended when the EU becomes a contracting party to the Convention, thus exposing it to an "independent external control". The accession enables the individual to bring a complaint before the ECtHR regarding interferences with the ECHR rights by the EU institutions.

[67] ' The European Union's Accession to the European Convention on Human Rights', Fact Sheet.

5 The Data Retention Directive - Directive 2006/24/EC

After the bombings in Madrid in 2004, the European Council charged the Justice and Home Affairs Council with the task of creating a draft Framework Decision on data retention, constituting a part of the fight against terrorism[68] Sweden was one of the countries who cooperated in developing the action plan which was presented in the summer of 2004. In March 2006, the European Parliament and the Council adopted Directive 2006/24/EC. Whereas previously only some Member States legislated on the obligatory retention of certain traffic data, the Directive now imposes the obligation on all national service providers to retain traffic data generated or processed when supplying publicly available electronic communications services. The objective of the Directive is to harmonize the obligations on communication service providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, especially organized crime and terrorism.

5.1 The Purpose and Scope of the Directive

As with all directives, the purpose of the Data Retention Directive is that of harmonizing member state legislation, namely the obligation on providers of publicly available electronic communications services or of public communications networks to store certain data generated or processed when a communication takes place on the internet or via regular or cellular telephony. The traffic and location data and the related data necessary to identify a subscriber or a user,[69] whether a legal entity or a natural person, is stored in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime.[70] Data regarding the content of the electronic communication shall not be stored.[71]

It is stated within the preamble introducing the directive that in this new age when electronic communication is increasing significantly, the retained traffic data will be invaluable in the work of the prevention, investigation, detection and prosecution of criminal offences, in particular organized crime.[72] It is stated that the need for and value of retaining traffic data from certain types of communication has been demonstrated in several Member States, as well as by research,[73] especially concerning investigations of

[68] The Council of the European Union, 26226th meeting (Press Realease) 14894/04 (Presse 332), Brussels, 2 December 2004, p. 12
[69] Directive 2006/24/EC, article 2.2
[70] Directive 2006/24/EC, article 1.1
[71] Directive 2006/24/EC, article 1.2
[72] Directive 2006/24/EC, the Preamble, recital 7
[73] Directive 2006/24/EC, the Preamble, recital 11

serious criminality such as organized crime and terrorism.[74] It is thus important to ensure that the retained traffic data are made available to law enforcement authorities for a certain period and subject to the conditions provided by the Directive.

Several Member States had, as mentioned above, already legislated regarding an obligation for service providers to store traffic data; this had led to a discrepancy in the legislation of the different States. These legal and technical discrepancies concerning traffic data retention would present obstacles to the internal market for electronic communications due to the fact that service providers were faced with different requirements regarding the types of traffic and location data to retain and the conditions and length of retention.[75] It is not the technology for retaining the data which is to be harmonized, the choice of technology is left to be dealt with on a national level. The aim of the Directive is thus simply to harmonize the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime since it is felt that these goals are better achieved at the Community level instead of having the obligation to retain data defined by each Member State. [76]

5.2 Personal Integrity

The preamble of the Directive discusses personal integrity at several instances. Most prominently, it refers to article 8 of the European Convention of Human Rights, reminding the Member States of everyone's right to respect for private life.[77] As a counterweight, it is pointed out that this right may be interfered with by public authorities if it is necessary in a democratic society, e.g. in the interests of national security, for the prevention of crime or for the protection of the rights and freedoms of others. It is said that the retention of data has proved to be an invaluable tool for the law enforcement in several Member States, e.g. when dealing with serious affairs such as organized crime and terrorism. It is thus necessary to make sure that traffic data is made available to law enforcement authorities, under the conditions of the Directive. One of those conditions will be compliance with article 8 of the ECHR. The right to private life as provided by the ECHR is presented in its own chapter further down.

Recital 22 of the preamble states that the Directive does respect the fundamental rights and has observed the principles stated in the Charter of Fundamental Rights of the European Union. The Directive particularly aims to ensure full compliance with Article 7 and 8 of the Charter. According to Article 7 everyone has the right to respect of his or hers private life and communications. Everyone also has the right to protection of their personal

[74] Directive 2006/24/EC, the Preamble, recital 9
[75] Directive 2006/24/EC, the Preamble, recital 6
[76] Directive 2006/24/EC, the Preamble, recital 21
[77] Directive 2006/24/EC, the Preamble, recital 9

data. Any processing of the data must have the consent of the person concerned or have a legitimate basis laid down by law. It is further stated that "[e]veryone has the right of access to data which has been collected concerning him or her[…]" and that it must be subjected to an independent authority to control the compliance with these rules.

Recital 21 of the preamble makes reference to Article 5 of the Treaty on the European Union.[78] Recital 21 ensures that the Directive is in accordance with the principle of proportionality as set out in the Article; " [The] Directive does not go beyond what is necessary in order to achieve" the objectives of investigating, detecting an prosecuting serious crime.

5.3 The Content of the Directive

This subchapter briefly presents the regulatory content of the Directive.

5.3.1 The obligation to store traffic data

The Directive obliges the Member States to adopt measures to ensure the retention of such traffic data as defined in Article 5 of the Directive.[79] The Directive does not oblige states to retain data concerning unsuccessful call attempts, *i.e.* "a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention",[80] but Member States are free to include it in their legislation.[81]

The Directive explicitly states that no data which may reveal "the content of the communication may be retained pursuant to the Directive".[82]

Member States are obligated to legislate on the retention of traffic data generated and processed by publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned to the extent that such activity is within the State's jurisdiction. The data must be stored for a minimum of 6 months and a maximum of 2 years; it is up to the individual Member State to decide upon the time period of the retention within this time span.[83]

Article 5 contains the details regarding what particular data is subjected to retention. The retention concerns data necessary to trace and identify the source of a communication;[84] the destination of a communication;[85] the

[78] Consolidated Version of the Treaty on The European Union [2010]
[79] Directive 2006/24/EC, Article 3
[80] Directive 2006/24/EC, Article 2.2f
[81] Directive 2006/24/EC, Article 3.2
[82] Directive 2006/24/EC, Article 5.2
[83] Directive 2006/24/EC, Article 6
[84] Directive 2006/24/EC, Article 5.1a
[85] Directive 2006/24/EC, Article 5.1b

date, time and duration of a communication;[86] the type of communication;[87] the users' communication equipment or what purports to be their equipment,[88] and lastly data necessary to identify the location of mobile communication equipment.[89] For each of these different categories, the article states the details of which data to retain depending on the way of communication.

In order to trace and identify communication using fixed network or cellular telephony the data concerned is the dialed phone number and the name and address of the subscriber/registered user. As regards Internet access, Internet telephony and Internet email, the retained data will concern the allocated user-id(s)[90] and the user-id and phone number allocated to a communication that have entered the public telephone network, as well as the name and address of the subscriber/registered user to whom an IP-address, phone number or user-id was given.

In order to identify the destination of a telephone communication, fixed or cellular, data regarding the dialed number(s) and the subscriber/registered users name and address must be retained. As regards Internet telephony and email, the data will concern the user-id or phone number allocated to the subscriber/registered user, and also the user-id of the intended recipient.

Regarding data for determining the date, time and duration of a communication, for fixed or cellular telephony the information retained will simply be the time and date for the start and end of the phone call. As regards Internet access, Internet telephony and Internet email, the retained data will regard the time and date of the log-in and log-off the Internet service, the user-id of the subscriber/registered user and the IP-address allocated by the Internet access service.

For fixed telephony, data regarding the calling and called phone numbers shall be retained. Data concerning the calling and called phone numbers shall be retained when it comes to cellular telephony too, but, furthermore, data shall also be retained concerning the identity of the SIM-card and the physical phone device used. In the case of prepaid and anonymous cellular services, data regarding the date and time for the activation of the service and the cell-id from which the service was activated is to be retained.[91] Lastly, concerning Internet access, Internet telephony and Internet email, the data retained will concern calling phone-numbers for dial-up access, and the digital subscriber line or other end-point of the sender of the communication.

---

[86] Directive 2006/24/EC, Article 5.1c
[87] Directive 2006/24/EC, Article 5.1d
[88] Directive 2006/24/EC, Article 5.1e
[89] Directive 2006/24/EC, Article 5.1f
[90] The term user-id is defined by the directive in Directive 2006/24/EC, article 2.2d as "unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;"
[91] Directive 2006/24/EC, Article 2.2e defines cell-id as meaning "the identity of the cell from which a mobile telephony call originated or in which it terminated".

Lastly, to identify the location of mobile communication equipment, the necessary data will regard the cell-id at the start of the communication and data for identifying the geographic locations of the cells used by reference to their cell-ids during the time period that the communications data is retained.

Article 11 of the Directive exempts the retention of data pursuant to the Directive from the provisions of Article 15(1) of directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Article 15(1) states that retention of traffic data for purposes of law enforcement may be allowed beyond the restrictions of certain articles in that directive, but must then meet the requirements of being necessary, appropriate and proportionate and have the aims of protecting State security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system. Such data may only be retained for a limited period of time. Article 11 of the Directive amends article 15 of directive 2002/58/EC by adding to it a paragraph which states that article 15(1) does not cover data which is retained pursuant to the Directive.

5.3.1.1 In Less Technical Terms

While not appearing so for a layman, the technological aspect of the Directive has intentionally been kept rather vague in order to avoid that the regulations become outdated as technology evolves, which, as we all know, happens rather quickly. Now follows an attempt to present what the data tells about us, as far as understood by the author.

As has been pointed out, the *content* of the communication is never to be stored. Instead, traffic data is stored in order to create a puzzle from the communications, and the traffic data will be used in an historical sense, *i.e.* the request to access data will, naturally, concern data of past events and actions. These data could help e.g. the police to e.g. map out the escape route of somebody who has committed a crime.[92]

The information that will be stored will tell the law enforcement authorities *to whom* you were calling and *where you were* when you were making this phone call. The *time and the duration* of your conversation will also be logged. The same goes for texting and emailing. This means that all of the Swedish citizens' phone, sms, and email contacts will be registered.

As regards the Internet, whenever you use your computer to go online, your IP-address, which essentially is your online identity during said Internet session, will be registered and connected to your Internet subscription from you Internet Service Provider ('ISP'). The time of your Internet access will also be registered.

[92] Prop. 2010/11:46 p. 18

The usage of cell phones will effectively provide a map of an individual's pattern of movement. Not only are cell phones used to call and text from anywhere and everywhere, thus providing a frequently updated map of your whereabouts; with the introduction of Smartphones, such as Androids or iPhones, the updates are far more frequent. Smartphones make use of the Internet to provide services such as automated inbox updates; the constant updates of your inbox requires that the Smartphone finds and communicates with the closest 3G pylon. The result of this is that the flow of traffic data between your Smartphone and your ISP is constant and your location will be determined with a precision often down to a few hundred meters, effectively turning the Smartphone into a tracking device. In retrospect and for a period of 6 months, the pattern of your movement habits will be around-the-clock and complete.

5.3.2 Management of Retained data

5.3.2.1 Data Security and Protection

Member States are obliged by article 7 to ensure, as a minimum, certain "data security principles" concerning the data retained pursuant to the Directive. These minimum security principles include that the data shall be subject to appropriate technical measures to protect the data against unauthorized or unlawful storage, processing, access or disclosure and to ensure that they can be accessed by specially authorized personnel only.[93] To ensure that the security principles are followed, the Member States must designate one (or more)completely independent public authorities for monitoring the application of article 7.[94]

Recital 15 of the preamble makes Directive 95/46/EC, which concerns the protection of personal integrity with regard to the processing and the free movement of personal data, fully applicable to the retained data. Recital 16 specifies the obligations from Directive 95/46/EC by explicitly saying that its obligation to ensure data quality as stated in its Article 6 will apply fully to the retained data. For example, these provisions mean that the Member State shall provide that the data will be processed fairly and lawfully and collected for specified, explicit and legitimate purposes and not further processed in an a way which is incompatible with these purposes.[95] However, it is not considered incompatible if further processing of data is made for historic, statistics or scientific purposes as long as appropriate safeguards are provided[96]; this should not be of any importance to data retained pursuant to the Directive, since there is a time limit of 2 years for the retention of data except, as mentioned above, in the case of particular circumstances. The data must not be excessive in relation to the purposes for

[93] Directive 2006/24/EC, Article 7e and c.
[94] Directive 2006/24/EC, Article 9
[95]Directive 95/46/EC Article 6.1a & b
[96]Directive 95/46/EC, Article 6.1b

which it has been collected for.[97] Recital 16 also refers to article 16 and 17 of directive 95/46/EC, which, in short, imposes an obligation on the Member States to ensure confidentiality and security of the processing of the data which is retained.

Article 13 of the Directive obligates the Member States to take the necessary measures to ensure that any intentional access to or transfer of retained data, that is not permitted under the national legislation adopted pursuant to the Directive, is punishable by effective, proportionate and dissuasive penalties (including administrative and criminal penalties).[98] Furthermore, article 13 states that each Member State must take the necessary measures to ensure that the national measures that the State has already taken to ensure the compliance with chapter III of directive 95/46/EC are fully implemented the processing of the data under this directive as well. The chapter referred to contains 3 articles, one each for judicial remedies, liability and sanctions. These articles ensures the right for the individual to have access to judicial remedies in case of a breach of the individuals rights under national law applicable to the processing in question.[99] The Member States shall also provide that any individual who has suffered damage as a result of an unlawful processing operation is entitled to compensation for the damage suffered. Member States must adopt special measures to ensure the full implementation of the provisions, and "in particular lay down the sanctions to be imposed" where there has been a breach of the provisions adopted pursuant to the Directive. Recital 19 of the preamble of the Directive states that "[t]he right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC", namely its article 23, applies also to the illicit processing of any personal data pursuant to the Directive.

5.3.2.2 Access to data

Article 4 of the Directive obliges Member States to adopt measures which will ensure that retained data will be available to the competent public authorities only, and only in specific cases and in accordance with national legislation. It is thus up to each Member State to define in its national legislation "[t]he procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements".[100] It must be ensured that the retained data, and any other necessary information relating to the data, is stored in such a way that it can be transmitted to the national authorities without undue delay, upon request.

It is pointed out in recital 25 of the preamble that the Directive is without prejudice to the power of the Member State to legislate regarding access to

[97] Directive 95/46/EC Article 6.1c
[98] Directive 2006/24/EC, Article 13.2
[99] 95/46/EC chapter III"JUDICIAL REMEDIES, LIABILITY AND SANCTIONS", articles 22-24.
[100] Directive 2006/24/EC, Article 4

and use of the retained data by national authorities, *i.e.* the Directive does not aim towards affecting this issue and it is totally up to each Member State to decide. When data is retained for such activities which do not fall within community law, e.g. the activities of a State in areas of criminal law or operations concerning State security[101], the legislation will have to respect the fundamental rights provided by the ECHR, namely its article 8 as interpreted by the European Court on Human Rights. Further on this matter, recital 17 of the preamble reaffirms that Member States must adopt legislative measures that ensures not only that the retained data is provided only to the competent national authorities, but also ensures the full respect for the concerned individual's fundamental rights.

5.4 Critique

The main and general critique against the Directive has concerned the proportionality of blanket retention of traffic data from individuals' private communications in relation to the aim of fighting crime. Other concerns are the differing and subpar implementations of the Directive in terms of security of the storing of the data and access to the data.

The Article 29 Working Party (the Working Party) is an independent advisory body on data protection and privacy. The Working Party was established pursuant to Article 29 of directive 95/46/EC. It consists of representatives from the national data protection authorities of each Member State, the European Data Protection Supervisor and the European Commission. The scope of the body is to examine any question concerning application of the various data protection directives and will as such contribute to a uniform application of the directives. It will do this by making recommendations, opinions and documents.

Previous to the Framework Decision that resulted in the Directive, the Article 29 Working Party was skeptical towards the need for such a Framework Decision, mainly questioning the proportionality.[102] The Working Party has noted that the retention proposed in the draft decision (and subsequently in the Directive) would make surveillance which was authorized in exceptional circumstances the rule.[103] The retention would be

[101] Directive 2006/24/EC, Preamble, Recital 25, 2nd sentence, which refers to the areas mentioned in article 3(2), 1st indent of Directive 95/46/EC. Article 3(2) of Directive 95/46/EC in turn refers to the areas covered in the TEU under Title V ("PROVISIONS ON A COMMON FOREIGN AND SECURIY POLICY") and Title VI ("PROVISIONS ON POLICE AND JUDICIAL COOPERATION IN CRIMINAL MATTERS") and adds that "in any case" operations concerning public security, defense, State security and the activities of a State in areas of criminal law fall outside the scope of Community law.
[102] Article 29 Working Party , 'Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]', 9 November 2004, p 2
[103] Article 29 Working Party , *ibid.*, p 4

clearly disproportionate as it applies to all individuals who use electronic communications and not only those who would be monitored. The Working Party has argued that not every tool can be deemed desirable or necessary in a democratic society merely because it has proved to be useful tool for law enforcement, especially if it leads to the systematic recording of all electronic communications. It had not been shown by the draft decision that there were no other less invasive means which would render comparable results in combating serious crime or protecting national security. The Working Party has suggested using the so called "quick-freeze" procedure instead, a method used in e.g. the US and in Germany where law enforcement authorities would communicate with the service provider requesting them to not extinguish certain traffic data once it has been used for the service provider's needs.[104] The authorities would then be given the time to needed to receive the court order necessary to access the "frozen data". After the data has been accessed, the service provider may than delete it as per usual.

The Working Party has noted that the precedent principle for retaining traffic data was for the service providers own purposes, and that this retention would constitute a derogation from this principle. The Working Party has pointed out that it has been revealed that the majority of the data requested by the law enforcement authorities throughout Europe were not older than six months, showing that longer periods of retention are clearly disproportionate. The Working Party has stressed that while law enforcement authorities must have effective powers available to them in the fight against terrorism, there must always be made considerations of proportionality so as to not undermine the democratic society that we are wishing to protect by the measures.[105] The regulations would force the retention of traffic data which service providers have no need for; in this manner, the Working Party has held, it was possible to eventually achieve an unprecedented and ubiquitous monitoring of every type of "communication and movement of the totality of citizens in their daily life".[106] Only a small portion of the stored data would actually be useful for investigational purposes. The Working Party has clearly stated that no traffic data related to unsuccessful calls should be included since there has been no in-depth assessment made concerning the adequacy of retaining this data, nor should any data concerning geographical location when using a cellphone be stored other than at the start of the communication.[107] The list in the Directive is to be considered exhaustive and no additional data may be imposed on service providers pursuant to the Directive.[108]

---

[104] Article 29 Working Party , 'Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)', 21 October 2005, p.5
[105] Article 29 Working Party , *ibid.*, p.6
[106] Article 29 Working Party , *ibid.*, p.5
[107] Article 29 Working Party , *ibid.*, p.10
[108] Article 29 Working Party, 'Report 01/2010 on the second joint enforcement action Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-

After the implementation of the Directive, the Working Party stood by its previous opinions and added its concern regarding the lack of details in the Directive on the treatment of the traffic data.[109] This would leave room for diverging interpretations by the Member States, thus not properly assuring that all European citizens are afforded the same level of protection and safeguards. The Working Party reminded that the types of data to be retained must be kept at a minimum and any changes must have been assessed in a strict necessity test.[110]

In 2010, the Working Party issued an alarming report on the differing and subpar security measure standards for the stored data in various Member States.[111] Article 7 of the Directive concerned the obligation for Member States to ensure that the service providers take the technological and organizational security measures needed to keep the data safe from unauthorized use and leakage, but gave no detailed directions. The report found that the security measures seems to depend on the business size of the service provider and that the handover procedures of traffic data to the authorities are very heterogeneous. [112] Service providers employ a wide variety of solutions with varying levels of transmission security; some would use dedicated, encryption-protected transmission channels, while other would simply send the data to the authorities by email, fax, standard mail or courier mail.[113] The Working Party therefore requested the establishment of a pan-European handover standard.[114] It seemed to the Working Party that there was no standard awareness among the service providers of the risks inherent in storing large volumes of traffic data.[115] The Working Party suggested that external audits on a regular basis might contribute to an independent and objective risk assessment.[116] As the Directive lacked guidelines for the service providers on how to achieve adequate security standards, the Working Party gave guidelines for service providers in the report. These included: strong authentication mechanisms where the physical presence of the person in charge is required; detailed tracking of accesses and log management solutions; logical separation from other systems processing traffic data for commercial purposes; the roles and functions of system administrators should be detailed in ad-hoc documents as they are of special organisational importance; etc.[117] Some of the

---

Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive' WP 172, 13 July 2010, p. 9

[109] Article 29 Working Party, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC', 25 March 2006, p.2

[110] Article 29 Working Party, *ibid.*, p.3

[111] Article 29 Working Party, *supra* note 110

[112] Article 29 Working Party, *ibid.*, p.1

[113] Article 29 Working Party, *ibid.*, p.14

[114] Article 29 Working Party, *ibid.*, p.15

[115] Article 29 Working Party, *ibid.*, p.12

[116] Article 29 Working Party, *ibid.* ,p.11

[117] Article 29 Working Party, *ibid.*, p.13

suggested methods were already in use by some of the service providers, but not all. While most suggestions were aimed at the service providers, the Working Party reminded that they require that public authorities will also act, including the European Commission, Member States and the national data protection agencies, especially regarding cost issues which could reduce the service providers will to deploy the necessary security measures.[118] Relying on self-regulation the way the Directive did is thusly not sufficient in this context, mainly because of the discrepancy of powers between the law enforcement authorities and the service providers, but also because of cost related issues may not lead to an approach ensuring high security standards. The Working Party concluded that the numerous varieties of security measures currently in place shows that the Directive has failed in achieving the goal of homogenous legislation in all Member States and equal security standards for all European citizens.[119]

In 2011 the European Commission ('the Commission') adopted an evaluation report on the retention of traffic data pursuant to the Directive.[120] The Report observed that the retention of traffic data has been valuable for the law enforcement authorities in their fight against serious crime.[121] A total of over 2 million requests for access to the data was made in Europe in each of year 2008 or 2009, with Cyprus having such low figures as 100 while Poland had an amount of 1 million requests.[122] Most frequently, requests were made for cell phone data. The Commission's figures did not indicate the precise purpose for which the requests were made in each instance. The statistics also show that the data accessed were not older than 6 months in 86 % of the time; the numbers for data under 3 months old were 67%.[123] The data had helped in constructing evidence trails leading up to an offence, starting criminal investigations when there were no eye witnesses or forensic evidence e.g. in cases of cybercrime where the IP-address is often the initial lead, and was an integral part in 'regular' criminal investigations.[124] The Commission noted the same serious concerns which the Working Party had observed in their 2010 report. The level of security would vary depending on the size of the business.[125] There exists vastly different versions of regulation in the different Member States on the issue of the purposes for accessing and using the data, and the legal procedures for accessing it.[126] For example, while some member states require judicial authorization for each request for access, some States require an authorization from a senior authority only and not a judge, while in two

[118] Article 29 Working Party, *ibid.,* p.19
[119] Article 29 Working Party, '*ibid.,* p.14
[120] Commission (EU), 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)**'** COM(2011) 225 final, 18 April 2011
[121] Commission (EU), *ibid.,* p.2
[122] Commission (EU), *ibid.,* p.21
[123] Commission (EU), *ibid.,* p.22
[124] Commission (EU), *ibid.,* p.23-25
[125] Commission (EU), *ibid.,* p.9
[126] Commission (EU), *ibid.,*p.11

Member States the only condition appeared to be that a request was made in writing.[127]

After the Commission has made this evaluation, it has started to prepare a proposal for an amendment of the Directive, [128] correcting its weaker points in order to clarify who is allowed to access the data, the purpose and procedures for accessing it.[129] In the Report it was said that options might include defined lists of competent authorities, independent and/or judicial examination of requests for access and a minimum standard of procedures for operators when they allow access to competent authorities.[130] The Commission also stated its intention to consider options for strengthening data security and protection standards.[131] This would be done through introducing 'privacy-by-design solutions' which will ensure that the standards are met both during storage and transmission of the data. The Commission would also take into considerations the recommendations on minimum safeguards which the Working Party made in their 2010 Report.[132]

In May 2011, the European Data Protection Supervisor (EDPS) adopted an opinion on the Directive, where it was stated that the Directive has failed meet privacy and data protection requirements.[133] The Opinion was based on what the Commission had presented in its evaluation report. The EDPS held in its opinion that the Commission Report shows that the Directive had failed in its main goal of harmonizing national legislation on data retention.[134] The EDPS also held that it had not been sufficiently demonstrated in the Report that data retention as provided for in the Directive is necessary or that it could not have been regulated in a less privacy-intrusive manner.[135] The Directive also lacks foreseeability, according to the EDPS. Since the days of the draft for the Directive, the Commission had stated that that the limitations on the rights to privacy and data protection were 'necessary to meet the generally recognized objectives of preventing and combating crime and terrorism,[136] something which the EDPS has always disputed on the basis of lack of evidence. In its opinion it noted that recital 9 of the Directive stated that data retention had proven to

[127] Commission (EU), *ibid.*,p.9
[128] Commission (EU), *ibid.*,p.1
[129] Commission (EU), 'Commission evaluates the Directive on retention of telecommunications data' (Press Release) IP/11/484, 18 April 2011
[130] Commission (EU), *supra* note 122, p.11
[131] Commission (EU), '*ibid.*, p.18
[132] Commission (EU), *ibid.*, p.18
[133] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)', 31 May 2011
[134] European Data Protection Supervisor, *ibid.*, p.7
[135] European Data Protection Supervisor, *ibid.*, p.7
[135]European Data Protection Supervisor, *ibid.*, p.7
[136]Commission (EU) 'Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC' COM(2005)438, 21 September 2005, p. 3.

be an effective and necessary investigatory tool, even though there was still no evidence presented to base such a conclusion on, which made the EDPS argue that Directive was based merely on an assumption that data retention was a necessary measure in the fight against organized crime.[137] The Commission had stated in its report that most Member States consider data retention a necessary tool. The EDPS stated in his opinion that "most" must mean the majority, *i.e.* at least 14 Member States, while in fact the Report referred to only nine states in this discussion.[138] The EDPS also criticized that the Commission had based its findings on the statements of the Member States rather than requiring that the States should establish to the Commission their need for data retention as a necessary measure. The statements could only be considered as opinions by the Member States on how they would like to have EU rules on data retention, and does not constitute sufficient evidence that blanket traffic data retention is a necessary tool in law enforcement activities. The EDPS held that while examples from the Member States of solved cases are interesting, the Report suffers from too many shortcomings regarding the quality and quantity of the evidence to satisfy the EDPS that the necessity of the measure has been proven[139] Regardless of whether the necessity has been proven, the EDPS held that blanket data retention is in any case beyond what is necessary.[140] The EDPS based this statement, *inter alia*, the unclear purpose of the measure and wide notion of what a competent national authority might be which has led to the data being used for a "far too wide range of purposes and by far too many authorities".[141] Furthermore, the inconsistency in the safeguards of the access to the data (the EDPS seemed to request that court orders be required) and the fact that the level of security is not sufficiently harmonized also affects the necessity assessment.[142] The EDPS is not satisfied with the Commission's conclusion that the security measures in the Directive are sufficient since it had found "no concrete examples of serious breaches of privacy";[143] the EDPS criticized this conclusion due to the fact that it appeared that the Commission had only asked Member States to report on the matter, rather than making a broader consultation.[144] As part of the necessity requirement follows the investigation on whether there are less intrusive measures that would render equal results.[145] The EDPS requested a more in-depth analysis on the method of "quick-freeze" as an alternative measure.[146] It is not satisfied with the Commissions commitment in the Report to investigate whether the "quick-freeze" method is a good compliment to data retention. Concluding the assessment of the Directive's compliance with fundamental human rights, the EDPS looked into the

[137] European Data Protection Supervisor, *supra* note 135, p.7-8
[137]European Data Protection Supervisor, *ibid.*, p.8
[138] European Data Protection Supervisor, *ibid.*
[139] European Data Protection Supervisor, *ibid.*, p.9
[140] European Data Protection Supervisor, *ibid.*, p.11
[141] European Data Protection Supervisor, *ibid.*
[142] European Data Protection Supervisor, *ibid.*, p.12
[143] Commission (EU), *supra* note 122, p.30
[144] European Data Protection Supervisor, *supra* note 135, p.12
[145] European Data Protection Supervisor, *ibid.*, p.10
[146] European Data Protection Supervisor, *ibid.*, p.11

foreseeability of the regulation. While he recognized that ultimately, it is for the Member State implementing a Directive to fulfill the foreseeability requirement, he also believe that to a certain extent a Directive must in itself fulfill the requirement too.[147] The EDPS took the view that the Directive should at least clearly define the purpose and indicate who can access the data and under which conditions. This would be sanctioned, according to the EDPS, by the new constructions made by the Lisbon Treaty where the EU is allowed competences in the field of judicial and police cooperation in matters of crime.[148] The EDPS supported the Commission's decision to propose a revision of the current Directive, but not the fact that the Commission seemed to have excluded the possibility of repealing the Directive. [149] The EDPS sees a repeal as one of the possible options for the Commission to take after it has done its impact assessments.

5.4.1 Ireland v. Parliament and Council

The Directive has been under scrutiny by the Court of Justice, after Ireland brought action to the Court of Justice in 2009.[150] However, there was no examination on the Directive's compliance with the fundamental rights. Instead, the Directive's compliance with the Treaty on the Functioning of the European Union ('TFEU') was discussed. Ireland requested the annulment of the Directive on the grounds that it was not adopted on an appropriate legal basis. The Directive had its legal basis in Article 114 of the TFEU (former Article 95 of the Rome Treaty),[151] which permits the adoption of measures which have as their object the establishment and functioning of the internal market. Ireland argued that the Article was not a sound legal basis for the Directive, since the main objective of the Directive is to facilitate the investigation, detection and prosecution of crime, including terrorism. Ireland submitted that measures based on Article 114 must have as their 'center of gravity' the harmonization of national laws in order to improve the functioning of the internal market.[152] The Slovak Republic supported Ireland's position and questioned the extensiveness of the interference in the individuals' rights as a possible breach of Article 8 of the ECHR.[153] While the Parliament and the Council answered the question on Article 8 by referring to the pursuit of a legitimate interest, *i.e.* fighting crime, as permitted by the second paragraph of the Article, the Court of Justice made no mention of the Slovak Republic's reference to the ECHR. The Court of Justice held that recourse to Article 114 is possible if the aim is to prevent the emergence of future obstacles to trade resulting from a diverging development of national laws, if the emergence of such obstacles are likely.[154] The Court of Justice found that the submitted evidence proved

[147] European Data Protection Supervisor, *ibid.*, p.13
[148] European Data Protection Supervisor, *ibid.*, p.13
[149] European Data Protection Supervisor, *ibid.*, p.14
[150] Case C-301/06, *Ireland v Parliament and Council* [2009] ECR I-593
[151] *Ireland v Parliament and Council , ibid.*, para. 20
[152] *Ireland v Parliament and Council , ibid.*,, paras. 28, 30
[153] *Ireland v Parliament and Council , ibid.*,, paras. 33-34
[154] *Ireland v Parliament and Council , ibid.*,, para. 64

that the national measures which had been adopted prior to the Directive had differed substantially and that it was entirely foreseeable that the Member States which had not yet adopted rules on data retention would introduce rules in that area which were likely to heighten the differences between the various national measures.[155] It was apparent to the Court that the existing various national rules on traffic data retention were liable to have a direct impact on the functioning of the internal market, and that this would grow more serious as time passed.[156]
Additionally, the Directive did not concern implementation of any police or judicial cooperation in criminal matters, nor did it harmonize the issue of access to data by the competent national law enforcement authorities.[157] These provisions were excluded out of the Directive as they did not fall within the area of the third pillar.[158] The Court of Justice held that the substantive content of the Directive is directed towards the activities of the service providers. In light of this the Court of Justice held that the directive relates predominantly to the functioning of the internal market.[159] Ireland's action was dismissed.[160]

Thusly, the Court of Justice gave no attention to the issue of the right to respect for private life. However, on 5 May 2010 the Irish High Court granted the Digital Rights Ireland Limited the motion for a reference to the Court of Justice under Article 267 of the TFEU.[161] The Digital Rights Ireland Limited questions whether mass surveillance of the kind endorsed by the Directive is compatible with fundamental rights. The Irish High Court allowed the plaintiff company to litigate the matters fully, *i.e.* both with regards to the infringement of the company's rights but also, more importantly, with regards to natural persons, as the plaintiff company is a digital rights interest group representing the interests of natural persons.[162] The plaintiff sought that the question be referred to the Court of Justice on whether the Directive is valid notwithstanding, *inter alia*, the rights under the European Charter of Fundamental Rights and the European Convention on Human Rights, and Article 5 of the TEU on the principle of proportionality.[163]

[155] *Ireland v Parliament and Council , ibid.,*, paras. 69-70
[156] *Ireland v Parliament and Council , ibid.,*, para 71
Ireland v Parliament and Council , ibid.,, para 83
[158] Note of interest: since the Lisbon Treaty, the distinction between the first pillar and the third pillar has been removed.
[159] *Ireland v Parliament and Council , supra* note 152, para 85
[160] *Ireland v Parliament and Council , ibid.,*, para 94
[161] *Ireland Ltd -v- Minister for Communication & Ors* [2010] IEHC 221, 5 May 2010
[162] *Ireland Ltd -v- Minister for Communication & Ors, ibid.*, para.93
[163] *Ireland Ltd -v- Minister for Communication & Ors, ibid.*, para.14

6 The Swedish Implementation of the Directive

According to the directive, Member States should have implemented Directive 2006/24/EC on data retention (hereafter 'The Directive') into their national legislation by September 15 2007. As regards Internet access, Internet telephony and Internet e-mail, the Directive allowed the Member States to postpone the implementation till March 15 2009. Sweden claims to have used this possibility to postpone.[164]

As per the regular way of imposing new legislation in Sweden, the government of Sweden arranged a specially appointed investigator. The inquiry was called the Traffic Data Inquiry (*Trafikuppgiftsutredningen*) and a report was handed in to the government in November 2007.[165] The report was referred to various public bodies, NGOs, and other bodies, for consideration, in order to obtain critique regarding the legislation that had been suggested by the investigator. After this procedure, a refined proposal for a new legislation was handed in to the Swedish Legal Council in November 2010 in order to obtain their observations. After this part of the legislation process, the government handed in its final proposition to the Swedish Parliament (the *Riksdag*).[166] On March 16 2011 the Riksdag voted on whether or not to pass the suggested legislation. Three minority parties (The Left Party, The Green Party and The Swedish Democrats) voted for a postponement of the voting until 2012.[167] The Swedish implementation of the directive is thus years behind the time table set out by the European Parliament and the Council of the European Union in the Directive. In February of 2010, the Court of Justice proclaimed that the Kingdom of Sweden had failed to adopt the Directive within the prescribed period and thusly failed to fulfill its obligations over said directive.[168]

Because of this ruling, and because Sweden lacked of a precise time table for the implementation of the Directive, the European Commission (the Commission) decided to hand over a letter of formal notice to Sweden in June 2010, where it asked for details of the actions Sweden intended to take

[164] Prop. 2010/11:46, p. 11
[165] The report was named 'SOU 2007:76 - *Lagring av Trafikuppgifter för Brottsbekämpning'*, a so called *betänkande* in Swedish.
[166] Prop. 2010/11:46. *Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv* 2006/24/EG (translation in to English: Retention of traffic data for crime fighting purposes – an implementation of Directive 2006/24/EC).
[167] Riksdagens Protokoll 2010/11:73, March 16 2011, under §7 *Lagring avtrafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv* 2006/24/EG.
[168] Case C-185/09, *European Commission v Kingdom of Sweden*, Judgment of the Court (sixth chamber), 4 February 2010

to guarantee the compliance with the Court of Justice ruling.[169] In January 2011, Sweden informed the Commission that a draft legislation had been submitted to the *Riksdag* with the intention of having the legislation adopted in March 2011. However, since the voting in the *Riksdag* led to a postponement of the vote on the proposed legislation for another 12 months, the Commission decided to refer Sweden to the Court of Justice with the request that the Court imposes financial penalties. The Court of Justice may determine sanctions in the form of penalties and/or a lump sum. [170] While the lump sum will penalize the persistence of the infraction between the first judgment of the Court of Justice and the second judgment, the penalty will regard the time period after the second judgment. The Commission proposed to the Court of Justice that Sweden shall be imposed a lump sum of €9.597 for each day of the period between already existing Court of Justice ruling and the second ruling, and €40.947 for each day the infringement continues after the second Court ruling. [171]

6.1 The proposed changes in legisation

Proposition 2010/11:46 suggests major changes of the Electronic Communications Act (*Lag (2003:389) om elektronisk kommunikation).*

In Sweden, all public communication networks usually provided in exchange for remuneration or publically accessible communication services are under obligation to notify the designated supervisory authority in order to receive permission to supply their services. These suppliers are the ones obligated to store the data as regulated in chapter 6 of the Electronic Communications Act. It is within chapter 6 that amendments will be made if the proposition is adopted.

6.1.1 The Actual Data retained

The Swedish implementation is in rather good conformity with the directive. The Government chose to go with the minimum time period of 6 months for the retention of the traffic data.[172] The proposed legislation goes beyond the minimum requirements of the directive in two instances: it proposes that data be retained as regards unsuccessful phone calls and for locating mobile communication devices used at the beginning *and* at the end of the communication.[173] While it was an option in the Directive to retain data on unsuccessful phone calls, data for locating mobile devices at the end of a communication was not included in the Directive at all.

[169] Press Release: "Data retention: Commission refers Sweden back to Court for failing to transpose EU legislation". Reference Number: IP/11/409. April 6, 2011. Brussels.
[170] See article 260 of the TFEU
[171] Press Release: "Data retention: Commission refers Sweden back to Court for failing to transpose EU legislation". Reference Number: IP/11/409. April 6, 2011. Brussels.
[172] The Electronic Communications Act, Chapter 6, Article 16d
[173] The Electronic Communications Act, Chapter 6, Article 16a

The Government proposed these additional data to be retained based on the need of the law enforcement authorities. The Government argued that these data are equally as important as all the other data in crime investigations.[174] The government finds the legal basis for adding these types of traffic data in Article 15(1) of the EU directive 2002/58 which the Directive amends in part.[175]

Already in the Traffic Data Inquiry, a separate opinion was stated in the matter by Per Furberg.[176] He questioned the 'technique' applied by the commission of inquiry when using exemption clauses in directive 2002/58/EC in order to put these additional data in the same legislative category as the ones derived from the Directive.[177] The statement by the committee (and, subsequently, the government) that there is legal basis for this approach in article 15(1) of directive 2002/58/EC fails to recognize that there are requirements for when a Member State can impose an obligation to store the data exemplified in Article 15(1). The commission made such an extensive interpretation of the relationship between Article 11 of the Directive and Article 15(1) of directive 2002/58/EC, that it seemed to Furberg as though the commission has understood it to mean that the Directive's detailed account for which traffic data to store would be merely examples and not an exhaustive list.

The Swedish Council on Legislation held that the Swedish proposition for implementation of the Directive complied with the Directive in all the essential parts and thusly constitutes, seen from the European point of view, a legitimate and necessary interference with personal integrity.[178] The additional retention of the two types of data are seen by the Council as marginal interferences in their context and the government provided sound arguments for the retention of them.[179]

In the 2010 report by the Article 29 Working Party, it was specifically recommended that no Member State may impose additional data retention obligations on providers pursuant to the Directive.[180] The recommendations made by the Article 29 Working Party were based on the report's findings which clearly showed "a lack of harmonization and diversity in national implementation".[181] It was noted in the report that the Directive detracts from the provisions of directive 2002/58/EC and that the list of data which is obligatory to retain is supposed to be regarded as exhaustive, meaning that no additional obligations on data retention may be imposed on the service providers pursuant to the Directive.[182]

---

[174] Prop. 2010/11:46, p. 32-33
[175] Prop. 2010/11:46, p. 32
[176] SOU 2007:76 – 'Särskilt yttrande av Per Furberg', p. 317-318
[177] SOU 2007:76 – 'Särskilt yttrande av Per Furberg', p. 317
[178] Prop. 2010/11:46, Bilaga 8 "Lagrådets yttrande", p. 125-128
[179] Prop. 2010/11:46, Bilaga 8 "Lagrådets yttrande", p. 126
[180] Article 29 Working Party, *supra* note 110, p 19
[181] Article 29 Working Party, *ibid.*,, p.2
[182] Article 29 Working Party, ' *ibid.*, p.9

6.1.2 Access to data

As Article 4 stated, it is up to the individual Member State to regulate in legislation the access to the retained traffic data. Article 16c of chapter 6 regulates the conditions for handing out the stored data to the authorities. It is done so by referring to two different regulations: Article 22 section 1, point 2 and 3 of chapter 6 of the Electronic Communication Act, and alternatively chapter 27 Article 19 of the Swedish Code of Judicial Procedure (*Rättegångsbalken*). These are not new regulations, thus the situation for access to data will be the same after the implementation of the Directive as it was before.

There is an obligation for the service provider to conduct its agency so that the data can be handed out upon demand without delay and so that execution of the yielding of the traffic data is not exposed.[183] This means that the service provider must hand out data regarding a subscription if demanded by the DA, police or other authority with a responsibility to intervene against crime, when there is a suspicion of a criminal offence and where prison is the, or one of the, prescribed punishments for the crime and the authorities believe that the act will lead to other punishments than a penalty.[184] The other instance concerns data regarding electronic communications and is of more interest to this thesis. The service provider must hand out the data when demanded by the DA, police or other authority with a responsibility to intervene against crime, when there is a suspicion of a criminal offence and where the law prescribes no less than 2 years imprisonment.[185] The data may be of any kind, excluding the content of the communication, and shall regard a certain message.

As regards the reference to the Code of Judicial Procedure, the article referred to concerns secret tele-monitoring.[186] Transformed to the current context, it would mean that a service provider is obliged to hand out data when demanded to do so during a preliminary investigation of a crime for which the law prescribes no less than 6 months of imprisonment *or* the suspected crime is any of the following: [187]certain kinds of hacking, child pornography offenses which are not of a minor character, drug offenses and drug smuggling. In the case of an attempt, preparation or plotting to do any of said crimes, authorities may likewise demand to have data handed out to them if the offense of attempting, preparing or plotting the crime is a punishable act.

[183] The Electronics Communications Act, Chapter 7, Article 16f
[184] The Electronic Communications Act, Chapter 6, Article 22 section 1(2)
[185] The Electronic Communication Act, Chapter 6, Article 22 section 1 (3)
[186] The Code of Judicial Procedure , Chapter 27, Article 19
[187] The paragraph refers to the following regulations: Chapter 4, Article19 and Chapter 16, Article 10a of the Code of Judicial Procedure , The Narcotic Offenses Act (*Narkotikastrafflagen* (1968:64)) Article 1, and lastly the Smuggling Offenses Act (*Lag* (2000:1225) *om straff för smuggling*) Article 6 para.1

6.2 Critique

Here follows a presentation of various critique received by the government after the round of referrals for consideration, and how the government has responded in order to justify the legislation. Only the critique most relevant to the discussion of personal integrity will be presented, thus leaving out plenty of criticism regarding other aspects of the proposed legislation.

6.2.1 Crime Fighting

The implementation of the Directive puts two different interests against each other: the protection of the personal integrity of the individual against the law enforcement authorities' need for effective tools. As has been demonstrated in chapter 5, the European Parliament and the Council of Europe is of the point of view that the Directive has struck a correct balance between these interests. The matter is further discussed in the Swedish proposition in order to answer to the critique received after the round of referrals for consideration.[188]

Some of the bodies from which consideration was asked felt that an adequate balance had been struck between the two interests and that the Traffic Data Inquiry had done a well job presenting the discussion of balancing the two. These three bodies were the Swedish Anti-Piracy Agency (*Svenska antipiratbyrån*), the Swedish group of the IFPI (*IFPI Svenska Gruppen*), and the Swedish Customs (*Tullverket*).[189] Several other bodies put their emphasis on the outmost importance of limiting, as far as possible, the intrusion on personal integrity when retaining traffic data.

The Parliamentary Ombudsmen (*Justitieombudsmännen)* quotes the Traffic Data Inquiry where it was stated that the psychological effect of knowing that data is retained regarding your communications is the major infringement on personal integrity, not the fact that law enforcement authorities will access a very small portion of the retained traffic data in a limited amount of instances.[190] While the Parliamentary Ombudsmen did not wish to brush over the "abstract infringement on integrity" and the feelings one might have of an omnipresent 'Big Brother', they felt that these circumstances may not be used to pull away the focus from the concrete infringement of subjecting the individual to monitoring and registering of her communication activities. Because of the development of society and its communication infrastructure, the abstract fear, while being relevant, may not be put in focus. The data from all communications are already being

[188] Prop. 2010/11:46, pp.16-22
[189] Prop. 2010/11;46, p.17
[190] JO – "remiss angående betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)", Dnr 5927-2007. The quote referred to by the Parliamentary Ombudsmen, in swedish: "*den psykologiska effekt det innebär att människor vet om att uppgifter lagras om deras kommunikation är den stora integritetsskadan i sammanhanget och inte att de brottsbekämpande myndigheterna får ut en mycket liten del av de lagrade trafikuppgifterna i ett begränsat antal ärenden årligen*", SOU 2007:76, p. 235

stored to some extent and the law enforcement must be provided the data as a tool in the resistance against serious crime. The rules must be clear enough so that the citizens trusts the authorities and their usage of the data.

The Data Inspection Board ('the Board', *Datainspektionen*) questioned the Directive in its entirety.[191] The Board held that according to fundamental principles regarding the protection of data and integrity, personal data may normally be processed only for certain specified and legitimate reasons and may not later be processed for reasons incompatible with the original reasons. The Directive imposes the obligation to store data not for the service providers' purpose of providing the service, but solely for the interest of fighting crime. Thus, from a data safety point of view, there is nothing justifying such retention. However, the Board recognized that the implementation of the Directive is obligatory, and settled with reminding the government to respect integrity issues as far as possible and to take the statements of the Article 29 Working Party into great consideration.[192]

The Swedish Bar Association ('the Bar', *Sveriges Advokatsamfund*) , while recognizing the obligations as a Member State to the EU to implement the directive, had some heavy arguments on why the implementation of the Directive is unsuitable.[193] The Bar found that today, in Sweden, the general rule is that unless there is a court order for secret phone surveillance, the service provider decided which data to store for e.g. the company's invoicing purposes.[194] This would completely change with the implementation of the Directive. Now all data as specified by the proposed legislation will be stored for the investigation, detection & prosecution of crime. This is, according to the Bar, a paradigmatic shift due to the disregard of the same fundamental principle of which the Board spoke. The Bar holds that by principle, replacing the original purposes for storing data has never before been accepted.[195] In the context of Sweden's obligations under the ECHR, the Bar recognized the need for the legislation, *i.e.* crime fighting purposes. Instead it questioned the proportionality of the measures; an enormous amount of data will be retained, constituting a massive intrusion on the privacy of individuals of which the vast majority are not suspected of anything at all.[196] Furthermore, due to the massive amount of data, there is an increased risk of leakage. The Bar also points out the risk for further shifts in purposes for retaining data when the retention is of the proposed size.[197]

6.2.1.1 The Government's reply

Regarding the various critique, the government answered as follows.

[191] Datainspektionen – "Betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)", Dnr 1673-2007, p. 1
[192] Datainspektionen , *ibid.*, p. 1-2
[193] Sveriges advokatsamfund –Dnr R-2008/0035,
[194] Sveriges advokatsamfund *ibid.*, p. 1
[195] Sveriges advokatsamfund *ibid.*, p. 2
[196] Sveriges advokatsamfund *ibid.*, p. 4
[197] Sveriges advokatsamfund *ibid.*, p. 3

The government responded to the considerations by referring to the law enforcement authorities need for the traffic data in various stages of their work. The government pointed to the Report made by the *Beredning för Rättsväsendets Utredningar* (the 'BRU') in 2005, wherein the inquiring committee had presented the various ways of using traffic data.[198] If we read the part which the government referred to in their response, we learn that based on information from the authorities, traffic data is used in nearly each and every case of serious crime (murder, rape, serious drug offences, terrorist crimes, etc.) and using it is directly related with getting any development in the case at all.[199] Through using traffic data, in combination with other information from the investigations, the police is able to narrow down the suspects, and in many cases a person may be dismissed as a suspect thanks to the information gained from the traffic data. The traffic data provides the law enforcement authorities with information that will tell them things such as how a crime was planned and conducted or how the offenders acted after the act of the crime e.g. what escape route they took. The National Bureau of Investigation (*Rikskriminalpolisen*) held that in cases of Internet related crimes the criminal will most likely act anonymously and thus it is rare to have a suspect when a preliminary investigation is launched.[200] Accessing traffic data is then the only way for the police to find out who the suspect may be.

The Government also referred to the Traffic Data Inquiry, which preceded this very proposition for new legislation, *i.e.* SOU 2007:76, wherein the inquiry committee had given specific examples of cases where the traffic data had been of the outmost importance for solving the case.[201] For example, in a rape case, the underage victim informed the authorities that the offender had received two calls to his cell phone during the assault and that he had not answered them. By accessing the required traffic data, the identification of the offender was made possible and he could furthermore be linked to several other similar crimes a couple of years ago. Other interesting examples brought up is a case of human trafficking where the offenders were identified, linked to each other and geographical places, the transportation routes were mapped out along with the locations for the prostitution as well as the international network.

The gathered conclusion regarding the crime preventing aspect of the dilemma, was thus that there was a real and paramount need for the law enforcement authorities to access data. [202]While there is a possibility to access traffic data with the current legislation, there is a momentum of uncertainty involved: what type of data is stored and for how long is something that each service provider may decide for themselves and the decisions will be based not on the need of the law enforcement authorities

[198] Prop. 2010/11:46 p 18, reference to SOU 2005:38 .p 322-325
[199] SOU 2005:38, p. 322-323
[200] SOU 2005:38, p. 324
[201] Prop. 2010/11 :46, p. 18, reference to SOU 2007 :76 p. 133-134
[202] Prop. 2010/11:46, p. 18

but rather matters such as invoicing the costumers. With the implementation of the Directive, the access to the necessary traffic data will be secured.

The government stated that while the actual retention in itself will conclude an intrusion on privacy since there will be a psychological effect on the individual where she experiences that her private sphere and means of communication are being restricted,[203] the absolute majority of traffic data concerning the private affairs of individuals will be destroyed after the period of 6 months without having ever been accessed.[204] The government reminds the reader that the Directive itself made an assessment as to the balance between privacy and crime fighting, and that Sweden as a member state is obliged to implement the Directive.[205] But, the government continues, the obligation does not free Sweden from making integrity assessments in its implementation. Thus, in constructing the new legislation, the Government aimed towards creating a transparent system ensuring that the individual may predict what types of data will be stored about her, and how they may be used by law enforcement authorities. In line with this, the government has chosen to legislate to a greater extent than what was suggested by the Traffic Data Inquiry, *i.e.* put more of the details regarding what data to store in the law rather than in regulations issued by the government (*förordningar*) at a later stage,[206] the main reason behind this being that it increases parliamentary insight and eliminates the risk that further intrusions on privacy will be regulated without the participation of the parliament.[207] The very technical details will however still be regulated through government issued regulations.

The Government continues by holding that the part of the inquiry concerning locations for the retention, by whom and for how long data may be retained and other conditions surrounding the retention in itself shall assure the privacy of the individuals. Furthermore, the technological and organizational safeguards for the retained data must be sufficient, which is of importance not only for minimizing the risk for unauthorized access to the data but also for creating a trust among the public for the system.[208] The laws which will come into play when there has been an instance of unauthorized access must be preventive and reparative enough.[209] The government states that the already existing Swedish legislation in the areas of sanctions, trials and reparations for intrusions in privacy are adequate and no changes are necessary.[210]

[203] Prop. 2010/11:46. p. 19
[204] Prop. 2010/11:46, p.18
[205] Prop. 2010/11:46, p. 20
[206] Prop. 2010/11:46, p. 20
[207] Prop. 2010/11:46, p. 28
[208] Prop. 2010/11:46, p. 20
[209] Prop. 2010/11:46, p. 20
[210] Prop. 2010/11:46, p. 61

6.2.2 Access to data

The Parliamentary Ombudsmen held that Swedish legislation on access to the data is not as clear and well-arranged as would be desirable.[211] The Parliamentary Ombudsmen finds it hard to understand why the proposed changes in the BRU Inquiry had not yet been implemented.[212] The inquiry had proposed that the regulations on access in the Electronic Communications Act be abolished and completely replaced by the current regulations in the Code of Judicial Procedure. The Parliamentary Ombudsmen felt that it would be natural for the implementation of the Directive to be coordinated with the earlier made suggestions by the BRU Inquiry. The Chancellor of Justice ('the Chancellor', *Justitiekanslern*) shared the opinion of the Parliamentary Ombudsmen regarding the coordination of the two suggested changes in legislation,[213] as did the Bar.[214]

The Data Inspection Board expressed that there is a need for an independent and judicial examination prior to granting the authorities access to the traffic data, while not expressively saying that it must be a court decision.[215]

The Swedish Commission on Security and Integrity Protection (*Säkerhets- och Integritetsskyddsnämnden*) lamented the fact that if the current order in the Electronic Communications Act is maintained, there will be no independent and judicial examinations prior or after accessing the data.[216] The Commission on Security and Integrity Protection held that there is at least the need for an independent body with this function prior to access in order for Sweden to fulfill its obligations under Articles 8 and 13 under the ECHR.[217] As for examinations after an event of access to data, t felt it is only natural that its own supervision is extended hitherto in the future, as it already supervises secret phone monitoring. The Commission on Security and Integrity Protection referred to the Traffic Data Inquiry which stated that the requests to access data through the Electronic Communications Act far surpassed the instances of using actual secret phone monitoring. The Commission on Security and Integrity Protection saw this as an indicator that crime fighting has more and more become a matter of intelligence activities, and not preliminary investigations where secret phone monitoring is one of the available tools.[218] Thusly, the Commission on Security and

[211] JO – "remiss angående betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)", Dnr 5927-2007
[212] SOU 2009:1 'En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen'
[213] JK – "Betänkandet (SOU 2007:76) Lagring av trafikuppgifter för brottsbekämpning", Dnr 8771-07-80, p. 1
[214] Sveriges advokatsamfund , *supra* note 195, p. 5
[215] Datainspektionen – "Betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)", Dnr 1673-2007, p. 3
[216] Säkerhets- och Integritetskyddsnämnden – "Betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)", Dnr 4-2008, p. 1
[217] Säkerhets- och Integritetskyddsnämnden, *ibid.*, p. 2
[218] Säkerhets- och Integritetskyddsnämnden, *ibid.*

Integrity Protection saw the need for Sweden to implement the order used in many other countries, *i.e.* to give the law enforcement authorities the same delimitation of powers when working with intelligence as when they are working with preliminary investigations, thusly achieving that the rule of law and protection of privacy are safeguarded through independent judicial examinations.[219]

Further on this subject, in the Traffic Data Inquiry, it was briefly suggested that in order to safeguard the privacy and the integrity of the individual, the proportionality assessment which should be made in each instance of access to the traffic data should be made by a court.[220] However, the Inquiry Committee decided not to concern itself with the actual procedure of the consignment of the data, thus the matter was not further discussed. However, several bodies approved of this suggestion. Svea Court of Appeal (*Svea Hovrätt*) agreed that it would be beneficial for the protection of personal integrity if this order was implemented,[221] as did the Bar.[222]

Already in the Traffic Data Inquiry, a data counselor from the Data Inspection Board stated a separate opinion on the matter.[223]He was not satisfied that the inquiry had made an adequate analysis on how the regulations on access will be in compliance with the requirements of the Convention. The counselor criticized the committee of inquiry for stating that there are no reasons to change the existing legislation on the access to the traffic data. He questioned whether the Swedish implementation would be in conformity with the Directive if Sweden did not change the legislation on access.[224] The Counselor referred to recital 25 of the preamble to the Directive, where it is reminded that the national legislation on access and use of the retained data must respect the rights bestowed by the Convention. This means that the interference by the authorities must be necessary, proportionate and serve legislated, clear and legitimate reasons. The counselor was not of the opinion that there had not been any satisfying inquiries in the area of access to the data and compliance with the Convention, and requested a closer analysis on how the legislation in the Electronic Communications Act had been applied so far and careful considerations on how the application may now change due to the proposed obligation to store an extended amount of traffic data.[225]

6.2.2.1 The Inquiry by the BRU

This inquiry by the BRU was incorporated in to the SOU 2009:1 (*En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen*). To clarify, SOU 2009:1 is the gathering of three different SOU:s, which includes the SOU 2005:38 by the BRU. To understand what the bodies of

[219] Säkerhets- och Integritetskyddsnämnden *ibid.*
[220] SOU 2007:76, p. 228.
[221] Svea Hovrätt – ” Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)”, Dnr 683/07, p. 3
[222] Sveriges advokatsamfund , *supra* note 195, p. 5
[223] SOU 2007:76 – ’Särskilt yttrande av Hans-Olof Lindblom’, p 313-316
[224] SOU 2007:76 – ’Särskilt yttrande av Hans-Olof Lindblom’, p. 315
[225] SOU 2007:76 – ’Särskilt yttrande av Hans-Olof Lindblom’, p. 316

referral were speaking of when they referred to the inquiry by the BRU, I will present the main points of SOU 2009:1 that are of importance to the topic of access to retained data.

The SOU 2009:1 proposed, once again, that the current regulation in the Electronic Communications Act should abolished. To access traffic data for purposes of preliminary investigations, the authorities would have to go through the regulations on secret tele-monitoring in the Swedish Code of Judicial Procedure. If traffic data is needed for intelligence activities, the authorities would have to gain access through what is proposed to be a new Act,[226] where the data may be accessed for crimes of the same magnitude as is allowed in Swedish law today with one exception; law enforcement authorities may access data concerning subscriber information, *i.e.* information such as name, phone number or IP-address, even if the offense is suspected to lead only to a fine as the punishment. The Committee of Inquiry stated the police needs such possibilities, since there today is no possibility following the current legislation for the police to access subscription information when investigating instances of online bullying or grooming.[227] The government finds that in the balance between the intrusion that the access to traffic data means to the privacy of the individual contra the fact that the police today are extremely limited by the current legislation when it comes to investigating these online assaults, the scale is tipped in favor of the police's investigatory work.[228] It is pointed out that data that cannot be considered as data for identification, e.g. what other IP-addresses has been contacted by the holder of the primary IP-address, are not included in the category of subscription data. The suggested legislation goes further in that it sets requirements regarding what the purpose of accessing the data in the specific case should be, along with a requirement for a sort of minimum threshold concerning the importance that the traffic data holds for the purpose of which they are accessed.[229] The mere fact that it is suggested that the rules on access to data in the Electronic Communications Act should be abolished in favor of the rules in the Swedish Code of Judicial Procedure means that in preliminary investigations the traffic data shall not be accessed without a preceding court order,[230] however with the suggestion of a new possibility for prosecutors to make interim decisions on accessing traffic data in cases of urgency.[231] Since the use of court orders is not as natural in activities of intelligence gathering, the importance of an independent supervisory body is emphasized. It is suggested that the Swedish Commission on Security and Integrity Protection would have a

[226] The proposed Act is called "Förslaget till lag (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet", which may be translated to "the proposal for the Act (0000:00) on access to data on certain electronic communication in the intelligence activities of the law enforcement authorities"
[227] SOU 2009:1, p. 104
[228] SOU 2009:1, p. 105
[229] SOU 2009:1, p. 76
[230] SOU 2009:1, p. 70
[231] SOU 2009:1, p. 78

supervisory function on this access to the traffic data.[232] The Government handed in the proposal to the Council on Legislation to receive its view in December 2010, and received it on 18 January 2011. The legislation was anticipated to come into effect on 1 July 2011, but there is yet no official proposition for the new legislation.

6.2.2.2 The Government's Reply

The government begins by mentioning that the Directive leaves it up to the Member States to decide on legislation concerning the access to the data, and reminds the reader of the statement by the Council of Europe where the Council stated that when a Member State defines "serious crime" in its national law, it shall pay "due regard to the crimes listed in Article 2(2) of the Framework Decision on the European Arrest Warrant (2002/584/JHA) and crime involving telecommunication".[233]

The government agrees with the bodies of referral in the criticism against keeping the rules on access intact. The government mentioned the suggestion in SOU 2005:38 by the BRU to unite the separate legislation in the Swedish Code of Judicial Procedure and eliminate the rules on access to data in the Electronic Communications Act. The government wrote that in 2007 it decided to further add to the inquiry in parts, such as the access to traffic data within the intelligence work of the police and during preliminary investigation where there is yet no suspect, which in the end resulted in SOU 2009:1, the main points of which has been presented in chapter 6.2.2.1.

The Government chose to shortly answer the suggestion by the Parliamentary Ombudsmen and the Commission on Security and Integrity Protection, by referring to the fact that such as suggestion for legislation is already in play as part of the SOU 2009:1.[234]

[232] SOU 2009:1, p. 110
[233] Statement by the Council of the European Union, 5777/06 ADD 1 REV 1, Brussels, 17 February 2006, p. 2.
[234] Prop. 2010/11:46, p.. 58

7 The Electronic Communications Act and the Swedish Code of Judicial Procedure – a comparison

7.1.1 LEK o RB

The Directive stated as its purpose to regulate the retention of data for reasons of fighting and preventing serious, organized crime. The Directive came to be in the wake of several events of terrorist attacks throughout Europe. However, an area it did not regulate was the access to the retained data. It is clearly stated in the Directive that this is an area where it is up to the Member State to decide. Now, if we go back to the Swedish Traffic Data Inquiry, it seems as though the matter is brushed over in a sense. The committee noted the absence of Directive instructions on the matter. However, the committee stated that it was not for this inquiry to primarily examine the procedure of the access to the data but rather that its focus was to examine whether the crimes that may be solved using retained traffic data are of the magnitude that is required in the Directive, *i.e.* serious or organized crime and terrorism.[235] The committee referred to a statement by the Council where it was said that Member States should pay due regard to the crimes listed in Article 2 of the European arrest warrant framework decision when deciding the level of criminality for which retained data may be accessed.[236] The Article states the scope of the Framework Decision, *i.e.* which acts, that are punishable by the law of the issuing Member State, would give rise to surrender pursuant to a European arrest warrant. These crimes include: participation in criminal organization, terrorism, kidnapping, trafficking, child pornography, computer related crime, illicit trafficking in drugs, illicit trade in human organs, murder, racism, swindling, sabotage, counterfeiting or piracy of products, etc. The commission of inquiry stated that if the focus of the Directive and its connection to the European arrest warrant framework decision would warrant changes in the legislation concerning access to data, the committee would make such suggestions. The committee thus reviews what types of crimes were covered by the threshold in the Code of Judicial Procedure of "a crime for which the law prescribes no less than 6 months of imprisonment" and produced a list which was similar to the one of Article 2 in the framework decision.[237] As regards the threshold in the Electronic Communications Act, it was quite similar.[238] Since, according to the

[235] SOU 2007:76, p. 228
[236] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States
[237] SOU 2007:76, p.223-224
[238] SOU 2007:76, p.224

Swedish law, the crimes that would incur access to the retained data are at least as serious as those listed in the European arrest warrant framework decision the committee saw no reason to change Swedish legislation concerning access to the data as provided by the Electronic Communications Act.[239] The Government had a different opinion in its proposition to the Parliament, presented in chapter 6.2.2.2.

As we learn from Chapter 6 Article 16c of the Electronic Communications Act, there are two separate regulations which would allow the appropriate authorities to access the retained data. When accessed under the rules of the Code of Judicial Procedure , one will speak of the matter as "secret phone monitoring". The following will be a presentation on how these regulations coincide and differ. The regulations are not going through any upcoming changes in the near future, even though it has been discussed by several committees of inquiry.

7.2 The Type of Data

Secret phone monitoring as prescribed in the 27th chapter of the Swedish Code of Judicial Procedure is distinct from phone tapping. Phone tapping means listening to the content of the communication.[240] Tele-monitoring means accessing, in secret, the traffic data from telecommunications (the author's translation of *telemeddelanden*) which is being or has been forwarded to or from a certain tele-address.[241] By tele-address is meant the non-physical addresses that the communication is transmitted between , e.g. IP-numbers, phone numbers and email addresses.[242] Tele-monitoring also offers the possibility to hinder that such communications reach through to the recipient, but this aspect is not of interest for this thesis.

The *travaux préparatoires* defines telecommunication by referring to what is the obsolete legislation which was replaced by the Electronic Communications Act Chapter 6 Article 19 – the formulation is exactly the same in this article as in the obsolete on. Telecommunication is thus defined as sound, text, pictures, data or other information transmitted by radio or by light or electromagnetical oscillation using a specially arranged conductor.[243] In the context of secret tele-monitoring, this means that traffic data for the following types of communication may be accessed: regular phone calls, online phone calls, email, text messages and voice mails.[244] As with the definition of traffic data in the Electronic Communications Act, traffic data in this context also means the data processed by the service provider which is necessary for forwarding a communication or for invoicing such communication.

[239] SOU 2007 :76, p. 227-229
[240] Code of Judicial Procedure, Chapter 27, Article 18
[241] Code of Judicial Procedure, Chapter 27, Article 19
[242] Prop. 1994/95:227, p. 31
[243] Prop. 2002/03:74, p.14
[244] Prop. 2002/03:74, p.13-14

Thus, one can conclude that the data that may be accessed is much the same.

In the Electronic Communications Act, the data will naturally regard passed communications. When using secret tele-monitoring, it may regard both past and future communications as per the law enforcements request in the individual cases. This would be the only difference in the aspect of the type of data retained.

7.3 The Severity of the Crime

When secret phone monitoring was first introduced in the 1980's it was not considered as intrusive in privacy as phone tapping and therefore received a lower threshold than phone tapping. Hence, phone monitoring requires a minimum of six months of imprisonment for the crime which the person is suspected of.[245]

As regards the Electronic Communications Act, data on subscriptions, *i.e.* the person's name, title, address and subscription number (e.g. telephone number, IMSI-number and IP-address), may be accessed when there is a suspicion of a crime where imprisonment is one of the prescribed punishments and the authorities believe that the punishment in the individual case will exceed that of regular fines.[246] As for the rest of the data that the Directive obliges the State to retain, these data requires a minimum of two years of imprisonment for the suspected crime. This means that crimes of attempt, preparation, conspiracy and complicity, which all have lower prison sentences than two years, are not covered by the Electronic Communications Act, while they very well may be under regulations on secret tele-monitoring of the Code of Judicial Procedure.[247]

It may not make sense that a regulation which was originally not of a criminal procedural nature prescribes a higher threshold than the Code of Judicial Procedure. Firstly we must consider the obsolete legislation that the Electronic Communications Act replaced, for through that legislation the release of data was done through using exceptions on Swedish secrecy legislation. The discussion in the *travaux préparatoires* concluded that the data could be very intrusive on privacy and in order not to water out the Swedish secrecy legislation too much, a high threshold was needed.[248]

Secondly, we must also consider that while the threshold may look severer in the Electronic Communications Act, it is more lenient in another closely related manner. The Code of Judicial Procedure requires that there must be individual who is suspected on good grounds for the crime, and that the court order for tele-monitoring must concern a certain tele-address which the law enforcement authorities have connected to the suspects.[249] As

[245] Prop. 1988/89:124, p.48
[246] SOU 2007:76, p.64
[247] Penal Code, Chapter 23, Articles 1-2
[248] Prop. 1983/84:142, p 38-39
[249] Code of Judicial Procedure, Chapter 27, Articles 20 & 21

regards tele-addresses that the suspect may contact, these may also be monitored if there are extraordinary reasons to believe that the suspect will contact the person,[250] meaning that the authorities must have this assumption supported by trustworthy information making them more or less convinced that communications will take place.[251] In the Electronic Communications act, on the other hand, any demands regarding the level of suspicion on the individual are absent. There does not have to be any suspect of the suspected crime. The reason for legislating the requirement of 'suspicion on good grounds' in the Code of Judicial Procedure was to avoid that the method of secret monitoring would be used to lightly, thus constituting gross intrusions on individuals' privacy.[252] This seems to be an aspect completely forgotten in the *travaux préparatoires* of the Electronic Communications Act. If the data is accessed pursuant to the Act in order to determine who might be suspected, there is also a high risk that the authorities were wrong, *i.e.* the person was innocent and the intrusion on her privacy completely unwarranted.

Neither does the Electronic Communications Act contain a requirement that the authorities must have connected a certain tele-adress to an individual that actually is a suspect. This will enable the authorities to make a 'base station depletion' (the author's translation of *basstationstömning*), meaning that data will be accessed regarding e.g. all of the cell phones that have been connected for communication and therefore in contact with a base station in close proximity to a crime scene during a limited period of time.[253] This does not include phones which have just been switched on. These base station depletions are only allowed under Article 20(3) of Chapter 6, namely for suspected crimes where imprisonment no lower than two years is prescribed. A large amount of data concerning the activity of numerous irrelevant, *i.e.* innocent, individuals will be available to and accessed by the authorities.

7.4 Neccessity of Accessing the Data & Time Limits

For secret tele-monitoring there is a requirement that the data which is asked for must be of extraordinary importance for the investigation at hand.[254] The meaning of this is according to the *travaux préparatoires* that the data has to reach up to a certain level of quality in addition to the requirement that there are no less invasive measures which may render the same result.[255]

There are no such 'necessity-requirements' in the Electronic Communications Act. The authorities do not have to motivate the use of the

[250] Code of Judicial Procedure, Chapter 27, Article 20(2)
[251] Prop. 2002/03:74, p. 38
[252] Prop. 1988/89:124, pp.49-50
[253] SOU 2007:76, p.65
[254] Code of Judicial Procedure, Chapter 27, Article 20, 1st sentence.
[255] Prop. 1988/89:124, pp. 44-45

data and may also require it even if less invasive measures could be at hand; the *travaux préparatoires* do not address the issue in the way that was done when legislating on secret tele-monitoring.

While there is no formal imitation in the Code of Judicial Procedure for the maximum time limits of the monitoring, the time period may never be decided to be longer than necessary,[256] but one should keep in mind that the court order for secret tele-monitoring must specify the time period for the monitoring. However, while theoretically the time period could be infinite both through the Code and through the Electronic Communications Act, it can in reality only cover six past months, since this is the proposed limit for storing data according to the implementation of the Directive.[257]

7.5 Proportionality

Regarding secret tele-monitoring, and surveillance in general, it is subject to the principle of proportionality.[258] The principle of proportionality in this aspect means that surveillance measures may only be resorted to when the reasons for the coercive means used outweighs the individual's or other conflicting interests. [259] This means that the surveillance must, in terms of type, strength, extensiveness and duration, be in correlation to the aim pursued.[260] The principle must be considered when ordering tele-monitoring and when executing it.

In the Electronic Communications Act, we have to go back to the first chapter to find any reference at all to the principle of proportionality. It is stated that no measure pursuant to the Electronic Communication Act may be more invasive than what appears to be reasonable and the measure must be proportionate with consideration to the purpose of the act and the other interests.[261] It is clear from this Article that there are other interests more prominent than crime fighting in this Act, such as the original interests the Act had of guaranteeing the effectiveness and security of the concerned communications. This makes it doubtful how effective the mentioned proportionality regulation would be in practice. Nevertheless, the principle of proportionality is generally applicable without explicit legal basis for intervention measures by the authorities against the individual.[262] There therefore is a "general presence" of the principle of proportionality covering the authorities undertaking.

It will become clear from the chapter below that assessment of proportionality and other principles will be made by a court in situations of tele-monitoring. As regards accessing data using the Electron

[256] Code of Judicial Procedure, Chapter 27, Article 21
[257] SOU 2007:76, p.65
[258] Code of Judicial Procedure, Chapter 27, Article 1
[259] Prop. 1988/89:124, p.26
[260] SOU 2005:38, p.139
[261] Electronic Communications Act, Chapter 1, Article 2
[262] SOU 2007:76, p.231

Communications Act, even though a rather weak regulation on proportionality exists there will be no such assessment by the service provider as it is legally obliged to hand out the data upon request. The public is forced to place all its confidence on the assessment made by the authorities requesting the data.

7.6 Control mechanisms

Secret surveillance measures such as tele-monitoring requires court orders, pursuant to a request by the attorney.[263] Concerning means of compulsion in general, the individual will be aware of them since they usually are not secret. Thusly, the individual may seek judiciary examination through a supervisory authority, local court or through an examination by the Chancellor of Justice or the Parliamentary Ombudsmen. However, secret tele-monitoring, and other secret surveillance measures, are, by their nature, secret means of compulsion. The individual will not be aware of the measures being carried out, and cannot seek examination regarding the legality of e.g. the secret tele-monitoring. The Court will, when examining the attorney's request, safeguard the interest of the individual and take into account her privacy when making its decision.[264] After completion of the secret tele-monitoring, the individual will be aware of the occurrence of the monitoring either by the following prosecution or, if the monitoring did not lead to prosecution, through being notified by the authorities.[265] This is a rather new legislation, created to ensure that the individual pursuant to receiving the notification will have the chance to see to that his rights are safeguarded by the legal measures mentioned previously and have the legality of the surveillance examined.[266]

Secret surveillance measures are under scrutiny of a yearly parliamentary control. The Parliament will receive a summary of the utilization of secret surveillance measures over the past years, and the law enforcement authorities' accounts for the benefits that the surveillance measures has had during the year.

It is of interest to note that the Commission on Security and Integrity Protection was founded only a couple of years ago, replacing the Register Board (*registreringsnämnden*). It is an independent public authority with the responsibility to monitor the way that law enforcement authorities utilize means of secret surveillance.[267] The Commission will make statements, constituting its opinions on desirable changes in the activities of the authorities, and has as its aim to ensure that flaws in legislation or other types of regulations are amended.[268] If the Commission is approached by an individual with a request to control if she has been subjected to secret

[263] Code of Judicial Procedure, Chapter 27, Article 21
[264] Prop. 1988/89:124, p.53
[265] Code of Judicial Procedure, Chapter 27, Article 31
[266] SOU 2006:98, p.93
[267] Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet, Article 1
[268] Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet, Article 2

surveillance and if it has been according to law, the Commission must is obliged to investigate.[269] The Commission is also under the obligation to notify the individual that the investigation has been carried through. There is nothing in the law prescribing an obligation to notify the individual of the result of the investigation. However, if the Commission finds that the secret surveillance, in our case secret tele-monitoring, has been unwarranted the examined authority must be reported to the Swedish Prosecution Authority (*Åklagarmyndigheten*).[270]

Before examining the control mechanisms of the Electronic Communications Act, we will take a short look at its history in this regard. Previous to the new legislation, Sweden has a State monopoly on the telecommunications market. Since a public authority was in control, *Televerket*, the legislation on secrecy and public access to information that was current at the time would entrust the authority with making the assessment, in each individual case, whether the requirements for accessing data were met. Since then, the tele-market has been transformed into a free market with private actors, whereupon it was seen as less appropriate that the private actors should make the assessment previously entrusted to a public authority.

This means that today, and after the implementation of the directive unless amendments of the Act are made, when there is a question on whether or not an access request to the data retained pursuant to the Electronic Communications Act is necessary, the authority requesting it will be the "judge" in the matter; whereas before it was the authority handing out the data which made this assessment and decision.[271] The legislation was amended in the way that seemed appropriate at the time and the access to data retained pursuant to the Electronic Communications Act is still under no control. It is still for the requesting law enforcement authority to decide when it is appropriate to access the data. There are no proposed amendments of the Act to be presented to the Parliament concerning this aspect of the legislation, even though it has been proposed in reports by commissions of inquiry.

As regards possible control mechanisms after the data has been accessed, the major obstacle for the individual is the fact that there is no obligation in the Electronic Communications Act or in other Swedish laws to notify the individual of a past access pursuant to the Act. The individual will thus find out only if she is prosecuted, since defendants will have access to the information on which the case is built. While the Chancellor of Justice and the Parliamentary Ombudsman will technically be available, in practice the individual will not be aware of the intrusion and thus not able to approach them. Nor will an access to the data pursuant to the Act fall under the scope of the Commission on Security and Integrity Protection. It is not mentioned in anywhere as part of the Commission's responsibilities.

[269] Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet, Article 3
[270] Prop. 2006/07:133
[271] Prop. 1992/93:200, p.162 and 164

The Directive does not require that the state designates a supervisory body concerning how the data is accessed, it merely requires that the State designated a public authority to be responsible for monitoring the application of Article 7, *i.e.* the security of the stored data.[272] The Parliamentary Ombudsmen suggested that the Commission on Security and Integrity Protection should become the supervisory body as regards how the data is accessed and the Commission itself suggested that its scope should be extended to cover all access to traffic data and not only data retrieved by secret tele-monitoring as is the case today. Instead, the government suggest in its proposal that the Swedish Post and Telecom Agency (*Post- och telestyrelsen*, 'PTA') should be kept as the surveillance body.[273] The PTA is currently responsible for monitoring the activities of service providers pursuant to the Electronic Communications Act.[274] This means that it promotes the security and efficiency of electronic communications, healthy competition on the market and keeping an eye on any development concerning e.g. security of data processing or health hazards. The only concern of the PTA that touches upon the area of this thesis is that it is responsible for monitoring the service provider's adaptation of the systems for the realization of secret phone tapping and tele-monitoring.[275] The government has not seen any need for creating a new body or "allowing" an already existing body to monitor the compliance of the proposed new legislation, since the PTA already monitors the compliance with the Electronic Communications Act. The government wishes to extend the scope of the PTA's monitoring of the service provider's activities to e.g. ensuring that the service provider stores the correct data, that the data is extinguished on the prescribed time limit, that the special technological and organizational measures are taken for the protection of the retained data and the compliance with the rule of immediate access to data for the law enforcement authorities.[276] The suggest extensions thus concerns the monitoring of the activities of the service providers, which means that if this version of the legislation is passed by the Parliament in a year, there will still not exist a body controlling that the data is accessed with due regard to privacy concerns. Furthermore, even if the scope of monitoring would have been extended, the types of decisions, prohibitions, fines and statements that the PTA is allowed to make are only such which would concern the service provider. Naturally, being the type of body it is, it would have no power over the law enforcement authorities' activities. Law enforcement authorities would not be within the PTA's field of expertise.

So what possible remedies are available for the individual in the end? Basically, the individual is left with a combination of the Parliamentary Ombudsmen for Justice, the Chancellor of Justice.

[272] Directive 2006/24/EC, Article 7
[273] Prop. 2010/11:46, p.55
[274] *Förordning* **(***2007:951*) med instruktion för Post- och telestyrelsen, Articles 1 and 4
[275] Electronic Communications Act, Chapter 6, Article 19
[276] Prop. 2010/11:46, p.58

The Ombudsmen for Justice is a body which supervises that the public servants of the parliament and other state employees who conduct work for the public follow the laws and regulations. The Chancellor of Justice is the government's equivalent of the Ombudsmen of Justice. The Swedish Data Inspection Board is a public authority which monitors the respect for the individual's privacy in the information society while trying not to impede the use of new technology; they monitor not only the activity of authorities, but also individuals, companies and authorities.

However, the bodies and authorities presented in the paragraph above cannot take any direct action against another public authority.[277] The monitoring of the Ombudsmen for Justice usually results in a statement about an illegal or otherwise erroneous activity by a public authority or public official, or in a prosecution against a public official. They cannot stop the activity itself. The same is applicable to the Chancellor of Justice.

7.7 Conclusion

The presentation above shows that is far easier for the law enforcement authorities to access the exact same data using the Electronic Communications Act rather that the Code of Judicial Procedures. The statistics regarding requests for secret tele-monitoring vis-à-vis the statistics on events of accessed data through the Electronic Communications Act indicates that the law enforcement authorities have recognized this difference, making them more prone to access the data via the Electronic Communications Act rather than by means of secret tele-monitoring.

According to the latest annual parliamentary control of the utilization of secret tele-monitoring measures during 2009, a total of 2 140 applications were made and 2134 of these were approved by the courts, which constitutes an increase by 47% during 2009 compared to 2008.[278] The number of applications has increased consistently through the years; the statistics showing that in 1999 there were only 297 applications.[279] In 10 years that number has increased by nearly 2000. The increase is explained by the National Police Board (*Rikspolisstyrelsen)* and the Prosecution Authority as a result of an increase in organized crime and the fact that criminals use cell phones to a very high extent and tend to change telephone and tele-addresses on a regular basis, especially in connection with a specific crime event.[280]

We may compare these numbers with those regarding access to traffic data pursuant to the Electronic Communications Act. Since there is no parliamentary control or other mechanisms controlling how the data is

[277] Prop. 2006/07:63, p. 117
[278] Skr. 2010/11:66, p.12
[279] Skr. 2010/11:66, p.13
[280] Skr. 2010/11:66, p.17

accessed, there are no official numbers. However, the Traffic Data Inquiry appreciated it to a number of 8000 in one year.[281] This means that the numbers doubled between 2004 and 2006.[282] There is nothing to suggest that the numbers should have decreased, especially if we consider that the numbers of secret tele-monitoring in 2006 was 1119 and two years later, in 2009, the number had increased by 90%.[283]

[281] SOU 2007:76, p.130
[282] SOU 2005:38 p.402 – according to this report, the number of occasions in which data was accessed pursuant to the Electronic Communications Act was around 4000 in one year.
[283] Skr. 2010/11:66, p.13

8 The European Convention on Human Rights

'The Convention protects the community of men; man in our times has a need to preserve his identity, to refuse the total transparency of society, to maintain the privacy of his personality.'[284]

-

Judge Louis Pettiti of the European Court of Human Rights

8.1 Article 8 – The Right to Respect for Private Life

The right to respect for private life is provided in article 8 of the ECHR.[285] It has been suggested that if one looks at the case law of the European Court on Human Rights, the protection of private life under article 8 covers five different sections: freedom of interference with physical and psychological integrity; freedom from unwanted access to and collection of information; freedom from serious environmental pollution, the right to be free to develop one's identity; and the right to live one's life in the manner of one's choosing.[286] We may thus understand the Court's approach to the notion of 'private life' as wider than the idea of 'personal integrity' or 'privacy' as addressed in chapter 3. The Court has never sought to attempt an exhaustive definition of what the scope of 'private life' is, and has stated that it would be "[…]too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed in this circle."[287] The Court finds that the notion must also " to a certain degree" cover a right to establish and develop relationships, even going as far as covering activities

---

[284] '*Concurring opinion of Judge Pettiti'* Malone v United Kingdom, (App. 8691/79), 2 August 1984, Series A, No 82, (1985) 7 EHRR 14

[285] *'Everyone has the right to respect for his private and family life, his home and his correspondence.*
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.'

[286] N. Moreham, 'The right to respect for private life in the European Convention on Human Rights: a re-examination', [2008] EHRKR ff,45 cited in Jacobs *et al*, *The European Convention on Human Rights* (5th edn, Oxford University Press, New York, 2010) p. 357.

[287] *Niemietz v. Germany* (App. 13710/88), 16 December 1992, Series A No 251-B, (1993) 16 EHRR 97, para 29.

of professional nature seeing as that is where most people interact with other people and create relationships with the outside world.[288]
As we can see from the article itself, the right to respect for correspondence is explicitly protected by article 8. Correspondence does not only refer to written letter sent through the postal system. Case law shows that e-mails and telephonic communications are covered as well.[289] What separates 'correspondence' from being matters of 'expression' under article 10 of the ECHR, is that correspondence means directly communicating with another person.[290]. However, in cases concerning interference with correspondence, the applicant is usually a prisoner and therefore the case law is of little use when discussing surveillance on the broader public.

8.1.1 Restrictions of the Rights Under Article 8

There are limitations to the right to respect for private life and correspondence. These limitations are essentially the same for Articles 8 to 11. Why are interferences on human rights allowed in numerous articles of the ECHR? We must remember that it was States who drafted the Convention- While the individual has rights and interests, these interests needs to be balances with the interest of the community.[291] In the words of the Court: "Inherent in the whole Convention is a search for a fair balance between the demands of the general interested of the Community and the requirements of the protection of the individual's fundamental rights".[292] According to McHarg the relationship between human rights and the interest of the community is "one of the most important issues in contemporary human rights jurisprudence" because here we find the most political or value-laden of the choices that the Court faces.[293]

The limitations that are expressed and that the Court includes in their examinations are: whether the interference was prescribed by and in accordance with the national law; whether the aim pursued is legitimate, *i.e.* if it corresponds to the approved aims in the Article; and lastly, if the limitation is one that is necessary in a democratic society.

8.1.1.1 In Accordance With the Law

When the Court examines whether an interference has been in accordance with national law, it asks three questions.[294] The first question seems simply be "does the interference have any basis in national law?" Secondly, "is the

[288] *Niemietz v. Germany*, *ibid.*, para 29.
[289] *Copland v.United Kingdom*, (App. 3 April 200, (2007) 45EHRR 858, ECHR 2007-IV,, para. 41.
[290] Jacobs *et al*, *The European Convention on Human Rights* (5th edn, Oxford University Press, New York, 2010) p. 361
[291] Jacobs *et al*, *ibid.*, p. 309
[292] Soering v United Kingdom, (App. 14038/88), 7 July 1989, Series A, No 161, (1989) 11 EHRR 439, para 89
[293] McHarg, ' Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights' (1999) 62 MLR 671, 695
[294] Jacobs *et al*, *supra* note 292, p.312

law accessible?" And so the third question, "is the law formulated in a way which enables an individual to foresee, to an under the circumstances reasonable degree, the consequences that the given action will cause?" The last two question pertains to what are called the accessibility and foreseeability tests.[295] These have been described by the Court as the "quality of law" requirements.[296]

The first question is easy to answer. The Court treats this as a simple fact question; is there or is there not a national law prescribing the interference? The law does not have to be statutory, there are cases where a treaty between two countries was in issue, a European Community regulation, or even the rules of a veterinarian council.[297] The Court will always accept the national courts' interpretations unless there are strong reasons for disagreeing and substituting the interpretations with its own views.[298]

As to the two requirements concerning the quality of the law, the following can be said. The accessibility requirement means that the individual must be able to have an indication of the regulations applicable in the given case, and the indication must be adequate in the circumstances of the case.[299] The foreseeability requirement means that the norm may not qualify as being a "law" unless it reaches a sufficient level of precision. Individuals must be able "to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[300] This requirement is not designed to secure absolute certainty on behalf of the individual. Furthermore, it is allowed that the individual may need the proper advice in order to foresee the consequences. As we will see from the presentation of the case law, when it comes to matters of national security, the requirements of foreseeability are looser than what it may be under other circumstances. The court has stated that the level of required precision may vary depending on the "content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed".[301]

8.1.1.2 Legitimate Aims

If the interference passes the requirement of being lawful, we must then make an assessment regarding the legitimacy of the aim pursued. The Court rarely has to make an extensive analysis on the limitations in question, to be convinced that the interference falls within one of the categories mentioned

---

[295] Jacobs *et al, ibid.,* p. 312
[296] In e.g. *Liu v Russia,* (App. 7508/02), 6 December 2007, para 56
[297] Jacobs *et al, supra* note 292, p.313
[298] *Roche v United Kingdom,* (App. 3255/96), 19 October 2005 [GC], (2006) 42 EHRR 599, para 120. *N.B.*, this case concerned Article 6 and restrictions on access to court, but according to Jacobs *et al*, the same principles must apply to articlies 8 to 11; see Jacobs *et al, supra* note 292, p.313 footnote 26.
[299] Jacobs *et al, supra* note 292, p. 313
[300] *Sunday Times v United Kingdom,* (App. 6538/74) 26 april 1979, Series A No 30, (1979-80) 2 EHRR 245, para 49.
[301] *Vogt v Germany,* (App. 17851/91), 26 September 1995, (1996) 21 EHRR 205, para 48

in the Article.[302] The applicants seldom question the aims that the State claims to pursue, and the Court usually finds that a measure is justified as longs as there has been a connection to the specified aims. The specified aims for Article 8 are: national security; public safety or the economic well-being of the country; the prevention of disorder or crime; the protection of health or morals; and lastly the protection of the rights and freedoms of others

While it may thus seem as though the legitimate has little analytical relevance, the specified aims in the Articles will play an important role in the necessity and proportionality assessments that comes next

8.1.1.3 Necessary in a Democratic Society

Having assessed that an interference has been lawful and that it served a legitimate aim, one must then assess whether said interference was necessary in a democratic society for pursuing that legitimate aim. It must thus firstly be shown that the interference is a response to a pressing social need, and secondly that the interference was not greater than what can be deemed necessary to address said pressing social need.[303] The latter part of the necessity test is called the principle of proportionality. The proportionality test has received a formulation of its own in a case from the early 1980's:

> (a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"
> (b) the Contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention
> (c) the phrase "necessary in a democratic society" means that, to be compatible with the Convention, the interference must, inter alia, correspond to a "pressing social need" and be "proportionate to the legitimate aim pursued"
> (d) those paragraphs of Articles of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted. [304]

Within this test we find another terminology of importance: the margin of appreciation. The margin of appreciation and the principle of proportionality are entwined, illustrated by the many cases where the principle of proportionality is used to show that a state has stepped outside of its margin of appreciation.[305] It can be said, however, that while the principle of proportionality concerns the means used to achieve a legitimate aim, the

---

[302] Jacobs *et al*, *supra* note 292, p. 317
[303] Jacobs *et al*, *ibid.*, p. 325
[304] *Silver v United Kingdom*, (Apps. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75), 25 March 1983, Series A No 61, (1983) 5 EHRR 347, para 97
[305] Jacobs *et al*, *supra* note 292, p. 333

margin of appreciation concerns the legitimacy of the aim of the interference for responding to the pressing social need.[306]

Shortly put, the proportionality test is a tool for balancing the interests of the State and the rights of the individual. It has been established in case law that the greater and more far reaching that the interference is, the stronger the grounds for justification has to be.[307] An example would be that weightier reasons are required for sentencing someone to life in prison than sentencing someone to community service. As for the pressing social need served by the State's interference it can be established that if the State interferes for reasons of national security, it will have an easier time justifying it than when it interferes e.g. for the protection of morals.[308]

The margin of appreciation was introduced by the Court in 1976, in the well-known *Handyside* case.[309] The case prompted the Court to consider its own role in examining the necessity of a State's interference, especially for aims of protection of morals.[310] The Court considered that the margin of appreciation is given "both to the domestic legislator ('prescribed by law') and to the bodies, judicial amongst others, that are called upon to interpret and apply the laws in force […] Nevertheless [Articles 8 to 11 do] not give the Contracting States an unlimited power of appreciation. The Court […] is empowered to give the final ruling on whether a 'restriction' or 'penalty' is reconcilable with [the right protected by the Article]" and that the Court's "supervision concerns both the aim of the measure challenged and its 'necessity'[…]".[311] The margin of appreciation will, as was stated earlier, come into play when the Court must make a proportionality assessment, and since the national authorities have a "direct and continuous contact with the vital forces of their countries" they are in a better position than the Court to make an assessment of what the national opinion is and if there is a need for a measure.[312]

The scope or "size" of the State's margin of appreciation depends on whether the State authorities actually were in a better position than the Court to make an assessment of the need for measures which intrudes on the individual's Convention right. It also depends on whether or not there exists a common European ground between the contracting States' law and practice.[313] When the relevant laws and practice differs between the States,

---

[306] Jacobs *et al*, *ibid.*
[307] Kilkelly, 'The right to respect for private and family life – A guide to the implementation of Article 8 of the European Convention on Human Rights' (Council of Europe, 2003), p. 32
[308] Kilkelly, *ibid.*
[309] *Handyside v United Kingdom*, (App. 5493/72), 7 December 1976, Series A No 24, (1976) 1 EHRR 737.
[310] *Handyside* case, *ibid.*, para 22
[311] *Handyside* case, *ibid.*, paras 48-49
[312] *Handyside* case, *ibid.*, para 48
[313] Dijk & van Hoof, *Theory and Practice of the European Convention on Human Rights* (3rd edn, Kluwer Law International The Hague, 1998) p.87

the margin of appreciation could be wider.[314] Furthermore, the nature of the rights or of the activities of the individual may affect the scope of the margin; e.g., more discretion is awarded the State on issues of property rights than on freedom of expression.[315] Discussing the right to respect for private life under Article 8, the Court will give a slighter margin when dealing with issues of personal security and the well-being of the applicant,[316] compared to when the State's interface "would not constitute an obstacle to [the applicant's] leading a private life of his own choosing".[317]

Dijk and van Hoof notices that the margin of appreciation is a cause for concern in as much as it seems that the Court applies a looser proportionality test in more recent judgments.[318] The Court has gone from applying a "fairly strict proportionality test",[319] asking if the reasons for the interference were relevant and sufficient, if there was a pressing social need and if the interference was proportionate to the aim pursued, to now asking whether the interference was "justifiable in principle and proportionate",[320] and if there was a "reasonable relationship of proportionality" between the interference and the legitimate aim sought to be realized.[321]

8.1.2 Case Law

When reading case law concerning means of compulsion in the form of surveillance, one will find that most cases will concern actual tapping in on the telecommunications. While this thesis concerns monitoring of communication *activities* and not the *content*, the available case law is nonetheless relevant in that it gives guidelines on when an intrusion in the form of means of surveillance will constitute a violation of the individual's rights under Article 8, regardless of what type of surveillance it may be.

In an important case from 1978, the *Klass* case, a group of lawyers and judges contested their national legislation regarding surveillance. The applicants claimed that their rights under Articles 8 and 13 had been violated by Germany. I will return to the question of Article 13 in chapter 8.2. As for the question of Article 8 the following can be said. The legislation was constructed so that secrecy for mail, post and telecommunications could be interfered with when regulated in a statute and when needed for the protection of the democratic order or State security. If measures were taken, there was no obligation to notify the individual.

---

[314] Dijk & van Hoof, *ibid.*
[315] Dijk & van Hoof, *ibid.*, p.88
[316] Dijk & van Hoof, *ibid.*, p.89
[317] *Leander v Sweden*, (App. 9248/81), 26 March 1987, Series A No 116, (1987) 9 EHRR 433, para 25
[318] Dijk & van Hoof, *supra* note 315, p.94
[319] Dijk & van Hoof, *ibid.*, p.94
[320] See for example Demuth v Switzerland, (App. 38743/97), 5 November 2002, ECHR 2002-IX, para 43
[321] See for example *Larkos v Cyprus*, (App. 29515/95), 18 February 1999 [GC], (2000) 30 EHRR 597, ECHR 199-I, para 29

As in basically all cases, the applicants did not dispute that the State has the right to have recourse to surveillance measures, meaning that the aim pursued was not contested.[322] Instead they challenged the German legislation in that it permitted means of surveillance without obliging the authorities in every case to notify the persons concerned after the surveillance had taken place, even when such notification could be given without jeopardizing the purpose of the intrusion, and in that it excluded any remedy before the courts against the ordering and execution of such measures.

Firstly, the Court discussed whether or not the applicants could claim to be victims. The Court has consistently held in its case law that it task is not normally to review the way the State has applied the relevant law in general, but rather how they were applied to the applicant. However, owing to the nature of secret surveillance, the court had permitted general challenges to the relevant legislative regime.[323] The Government informed the Court that the applicants had never been subjected to surveillance measures under the contested laws.[324] The system in Germany instituted a system of surveillance where all individuals in the State may potentially have their communications surveilled without knowing if it had occurred or not. This meant that the ”disputed effect directly affects all users or potential users of the postal and telecommunication services” in the state.[325] Furthermore, the mere ”menace of surveillance” could be said to in itself restrict the free communication of individuals through postal and telecommunication services, thus interfering directly with the users’ rights as guaranteed by Article 8. The Court said that if the Convention was to effectively enforce the rights bestowed in it, there must be some possibility to have access to the Court under Article 34 (former Article 25) of the Convention even under said circumstances.[326]

Being satisfied that the applicants could claim to be victims and that there had been an interference under Article 8, the Court went on to examine the substantive complaint. They did this by examining limitations to the rights under Article 8, as described in chapter 8.1.1., in the context of the present case. The interference had been in accordance with the law, leaving the Court to examine whether or not it had been “necessary in a democratic society”. The applicants said that the legislation lacked adequate safeguards against possible abuse and held that the purpose of the requirements on interferences in paragraph 2 of Article 8 where instituted to ensure that the society would not ”slide imperceptibly towards totalitarianism”.[327] The Court noted the need for States to expand their surveillance since

[322] *Klass v Germany*, (App. 5029/71), 6 September 1978, Series A, No 28 (1979-80) 2 EHRR 214, para 10-11
[323] *Klass* case, *ibid.*, para 33
[324] *Klass* case, *ibid.*, para 37
[325] *Klass* case, *ibid*., para 37
[326] *Klass* case, *ibid*., para 34
[327] *Klass* case, *ibid.*, para 47

”[d]emocratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism”.[328] While the Court noted that the States enjoy a margin of appreciation in the way the system of surveillance is operated, the Court must be satisfied that said system contains adequate and effectives guarantees against abuse.[329] While there was no judicial control of the implementation of surveillance, there were several other stages of control: only when there were factual indications for suspecting a person could a measure be ordered, meaning that exploratory or general surveillance was not permitted; surveillance could be ordered only by written application and after a decision thereon by a Federal Minister empowered for this purpose by the Chancellor; the implementation of the measures were under the initial control of an official qualified for judicial office; subsequent control of measures were done at least twice a year by the Parliamentary Board.[330] The nature of surveillance is such that when measures are ordered or implemented, reviews may be carried out without the individual knowing, and this would not go beyond what is necessary in a democratic society. The Court was also satisfied with the subsequent controls in this case. The Court held that it is in principle desirable to entrust supervisory control to a judge, but concluded that because of the nature of the safeguards provided in German legislation the exclusion of a judicial control did not exceed the limits of what may be deemed necessary in a democratic society.[331] The possibility of improper action by a dishonest or negligent official could not be completely ruled out whatever the system, and the Court held that what matters is the likelihood for such abuse and the safeguards provided to protect against it.[332] The Court found no violation of Article 8.

The *Malone* case appeared 6 years later.[333] Malone had been accused of dishonest handling of stolen goods and in the subsequent trial it was revealed that the Post Office had intercepted a telephone conversation. The Post Office had acted on behalf of the police after a warrant had been issued. Malone further believed that his post had been intercepted, and that his telephone had been metered. Metering means using a meter check printer which will record the numbers dialed on a specific phone and the time and duration of each call.[334] The Post Office used metering in its daily activities in order to check that customers were correctly charged. It was disclosed by the United Kingdom that it was not unusual for the Post Office to cooperate with the police and metered telephone lines if “the information is essential to police enquiries in relation to serious crime and cannot be obtained from other sources”.[335]

---

[328] *Klass* case, *ibid.*, para 48
[329] *Klass* case, *ibid.*, para 50
[330] *Klass* case, *ibid.*, para 51-54
[331] *Klass* case, *ibid.*, para 56
[332] *Klass* case, *ibid.*, para 59
[333] *Malone v United Kingdom*, (App. 8691/79), 2 August 1984, Series A, No 82, (1985) 7 EHRR 14
[334] *Malone* case, *ibid.*, para 56
[335] *Malone* case, *ibid.*, para. 56

In a way, the Court's judgment compliments the *Klass* case in that it found a violation based on an unsatisfactory system which was not regulated by statute or its equivalent.[336] However, the discussion on the legality of the interference was focused on whether it had been "in accordance with the law", namely the requirements of precision and foreseeability. The Court stated that the way the United Kingdom had regulated the area lead to a situation where nobody could with any reasonable certainty say what elements of the powers to intercept are incorporated in legal rules and what elements are within the discretion of the executive.[337] There was a vast array of various regulations forming the entire picture. The Court used words such as obscurity and uncertainty regarding the state of the law; England's and Wales' laws simply did not indicate with reasonable clarity the scope and manner of the exercise of the interference conferred on the public authorities. The minimum degree of legal protection to which a citizen is entitled under the rule of law in a democratic society was lacking, thus the interference had constituted a violation of article 8.

Furthermore, since the metering was originally carried out for purposes of correctly charging the uses, the Court held that metering by its very nature is to be distinguished from the interception of communications which is undesirable and illegitimate in a democratic society unless justified. [338] However, the Court did not accept that the use of the data obtained from the metering, regardless of the purpose and circumstances, cannot be an issue under Article 8. The Court found that the metering contained information which is an integral part of the communications made by telephone, meaning that the recording of it constituted an interference with the individuals private life. The practice in England and Wales was that the Post Office would hand out the data even if the police did not have a subpoena, when it was essential for the investigation of serious crimes and could not be obtained through other sources. There appeared to be no legal rules concerning the scope and manner of the exercise of the discretion enjoyed by the public authorities. Again, the Court found a violation under Article 8.

An interesting concurring opinion was put forward by Judge Pettiti, where he said that the dangers that was threatening democratic societies the past decade, *i.e.* 1980-1990, was the temptation that was facing public authorities to "see into" the life of the citizens.[339] Noble aims such as needs of planning and of social and tax policy obliged the State to "amplify the scale of its interferences", computerizing personal data-files in administrative systems. He went on to describe that at a further stage, public authorities will seek to, "for purposes of their statistics and decision-making processes", build a "profile" for each citizen. He described the new technology of phone tapping, where the encoding and decoding in computer processes makes it possible for interceptions to be "multiplied a hundredfold" and analyzed in ever shorter time spans leading to "'mosaic' technique" where authorities

[336] '*Concurring opinion of Judge Pettiti'* in the *Malone* case
[337] *Malone* case, *supra* note 335, para. 79
[338] *Malone* case, *ibid.*, para. 84
[339] '*Concurring opinion of Judge Pettiti'* in the *Malone* case

will shape a complete picture of the "life style of even the 'model' citizen". He wrote of a diversification of the aims that the authorities pursue. Judge Pettiti agreed that there had been a violation of Article 8 in this case, but he was not satisfied with the limitation of the analysis to whether the violation had been in "in accordance with the law". He would have liked to see further analysis, namely on the lack of judicial control which he feels would also constitute a violation of Article 8. The requirement of judicial control over telephone interceptions, he writes, does not stem solely from a philosophical concern over power and institutions, but also from the necessities of protecting private life. Practices of systematic interceptions of communications without having an impartial, independent and judicial control would, according to Judge Pettiti, be disproportionate to the aim sought to be achieved.

The reasoning in the *Klass* and *Malone* cases was developed in the *Huvig* and *Kruslin* cases.[340] Both cases contained essentially the same Court ruling, where the Court examined the system for authorizing telephone-tapping in France; the courts in France would consistently approach the provisions of the Code of Criminal Procedure as authorizing telephone-tapping when implemented by a senior police officer with a warrant issued by an investigating judge. The practice was, according to the Court, in accordance with the law, since the courts had been consistent in this view. The Court did not approve of the quality of the law in that it was not foreseeable enough. The Government had listed seventeen safeguards which they said were provided for in French law, relating to the carrying out of the tapping, how the results were allowed to be used, and the means of having irregularities righted.[341] The Court valued the safeguards, in particular the need for a decision by an investigating judge, who is an independent judicial authority.[342] However, it also noted that only some of the safeguards are provided for by law, others were laid down piecemeal in judgments lapsing over several years, and others yet had not been laid down even in case law. The latter safeguards appeared to the Court to be inferred from general enactments or principles of legislative provisions or court rulings; the Court held that this did not provide sufficient legal certainty in the present context, despite being logical in itself. The Court put extra emphasis on the fact that the French system did not afford adequate safeguards against possible abuse.[343] The Court focused on the following which in the *Valenzuela* case was referred to as minimum safeguards that should be set out in the statute in order to avoid abuses of power: a definition of the categories of people liable to have their telephones tapped by a judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of the telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to

[340] *Huvig v France*, (App. 11105/84), 24 April 1990, Series A, No 176-B, (1990) 12 EHRR 528; *Kruslin v France*, (App. 11801/850), 24 April 1990, Series A, No 176-B, (1990) 12 EHRR 547
[341] *Huvig* case, *ibid.*, para 32
[342] *Huvig* case, *ibid.*, para 33
[343] *Huvig* case, *ibid.*, para 34

communicate the recordings intact and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court. Thusly, the French law, written or unwritten, did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities, constituting a violation of Article 8 of the Convention.[344]

In the *Valenzuela* Case, a woman had been subjected threatening phone calls, some of which were traced to company's telephone.[345] The applicant and four other persons had had access to the telephone. An investigating judge made an order under a provision in the Spanish constitution, whereby the interception of telecommunications was implemented. The surveillance method used was metering.[346] The applicant was considered the prime suspect. The Court, again, decided on a violation of Article 8 due to the interference not being "in accordance with the law", namely lacking in quality.[347] The provision under scrutiny was part of the Spanish Constitution which constituted the legal support for phone tapping. The provision did contain authorization for the courts to decide when phone tapping was permissible, however it lacked more specific limitations and requirements which would have to be fulfilled before the court could hand out an order in each specific case. The Court noted that:

> […] the requirement that the effect of the "law" be foreseeable means, in the sphere of monitoring telephone communications, that the guarantees stating the extent of the authorities' discretion and the manner in which it is to be exercised must be set out in detail in domestic law so that it has a binding force which circumscribes the judge's discretion in the application of such measures.[348]

This requirement would seem every bit as severe as the requirement for interception of actual phone tapping, since in the Huvig case a similar statement was made:

> Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.[349]

---

[344] *Huvig* case, *ibid.*, para 35
[345] *Valenzuela Contreras v Spain*, (App. 27671/95), 30 July 1998, (1999) 28 EJRR 483, ECHR 1998-V
[346] *Valenzuela* case, *ibid.*, para 47
[347] *Valenzuela* case, *ibid.*, para 61
[348] *Valenzuela* case, *ibid.*, para 60
[349] *Huvig* case, *supra* note 342, para 32

Other cases where the Court decided on a violation of Article 8 based on failure to comply with the requirement of "in accordance with the law" is the *Amann* case where the law was to generally stated;[350] the *Halford* case where the telephone of an police employee had been tapped and where there existed no regulation of interception of calls outside of the public network for when employees made private phone calls;[351] the *Iordachi* case where according to the Court the legislation did not reach the requirements set out in *Huvig/Kruslin* case.[352] These judgments means that in essence, the Court will usually 'only' examine whether there has been a violation of the requirement of "in accordance with the law", leaving little case law on the subject of the necessity and proportion of various forms of surveillance. For these assessments one can turn to the *Klass* case and the *Leander* case.[353]

In the *Leander* case it was established that the storage of personal data could constitute a breach of the rights to respect for private life. The applicants had been found unsuitable for employment, after having been subjected to the 'personnel control procedure' which applied to all navy employees in Sweden. This meant *inter alia* that a registry was maintained by the Swedish Security Police (*Säkerhetspolisen*), which contained information concerning their private life. In the end, the Court found no violation of Article 8 since Swedish law contained a system which was sufficiently clear and precise concerning its scope. The Court also found that the system was necessary in a democratic society since it was in the interest of national security. As has been previously mentioned in Chapter 8.1.1.3, States' margin of appreciation is wide in matters of national security, but there must still be adequate safeguards in place. Sweden had a highly structured system of safeguards, which satisfied the Conventions requirements under Article 8.

The *Kennedy* case concerned interceptions on telecommunications. The Court recalled that the powers to instruct secret surveillance is only tolerated to the extent that they are strictly necessary for safeguarding democratic institutions; in practice this means that there must be adequate and effective guarantees against abuse.[354] On the subject of the margin of appreciation, the Court recalled that while the margin exists, it is still subject to the Court to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". The Court recalled that in the *Klass* case, it had held that "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge".[355] In the present case, the Court

[350] *Amann v Switzerland*, (App. 27798/95), 16 February 200, (2000) 30 EHRR 842, ECHR 2000-II
[351] *Halford v United Kingdom*, (APP. 11855/85), 21 June 1997, (1997) 24 EHRR 523, ECHR 1997-III
[352] *Iordachi and others v Moldova*, (App. 25198/02), 14 September 2009
[353] *Leander* case, *supra* note 319
[354] *Kennedy v United Kingdom*, (App. 26839/05), 18 May 2010, para 169

[355] *Kennedy* case, *ibid.*, Para 167, with reference to the *Klass* case, *supra* note 324, para. 56

highlighted that the Investigatory Powers Tribunal ('IPT'), which was the controlling body, had an extensive jurisdiction where it could examine any complaint of unlawful interception and, unlike many other domestic systems, such as the one discussed in the *Klass* case, any person who suspected interception could apply to the IPT. This meant that the jurisdiction of the IPT did not depend on the notification to the individual that there had been an interception.

8.2 Article 13 – The Right to an Effective Remedy

The right to an effective remedy is provided in article 13 of the ECHR.[356] Article 13 aims to secure that the individual is provided with a system through which she can obtain relief at the national level when her Convention rights have been violated, before filing a complaint before the Court.[357] It is not a prerequisite for the application of Article 13 that a Convention right is in fact violated; the Article merely requires that when an individual considers herself to have been prejudiced by a measure allegedly in breach of the Convention, there must be an available remedy before a national authority for an examination of the case and for possible redress.[358] The applicant must nonetheless show an arguable complaint in order for her to be able to file her complaint of a violation of Article 13.[359] When determining if a remedy is effective or not it is irrelevant if the complaint is successful or unsuccessful at the domestic level. Nor do the remedies have to be judicial but they must, however, be effective; e.g., an Ombudsman procedure may be enough to satisfy the requirements of the ECHR.[360] However, in the case of a non-judicial procedure, the guarantees that the process affords the individual must be taken under consideration. The body conducting the process must, of course, be sufficiently independent from the authority which it investigates.

The Court has indicated that when examining the effectiveness of the provided remedies, one must look at the context in which the complaint is made. For example, when investigating an instance of secret surveillance the remedy must only be "as effective as could be having regard to the restricted scope for recourse inherent in any system of secret surveillance" and that an examination of the remedies would therefore entail whether they are effective in this limited sense.[361] Furthermore, while there might be a

[356] *'Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity'*
[357] *Kudla v Poland*, (App. 30210/96) 26 October 2000 [GC], (2002) 35 EHRR 198, ECHR 2000-XI, para. 152
[358] *Klass* case, *supra* note 324, para 64
[359] Jacobs *et al*, *supra* note 292, p. 135-136
[360] Jacobs *et al*, *ibid*.
[361] *Klass* case, *supra* note 324, para.69

situation where a single remedy will not, in itself, meet the requirements of article 13, the aggregate of remedies under the system might do so.[362]

In the case of secret surveillance where issues concerning rights under Article 8 would arise, the Court would have already made an examination of the way the remedies operate under the assessment of the necessity of the interference in a democratic society. It would then seem unclear how an examination under Article 13 could differ from the one under Article 8. In a case on secret surveillance where the Court had found under its examination on compliance with Article 8 that the control system had been acceptable, the Court stated that "[i]n such a situation, the requirements of Article 13 (art. 13) will be satisfied if there exists domestic machinery whereby, subject to the inherent limitations of the context, the individual can secure compliance with the relevant laws".[363] This interface between Articles 8 and 13 is the reason why an inspection of the right to effective remedy is of interest for this thesis.

8.2.1 Case Law

Going back to the *Klass* case, the applicants also alleged a violation of their rights under Article 13. There had been no violation of Article 8, but the question was nevertheless if the German law afforded the applicants an effective remedy before a national authority as prescribed in Article 13. The Court observed that the applicants had enjoyed an effective remedy in so far as they actually had challenged the legislation before the deferral Constitutional Court.[364]As regards an effective remedy in relation to the implementation of the surveillance measures, the Court noted that the examining authority did not have to be a judicial one. The Court further noted that the applicants' views meant that in order for a remedy to be effective, the individual would have, by means of subsequent information, to defend herself against any inadmissible interference with her rights. Regarding this aspect the Court has held and holds, "albeit to its regret", that secret surveillance is necessary in modern society which faces new threats.[365] Since the Convention must be read as a whole, the Court could not arrive at an interpretation of Article 13 which "would arrive at a result tantamount in fact to nullifying its conclusion that the absence of notification to the person concerned is compatible with Article 8[…]" in order to ensure effective surveillance.[366] The lack of notification therefore did not constitute a breach of Article 13.

Furthermore, the Court noted that pursuant to the Federal Court's judgment in the applicants' case before it, the competent authority was bound to inform the concerned individual as soon as the surveillance had been discontinued and notification could be made without jeopardizing the

[362] *Leander* case, *supra* note 319, para 84
[363] *Leander* case, *ibid.*, para 79
[364] *Klass* case, *supra* note 324, para 66
[365] *Klass* case, *ibid.*, para 68
[366] *Klass* case, *ibid.*

purpose of the measure.[367] This meant that a number of legal remedies before the courts were available to the individual. The Court found that the aggregate of remedies satisfied the requirements of Article 13, and that it was "hard to conceive of more effective remedies being possible".[368] Thus there had been no violation in this regard either.

In a case concerning Sweden, the *Segerstedt-Wiberg* case, the applicants had requested to view the information gathered about them by the Swedish Security Police. The information had been stored for different reasons for each of the applicants. One might note that for the first applicant, there was no violation of the right to respect for private life since the data was necessary to store for her own protection, has she had been the victim of bomb threats, thusly qualifying as necessary for the prevention of crime. As for two of the other applicants, there had been a violation of Article 8; the data stored on them were 30 years old and regarded political activities in the late 60's meaning that it was not necessary for the protection of national security to keep the data. The Security Police refused to give them any information, but the applicants had been partially successful in retrieving some information when trying to reach this information by going through different public authorities and administrative courts. The refusal to hand out the information to the applicants had however not constituted a violation of article 8.

While there was no violation of any of the Convention rights when the Security Police rejected the request to view the information since they were pursuing a legitimate aim, *i.e.* national security, also falling under a State's margin of appreciation, [369] the Court was not satisfied with the remedies that the State of Sweden offered. The remedies available were the Parliamentary Ombudsmen, the Chancellor of Justice, the Data Inspection Board, and lastly what is nowadays the Commission on Security and Integrity Protection. Neither the Board nor the Commission constituted effective remedies.

The Court stated regarding the Commission that it was a body specifically empowered to monitor on a day-to-day basis the Security Police's entry and storage of information and compliance with the Police Data Act, but it had no competence to order the destruction of files or the erasure or rectification of information kept in the files.[370] The Court also noted that while the Board may examine complaints by individuals, it is not itself empowered to order the erasure of unlawfully stored information but can make an application for such a measure to the county administrative court.[371] Sweden had not shown that the Board was an effective remedy since no information had been furnished to shed light on the effectiveness of the Board.

---

[367] *Klass* case, *ibid.*, para. 71
[368] *Klass* case, *ibid.*, paras. 70 and 72
[369] *Segerstedt-Wiberg and Others v. Sweden*, (App. 62332/00), 6 June 2006 (2007), 44 EHRR 14, ECHR 2006-VII, para. 104
[370] *Segerstedt-Wiberg* case, *ibid.*, para. 120
[371] *Segerstedt-Wiberg* case, *ibid.* para. 120

The Court remembered what it had said about the Parliamentary Ombudsmen and the Chancellor of Justice in a previous case concerning Sweden, *i.e.* the *Leander* case. In that case, the Court had not been satisfied with these two bodies alone since they did not have the authority to render a legally binding decision.[372] Furthermore, the two bodies conducted a general supervision of public authorities, and were not specifically aimed towards investigating the conduct of secret surveillance and the storing of the gathered intelligence. In the case before us, the Court did note that the two bodies "have competence to receive individual complaints and have a duty to investigate them […]" and that their statements "[…] command great respect in Swedish society and are usually followed".[373] The Court noted that since this case, the Chancellor of Justice had been enabled to award compensation with the possibility of judicial appeal against the dismissal of a compensation claim.

In the light of these considerations, the Court found that the applicable remedies, whether considered on their own or in the aggregate, could not be said to satisfy the requirements of Article 13.

Going back to the *Leander* case, one could note that the Court, in the end, had *not* found a violation of article 13, based on the aggregate or remedies which were the Parliamentary Ombudsmen, the Chancellor of Justice, the available parliamentary control of sorts and lastly the way the applicant had contacted the Government by letter. In the partially dissenting opinions of Judge Pettiti and Russo, the two judges held that "[…]even when combined, ineffective remedies cannot amount to an effective remedy where, as in the instant case, their respective shortcomings do not cancel each other out but are cumulative.[…]In our view, it is not essential to make it a mandatory requirement that the authority responsible for hearing appeals should be able to award damages, but it is absolutely essential that an independent authority should be able to determine the merits of an entry in the register and even whether there has been a straightforward clerical error or mistake of identity - in which case the national-security argument would fall to the ground."[374]

8.3 Article 10 – Freedom of Expression

It has been suggested that the traffic data retention pursuant to the Directive is also a violation of article 10, *i.e.* the freedom of expression. While this thesis regards the conflict between data retention and privacy, it would be negligent to not at least mention the arguments for why blanket data retention might violate European citizens' right to freedom of expression. Freedom of expression as guaranteed by the ECHR means the freedom to not only hold an opinion, but also the freedom to disclose and receive

[372] *Leander* case, *supra* note 319, para. 82
[373] *Segerstedt-Wiberg* case, *supra* note 371, para. 118
[374] *'Partially Dissenting Opinion of Judges Pettiti and Rosso'* in the *Leander* case

opinions, ideas and information.[375] As with Article 8, the rights under Article 10 is restricted. The second paragraph of the Article states that the freedom of expression may be restricted if prescribed in legislation, and the restriction is necessary in a democratic society, in the interest of e.g. national security or public safety or for the prevention of disorder or crime. There are other permissible grounds for restricting the freedom of expression; they are, however, not relevant here. Since there is the requirement that the restriction must be one of necessity for a democratic society, an obstruction must pass the proportionality test that we remember from the previous chapter on Article 8.

The blanket retention of communications traffic data would constitute an indirect obstruction of this freedom. As indirect obstructions go, they are only considered under article 10 if they "clearly hinder" the free communication of e.g. ideas. We are communicating more and more via technological instruments, and with some people we even exclusively communicate with the instruments that are being monitored, e.g. on a forum one frequents for discussing specific topics such as politics. Psychologically, you might feel less free to write on the same web forums you previously did knowing that your activity will be in a registry, or you may feel hesitant towards contacting a journalist with insider information knowing that there is a risk that the phone call may be traced back to you. Patrick Breyer writes that blanket data retention may be in violation of the right to freedom of expression under Article 10 of the convention.[376] He argues that the knowledge among the public that their communication activities are being monitored may have a harmful 'chilling effect', where the individuals will no longer communicate in the same manner that they used to.[377] Breyer notes that the fact that traffic data may be accessed "at will" may dissuade both providers and recipients of sensitive information [378] He considers the benefits of traffic data retention to be marginal whilst the negative effects on the freedom of expression are staggering; thusly blanket retention of traffic data falls short of being proportionate and is "incompatible" with the right to freedom of expression under the ECHR.[379]

[375] Breyer, ' Telecommunications Data Retention and Human Rights: The Compaitibility of Blanket Traffic Data Retention with the ECHR' (2005), 11 ELJ 365, p. 373
[376] Breyer, *ibid.*, pp. 373-374
[377] Breyer, *ibid.*, p. 371
[378] Breyer, *ibid.*, p. 373
[379] Breyer, *ibid.*, p. 374

9 Traffic data retention in context

'The tragedy of our day is the climate of fear in which we live, and fear breeds repression.'

-

Adlali Stevenson, Speech to the American Legion Convention, New York, 25 August 1952.[380]

This chapter has been named 'Traffic Data retention in Context'. With this is meant an attempt to put blanket retention of traffic data in the context of the implications of and reasons for surveillance in general.

9.1 History and Globalization of Surveillance

> Among the achievements of the scientific revolution are formidable technical aids which can be used for prying into the private lives of others, for obtaining and recording information they want kept to themselves[…]. It is obvious that these developments constitute a serious potential threat to the privacy of the individual, and this threat is all the more grave when, as is usually the case, the person concerned has no means of knowing either that information is being collected about him, or the use which is being made of it.[381]

The above paragraph was written by UNESCO in the 1970's and seems to be getting more valid as time and technology progresses. It was in the 1960s and 1970s that privacy issues began to gain some interest in public policy issues.[382] This was due to the two main characteristics of the era: bureaucratization and information technology. The states became more computerized in its functions and communication, which required the progress of public policies. Three dimensions of the reason to promote privacy can be distinguished: humanistic, political and instrumental.[383] Humanistic in the way that reason to promote privacy issues is to protect the dignity, integrity and individuality of each individual.[384] Political in the sense that privacy is an important cornerstone in a democratic society by preventing an all-encompassing politicizing of life.[385] It does so by promoting freedom of association, shielding the field of science from governmental interference, permitting secret ballots, controlling improper

[380] As quoted in "Democratic Candidate Adlai Stevenson Defines the Nature of Patriotism" in Lend Me Your Ears : Great Speeches In History (2004) by William Safire, p. 81
[381] UNESCO,' The Protection of Privacy', (2007) XXIV No 3 ISSJ 413, p 421
[382] Bennett, *The Privacy Advocates- Resisting the Spread of Surveillance* (MIT Press, Cambridge, 2008), p. 6
[383] Bennett, *ibid.*, p. 4
[384] Bennett, *ibid.*, p. 4
[385] Bennett, *ibid.*, p. 5

police conduct and keeping the press, and other institutions scrutinizing the government, free. Lastly, it is instrumental, which refers not as much to the collecting of data as it refers to the use of collected data; data may only be used by the right persons for the right purposes and when any of those conditions are absent, the rights of the individual are at risk of being violated.[386] In the 1970s, and since, states would identify the issues as concerns of information privacy, or data privacy.[387] While some laws in most countries would be dubbed as privacy acts, they have historically concerned the information dimension of the privacy issue meaning the processing of data. This has been done with the assumption that the courts will deal with the other aspects. It also seems as though the legislators, in general, are more persuaded by arguments of the instrumental kind rather than the humanistic approach, which is more abstract. There is more of a political appeal to concerns of inaptly processed personal data. And so the discourse of the 1960s and 1970s still effects policy making today.

Lyon writes that surveillance in its ancient forms served either census or taxation purposes and was relatively simple.[388] As times progressed, civil and census registrations helped set up a limited set of rights in that such registration helps granting civil rights, but at the same time it constituted a measure of social control since states may gain "informational power" over its citizens this way.[389] Lyon describes this as ambiguous and paradoxical characteristics of surveillance, adding that surveillance as such does not automatically translate into overreaching control. Lyon states that in the 20th century surveillance underwent changes related to new technologies as described above.[390] The "infrastructural basis of contemporary surveillance" was shaped by the technological developments with e.g. searchable databases, where the technology enabled, but did not cause, certain features of globalization and global surveillance to occur.[391] As technology and modern occurrences globalized, so did surveillance globalize with it.[392] Lyon identifies the attack on the World Trade Center in 2001 as one of the most prominent events for the globalization of surveillance, which is proven by two surveillance areas.[393] One is all of the proposed measures of states for meeting the terrorist threat with measures such as technologically advanced ID cards, CCTV with facial recognition, and other biometric identification tools. The other consequence is the rapid expansion seen in multiple states of anti-terrorist legislation, which relaxes preexisting laws with stricter limitations, e.g. laws on message interception. Surveillance developments are happening simultaneously in several countries around the world.[394]

---

[386] Bennett, *ibid.*, p. 5
[387] Bennett, *ibid.*, p. 6
[388] Lyon, 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) *International Sociology* 19, p. 136
[389] Lyon, *ibid.*, p. 136
[390] Lyon, *ibid.*, p. 139
[391] Lyon, *ibid.*, p. 139-140
[392] Lyon, *ibid.*, p. 144
[393] Lyon, *ibid.*, p. 143-144
[394] Lyon, *ibid.*, p. 144

When discussing legislation surveillance, we must acknowledge both sides of the coin. On the one side, the legislation makes privacy interferences legal by allowing the state authorities to interfere with individuals' privacy. On the other hand, the law regulates and contains the authorities' surveillance activities, allowing it only under certain conditions. Without any legislation on surveillance, surveillance could be used haphazardly. Surveillance is not merely of negative value for the individual: it may e.g. give a feeling of safety by constituting the "necessary glue that builds trust throughout a society of strangers."[395] While the common conception of surveillance in everyday language would be the observation of activities of subjects under suspicion, it would be more suitable to refer to it as the "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered".[396] The retention of traffic data for invoicing purposes thus is a form of surveillance, with the benefit of easing the individuals means of communication. Some have described surveillance as integral to the development of disciplinary power and of the modern nation state and new forms of governance.[397] As society advances, surveillance measures seem to advance too. In 1989, Flaherty made a comparative analysis, wherein Sweden was one of the studied countries, where he claimed that the central theme of his work was that "individuals in the Western world are increasingly subject to surveillance through the use of databases in the public and private sectors, and that these developments have negative implications for the quality of life in our society and for the protection of human rights".[398] Bennet argues that there is an important distinction to be made between the routine collection of personal data and the analysis that will follow the retention.[399] With this he means that whereas the retention is a feature of modern societies, e.g. whenever one makes a credit card purchase, surfs the Internet, or makes a call from a cell phone, the "everyday capture and storage of such data is qualitatively different from the use of that data to determine whether the person [...] would or would not be a credit risk, [...] may or may not be downloading child pornography, or is or is not a terrorist threat".[400] Bennett recommends that the analysis of the risks of surveillance makes a distinction between the routine data retention and the subsequent use of that data. However, one must note that in this respect, it seems as though Bennett has his focus of discussion on the general surveillance of modern society, *i.e.* surveillance measures acted out by public as well as private actors. By private actors is meant e.g. airline companies, credit card companies, etc.

---

[395] Bennett, *supra* note 384, p. 11
[396] Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, Buckingham, 2001) p.14
[397] Bennett, *supra* note 384, p. 11
[398] David Flaherty, *Protecting Privacy in Surveillance Societies* (The University of North Carolina Press, Chapel Hill, 1989), p.1
[399] Bennett, *supra* note 384, p. 17
[400] Bennett, *ibid.*

In a comparative study made on the attitudes towards surveillance in various countries, some interesting conclusions were made.[401] The survey showed that there exists a disconnection between the public's awareness on legal and technical means to protect ones privacy and the actions of the public, where governments will not hesitate to legislate on privacy interfering measures with national security as the justification.[402] The study demonstrated that immediately after the attack on the World Trade Center in 2001, people in general, *i.e.* not only in the United States, were more willing to "sacrifice personal privacy for the sake of national security".[403] A few years later, they no longer responded as positively towards the introduction of surveillance legislation. Lyon worries about the apparent willingness to give up privacy for the sake of public safety.[404] If one is willing to do so, one ignores the wider consequences of the structure of the surveillance which is based less on individual behavior and more on constructing profiles from mass flows of electronic data.[405] He criticizes one claim which is often repeated, that if we have done nothing wrong, we in turn have nothing to hide and therefore nothing to fear.[406] This is not how things work, Lyon writes, because against the claims of individual innocence, "surveillance practices are profoundly social, in the sense that persons are clustered into categories […] as potential lawbreakers. It is one's often unwitting membership of or association with certain groups which makes all the difference".[407] Prior to 11 September 2001 the concerns that Lyon brings up were related to consumer relationship management only, but since 2001 these issues have gotten more attention "in the light of expanded security imperative" pursued by our governments.[408] However, there is evidence that despite the massive changes made in US legislation pursuant to the famous Patriot Act of 2001, the US public was not well-informed about the intent and nature of the act.[409] Studies were made which showed that the more a citizen actually knew about the act, the less supportive she was of it.[410] The support of the Act despite a low rate of knowledge concerning its scope may be explained by the "relentless stream of media stories about the threat posed by international terrorism [which has] underscored [the surveillance's] apparent necessity".[411]

In an article on electronic monitoring (EM) equipment as a surveillance measure during probation, Corbett and Marx writes about certain 'technofallacies of electronical salvation', meaning fallacies which

---

[401] Zureik *et al*, *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (McGill-Queen's University Press, Montreal, 2010
[402] Zureik *et al*, *supra* note 403, p. 277 & 358
[403] Zureik *et al*, *ibid.*, p.358
[404] Lyon, David, 'Surveillance Technologies: Trends and Social Implications', *The Security Economy* , pp.s 127-148 (OECD, Paris, 2004)
[405] Zureik *et al*, *supra* note 403, p. 276
[406] Lyon *supra* note 406, p.140
[407] Lyon, *ibid.*, p.140
[408] Zureik *et al*, *supra* note 403, p. 277
[409] Zureik *et al*, *ibid.*, p. 121
[410] Zureik *et al*, *ibid.*
[411] Zureik *et al*, *ibid.*

characterize efforts to use technology to deal with social issues.[412] While they indeed are intended to describe fallacies on EM, some may be seen as applicable to surveillance measures in general. One of them is the fallacy of the explicit agenda, which entails that new programs are presumably developed for the declared purpose, and that there even is a clear purpose.[413] Apparently, policy decisions may even declare a reason while other considerations are underlying, which may give varied, contradictory or shifting goals. Another fallacy is that of novelty, where anything new is undoubtedly better than the old.[414] They write that "decisions are often based on newness rather than on data suggesting that the new will work or that the old has failed", which shows that it is important to appear up-to-date.[415] It seems as though the fallacy of 'intuitive appeal or surface plausibility' is connected to the one of novelty; a policy is adopted because it seems positive that it would work and emphasis is put on so called "commonsense 'real-world' experience" rather than on evaluative research.[416] There is also the fallacy of technical neutrality.[417] It includes the assumption that technology is morally and ethically neutral *per se* where the only bad consequences will depend on how it is used. Cabott and Marx writes that this fallacy can lead to a stop in critical thought and that it "ignores the fact that the technology is always developed and applied in a social context which is never neutral".[418]

Two terminologies are likely to come to mind when discussing surveillance: Orwell's 'Big Brother' and Bentham's 'Panopticon'. Taylor writes that the allusion of a 'Big Brother' is a popular modern metaphor because it describes the role of the State in social control.[419] However, he notes that the 'Big Brother' discourse ignored "the numerous benefits" that increased surveillance brings about.[420] I order for citizens to be able to accept and consent to surveillance, the State may not have unlimited discretion for determining when it will carry out surveillance and there must be opportunities to hold the State legally accountable for its actions. The idea of the Panopticon was an all-encompassing surveillance regime where the prisoners knew they were being watched. The Panopticon "operates anonymously, neutrally, flexibly"[421] The people who are subject to the surveillance will be shaped to a norm because even though they might not be specifically surveilled at a given moment, they still think that they are being watched and will adjust their actions and behavior thus. Lyon argues

[412] Corbett & Marx, 'Critique: No Soul in the New Machine: Technofallacies in the Electronic Monitoring Movement' (1991), *Justice Quarterly* 8, p. 401
[413] Corbett & Marx, *ibid.*, p. 402
[414] Corbett & Marx, *ibid.*, p. 404
[415] Corbett & Marx, *ibid.*
[416] Corbett & Marx, *ibid.*, p. 405
[417] Corbett & Marx, *ibid.*, p. 409
[418] Corbett & Marx, *ibid.*, p. 409
[419] Taylor, 'State Surveillance and the Right to Privacy' (2002), *Surveillance and Society* 1, p.66
[420] Taylor, *ibid.*
[421] Lyon, 'Benthams Panopticon: From Moral Architecture to Electronic Surveillance', Queens Quarterly 98 (1991), p. 607

that the discussion should be moved away from the idea of society slowly becoming Panopticon-like, [422] because surveillance today is more about 'synopticism' meaning that it is no longer only about a powerful body watching common citizens.[423] While panopticism refers to the few watching the mass, synopticism refers to the mass watching the few.[424] Surveillance can be made by states on their citizens or huge credit card companies on their customers, but it can also be peer-to-peer or citizens observing, through mass media, the everyday activities of celebrities and political leaders. Surveillance today is often, in the words of Haggerty and Ericson, "a mile wide and an inch deep" and could be described as rhizome.[425] However, Lyon also writes that panopticism should be seen as "one tendency among others, albeit one augmented technologically today".[426]

9.2 Current Surveillance in Sweden

A Swedish citizen today already faces retention of such traffic data which is necessary for the service provider for invoicing purposes; this the telephone or internet user has agreed to when purchasing the service. It now seems possible that the same citizen will be subject to blanket retention of data not necessary for invoicing purposes, but for crime fighting purposes.

It is argued by some that the Swedish public was less accepting of infringement on privacy just some 30-40 years ago.[427] For example, in 1983 it was suggested that the registries of various public authorities should be coordinated in order to make a census of population and residences instead of choosing the regular but more complicated and expensive way of sending out and gathering paper forms.[428] The suggestion was severely criticised and retracted.[429] Yet, in 1995, the very same suggestion was brought up again,[430] this time passed by Parliament without any public debate. It seems as though the public, at least the Swedish public, stopped being interested in concerns on privacy. Two explanations have been offered.[431] The first one is convenience; while we know that our movements can be traced via our cell phones and our purchasing habits via the use of our credit cards and online shopping, we still stick to using these modern items and services because we save time and effort. The second one is the offered sense of security. People are willing to sacrifice their privacy if it means that they are safer for it, e.g.

---

[422] Lyon, *ibid.*, p. 608
[423] Haggerty & Ericsson, ' The Surveillant Assemblage' (2000) *British Journal of Sociology* 51, p. 618
[424] Mathiesen, 'The Viewer Society: Michel Focault's "Panopticon" Revisited' (1997), *Theoretical Criminology* 1 , p 218-219
[425] Haggerty & Ericson, *supra* note 425 pp. 614 & 617-618. *N.B.* A rhizome is a plant which grows its roots horizontally, and shoots up roots and leaves over a large area.
[426] Lyon, *supra* note 423, p. 614
[427] Olsson, *supra* note 3, p 12
[428] Prop. 1983/84:85
[429] Statistics Sweden, Background Facts, Forty years of regional statistics from Statistics Sweden, p.15
[430] Prop. 1995/96:90
[431] Olsson, *supra* note 3, p. 14

through camera surveillance. Why is it that we accept more and more surveillance if the argument of public safety is used? Firstly, the increased media coverage of crime may be an explanation. While some people may fail to realise it, these headlines sell issues of the magazine and if one does not realise the commercial conditions of the free media one may get the wrong impression of the actual climate in society. Another explanation may be that people trust in the government is increasing. We trust that it has our best interests in mind and would not abuse its powers.

Swedish citizens have in the last few years seen an expansion in Swedish surveillance legislation which may have made some 'circles' more critic against privacy infringing measures yet again. Besides blanket retention of traffic data, there are two other surveillance measures which have produced great discussion in Sweden: the FRA Act and the IPRED Act.

The FRA Act was technically not as simple as the passing of one new act, but rather a new act which imposed several changes to already existing legislation. As a result of this new act and the accompanying changes, the FRA (the National Defence Radio Establishment*, Försvarets Radioanstalt*) is now permitted to monitor signals that are transmitted cross-border through cable; previously, the FRA was permitted only to monitor communications transferred through the ether. The government and its bodies would be able to instigate such surveillance without prior consent from an independent body or court. The justification for the changes was the change in the external threat against Sweden. The government felt that, as opposed to the threats during the cold war, the contemporary threats are those of terrorism and various types of organized international crime; these threats are usually transnational, non-military and do not seldom emanate from a non-state actor.[432] Due to these modern threats, there therefore had to be a change in the way Sweden gathers intelligence. There are a few remedies available regarding the FRA Act. Two of them are not available under 'the regimen of the Electronic Communications Act': the Data Inspection Board and an inspection board on military intelligence (*Statens Inspektion av Försvarsunderrättelseverksamhet*).

Before the discussion in the implementation of the Directive, Swedish service providers would already store much of the data which the Directive defines as obligatory to retain. This has been used as an argument by members of parliament who are for the directive.[433] While the Directive secures the future storage of such data it also ensures a regard to integrity aspects such as the fact that the data is stored for only a limited period of time whereas before in Sweden no definitive time limits were expressly stated in the legislation, thusly providing an integrity aspect in favor of the data retention. While the current Swedish government has been slow in implementing the Directive, members of parliament from the opposition,

[432] Prop. 2006/07:63, s 17

[433] Riksdagens Protokoll 2008/09:139 (2009-08-20). See '*§8 Svar på interpellation 2008/09:574 om lagring av trafikdata'*

who were active in the establishment of the preceding Framework Decision, questioned the government's reluctance to implementing the Directive while being positive towards the FRA Act.[434] The essence of the criticism is that the FRA Act went further in interfering with privacy, since it meant taking part in the content of the communications, while the Directive merely secured the retention of data which were already retained by the service providers. The answer was that the delay was due to the public debate on privacy that Directive had spawned in Sweden[435] The difference between the FRA Act and the implementation of the Directive was emphasized; the activities of the FRA do not fall into the area of law enforcement activities but rather the area of intelligence gathering.[436] The information gathered pursuant to the FRA Act only concerns communications crossing the Swedish borders and may not be stored.

The IPRED Act, which has been called the 'Pirate Hunter Act', is short for Intellectual Property Rights Enforcement Directive, and as the name suggest the Act is an implementation of Directive 2004/48/EC on the Enforcement of Intellectual Property Rights. The purpose of the directive was to harmonize the Member States' legislation to ensure a high, equivalent and homogeneous level of protection in the internal market.[437] While there were several changes made to already existing legislation, the most controversial one regarded the amendments in the laws on who may request and partake in information on suspected file sharers. Holders of property rights are entitled to seek court orders obligating a service provider to hand out information on origin and distribution networks when the right holder can show that they have good grounds for suspecting an individual of infringing their rights.[438] This means that e.g. a commercial trade association may request to receive IP-addresses and subscription information pertaining to the IP-addresses, when they *suspect* somebody of file sharing.[439]

Besides the implementation of the Directive, the FRA Act and the IPRED Act, there have been a continuous stream of legislation in the area of means of compulsion and surveillance, which entail a need for assessments on potential privacy interferences. Already in 2005, the Chancellor of Justice

---

[434] Riksdagens Protokoll 2008/09:139 (2009-08-20). See '*§8 Svar på interpellation 2008/09:574 om lagring av trafikdata'*, anf. 22 Thomas Bodström (S)
[435] Riksdagens Protokoll 2008/09:139 (2009-08-20). See '*§8 Svar på interpellation 2008/09:574 om lagring av trafikdata'*, anf. 23 Justitieminister Beatrice Ask (M)
[436] Riksdagens Protokoll 2008/09:139 (2009-08-20). See '*§8 Svar på interpellation 2008/09:574 om lagring av trafikdata'*, anf. 25 Justitieminister Beatrice Ask (M)
[437] Directive 2004/48/EC, The Preamble, recital 10
[438] Act on Copyright in literary and Artistic Works (*Lag (*1960:729) *om upphovsrätt till litterära och konstnärliga verk*), chapter 7, articles 53c and 56a
[439] The Swedish Supreme Court has referred a case to the ECJ, since it found a conflict between the Directive on data retention and the Directive 2006/24/EC on data retention and Directive 2004/48/EC on property rights enforcement – according to Directive on data retention, only law enforcement authorities would be permitted to access to information on IP-adresses, which would render the IPRED Act null and void in this aspect. Mål nr Ö 4817-09, 2010-08-25, available at https://docs.google.com/fileview?id=0B9fZz4FtBBY8MmY5YjZmYzEtOGMzZS00MGQ4LWFmYWYtOTI2YWM0ZjMwNWZh&hl=en&pli=1 accessed on 11 June 2011

expressed great concern regarding the fact that there are several simultaneous establishments of inquiry committees and changes in legislation which are processed in separate rounds of referrals for considerations, something which he has repeated since and which he referred to in his considerations on the implementation of the Directive.[440] The Chancellor stated that if one considers the inquiries and propositions individually, it is fairly easy to be convinced that there is a societal need which outweighs the interest of the individual. He feels confident that had the consideration bodies been presented with the opportunity to review all of the various propositions for the legislation on only one occasion, their considerations would be more negative. The Chancellor requested an all-encompassing analysis on the total effect on personal integrity by all means of surveillance in Sweden.

[440]JK, ”Remissyttrande över promemorian Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet” (Ds 2005:21)”, Dnr 3485-05-80, 2005-09-30. Repeated in” Remissyttrande över delbetänkandet (SOU 2005:38) Tillgång till elektronisk kommunikation i brottsutredningar m.m.” and in ”Betänkandet (SOU 2007:76) Lagring av trafikuppgifter för brottsbekämpning”

10 Analysis

10.1 Introduction

It was argued in chapter 9 that the public will be more accepting of surveillance measures if the State uses the idea of an imminent external threat, from which the State wishes to protect the democratic society. I do not argue the need for law enforcement authorities to make use of surveillance measures in gathering intelligence on new forms of crime, even though one may have doubts regarding the evidence on why data retention is necessary. Regardless of such consideration, there is another factor which may make data retention more acceptable for some. As we have seen throughout this thesis, the data to be retained is to a large extent such data which was already retained by the service providers for billing purposes. Some argued that the shift in purposes for retaining the data is alarming in itself, but it may nonetheless be so that the public will have gotten used to the fact that the traffic data from their communications is being stored. Thusly, an individual could in theory find the retention of data no less interfering than the commercial retention which is already happening. Had this data not been stored beforehand and the public was to be faced with data retention pursuant to the Directive from, so to speak, 'square one' it is highly doubtful that discussions on the EU level would have gone unnoticed by the public until the day when it became clear that all States had to implement a directive on data retention.

One must always keep in mind that surveillance is a vital tool for law enforcement authorities to protect the democratic society and its citizens. Accessing communications traffic data is becoming more and more important for fighting crime as the communication pattern in modern society changes; this conclusion can be easily drawn from simply looking at the digits in the latest Swedish parliamentary control on surveillance measures. The instances where the law enforcement authorities need this data has increased drastically the last years. It would be foolish to suggest that all surveillance amounts to, in the words of Lyon, "overreaching control". While surveillance is ultimately a form of social control, it can nevertheless be something from which we all benefit as a society. Problems will not occur until the surveillance is disproportionate to the legitimate aim which the State wishes to reach. Furthermore, the State must be honest with what its aims are and make sure that a shift in purposes does not happen over time. If we remember the 'technofallacies' which Corbett and Marx wrote of, we understand how paramount it is for States to have a good basis for all the measures they implement and not put too much faith in technology as 'neutral' because it will always be applied in a social context. It is the way the human applies the technology which is of importance; here we will therefore always find a risk of abuse. The only way to decrease the risk is through providing effective safeguards.

Lyon argued to move away from the idea of a Panopticon, and the discourse on surveillance today seem to move towards describing surveillance as rhizome, mainly thanks to Haggerty & Ericson, where the hierarchies between observer and observed vary more today than they did only 30 years ago. However, it seems premature to completely rid oneself of the idea of Panopticon in the discussion on surveillance when it is done in an automated manner. For example in Sweden, the citizens do not only risk to face blanket traffic data retention of their communications, but it will happen in combination with such laws as the FRA act and the IPRED act, among other modes of surveillance. Most citizens would at least have heard of these new acts, knowing that it affects their telephone and online communications, even if they do not know the specifics, especially concerning the details on who will access the data and for what purposes.

The idea of what should be held within a person's private sphere is to a large extent subjective, although attempts on general definitions have been attempted, as seen in chapter 3 of this thesis. Collste concluded, through Parent, that an infringement on integrity exists when data, which the majority would not want to be made public had the data been about themselves, is made public. Why is it that this is a suitable description of what should be kept private, or at least part of a suitable description? I chose to present this idea on personal information which should not be interfered with, because it is, in my opinion, a step on the way towards recognizing the most important aspect of privacy: developing your person. There is one aspect of surveillance which we cannot get away from: the idea that surveillance not only detects crime, but prevents it. Neighbourhoods are designed to increase neighbour participation in surveillance to deter burglars from breaking and entering. CCTV cameras are clearly put up not only to catch video footage of crimes, but also to deter people from e.g. vandalizing; huge posters are put up inside and outside of buildings using CCTV cameras to make it clear to anyone that should they attempt anything criminal, they will be caught on video. Surveillance thusly inhibits certain behaviour. One of the biggest fears of a homosexual person with homophobic parents and relatives may be that her sexual orientation would be revealed – could this fear prevent a Bulgarian citizen from contacting HBTQ-hotlines or discussing her orientation on internet forums now that data on her communications are being retained? Would a person living in a religiously conservative society feel free to participate in online discussion holding secular views, when no longer being able to assess the security of anonymity online? I argue that when you are aware of that your daily activities are being surveilled, you may in the end inhibit your daily behaviour, however innocent your habits may be. This is related to the chilling effect of which Breyer spoke. Breyer focused on the freedom of expression as an example on how democracy as a whole may be affected by surveillance measures. Surveillance thusly not only risks inhibiting personal development of individuals, it may also inhibit the democratic society that it originally is attempting to protect.

We find ourselves living in an information society. Part of the new idea of surveillance being rhizome nowadays is that anything you would like known about yourself is spread instantly. The second you post any information online, it is available world-wide. The three principles mentioned in chapter 3, *i.e.* limiting State interference, protecting personal data and protection of private zones, are suddenly not enough. For example, updating your Facebook status informing everyone that you are heading to the outpatient clinic due to illness means that anyone can take this personal information and spread it. You are shaping the idea of who you are, perhaps not only in order to display an idea for other of who you are but also for figuring out for yourself. With ehese types of personal information, we are ourselves responsible for keeping private or for making known to others. What we proclaim about ourselves, we do not see as interferences in our privacy or 'private spheres'. The problem with retention of traffic data is that it is not as easy for the individual to understand what the gathered information is exactly and what it says about your personal life. It is not as easy to control what information is stored regarding your personal life anymore, nor is it desirable on the State's behalf that the individual should learn to do so. The State "wants" to interfere, in order to retain data and map out suspicious activity.

One of the consequences that blanket retention of traffic data seems to have had is that criminals start using various means for becoming anonymous. I argue that a surveillance measure is only necessary in so far that it is useful. To use an example from two centuries ago, in the late 19th century England a system was developed whereby records were matched by name; the problem was that criminals would easily falsify their names. On this it was said that "registration is of no use, and might as well be got rid of at once".[441] The quote is an easy way to express the main arguments of some of the opponents of data retention; people with criminal intent will easily, and already do, find ways to circumvent the surveillance that is data retention. One obvious example on how to remain anonymous in your communications is to simply buy internet minutes at the local 7 Eleven, whereby the traffic cannot be traced to you as the specific user of the service. Another way, which has been brought up by the government in the proposition but which they felt they could not regulate the use of because it would be to extensive an interference, is to simply use prepaid cell phone services rather than the usual post-paid methods where your name is linked to the SIM-card via your subscription. However, data retention seems to have had a severe consequence: the increase of tools for being anonymous on the Internet. It is of little concern when innocent individuals use these methods, but when we find that criminals use tools for becoming anonymous while committing or plotting acts of crime, the consequences seem more severe. For example, criminals may make use of virtual private networks ('VPNs'). There will still be traffic data ensuing from the activities on the network, however the data will be strongly encrypted with technologies akin to that which banks use to encrypt their data. Firstly,

[441] Hastings, G.W. *Adress on the Repression of Crime* (Spottiswoode and Co., London, 1875), p.13

attempting to decrypt the data requires finding the key to the encryption which is time consuming and expensive to such an extent that effectively no one will attempt to decrypt the traffic. If this was not the case we would not see encryption being used on such a large scale in commercial applications. Secondly, if e.g. a group of pedophiles share child pornography through use of VPN tunnels, they will most likely never 'step outside' of the safe environment of the VPN thusly ensuring that there never will be any unencrypted data for the law enforcement authorities to notice in the first place. Even though the pedophiles may be scattered around the globe, the VPN tunnels will essentially render their network untouchable to anyone wanting to pry. This is a way to have your criminal activity go totally unnoticed. Anyone with the will and the money to get the technological know-how can make use of this technology.

The avoidance behavior of criminals will in the end effect all investigations negatively, in that other surveillance measures are rendered ineffective. For example, the reliance by criminals on pre-paid cellphones will render regular phone tapping less effective. The use of VPN tunnels will render several instances of child pornography offences to go unnoticed. One could thusly argue that not only is data retention not effective in itself as a surveillance measure, it also results in previously used investigatory tools to be less useful.

On a closing note, it is not hard to see the vicious circle which may ensue from this situation. As criminals find ways of eluding the surveillance, the States will feel inclined to legislate yet more extensive and interfering measures of surveillance, which in turn will encourage criminals to take further measures in evading the surveillance. In the end, we are moving forward *and* backward.

10.2 The Convention Rights

Please note that the analysis on Sweden's compliance with its obligations under the Convention will have the regulations in the Electronic Communications Act as its focus, whereas the regulations in the Code of Judicial Procedure will be referred to as a matter of comparison.

10.2.1 Article 8

In the chapter on Article 8, we found that five main categories of specific rights and freedoms can be said to fall under the right to respect for private life. The issue of data retention could possibly fall under the category of 'freedom from interference with physical and psychological integrity'. Within this category we would also find e.g. instances of forced physical examinations, searches of property, and recording and disseminating pictures.[442] It may seem that the category of 'freedom from unwanted access

[442] Jacobs *et al*, *The European Convention on Human Rights* (5th edn, Oxford University Press, New York, 2010) p. 363-373

to and collection of information', but it seems that personal information in this sense refers more to when public authorities collects and stores information regarding daily activities such as membership of organizations or political activities, or when the police retains fingerprints, DNA, photographs etc.[443] It is however possible that retained traffic data may unveil such information, e.g. what your political affiliation is. Furthermore, one could argue that it falls under the freedom to develop a personal identity, where everything from the right to find out the identity of your biological parents and giving your children your family name to enjoying your culture and being free to have whatever sexual orientation you have, [444] since you might feel hindered to contact e.g. your local LGBT rights group by fear of having the communication registered and stored by your communications service provider. Either way, the retention of traffic data would *per se* fall under the scope of Article 8 regardless of what subcategory we would want to fit it into.

There is one basic question to answer firstly though, an question to which I could not find any answer in the case law: is the retention the actual surveillance, or would it not constitute surveillance until somebody accesses the data and starts interpreting it? While case law does not really address such an issue, since no such issue has arisen, it seems quite clear to most of us that the retention in itself would constitute the surveillance measure, whereas the access to the data and the pursuant 'puzzle-making' is only an issue on how the information from the surveillance is used.

This leads us to another issue, which interestingly was brought up in the *Klass* case. When is a person a victim? In this case, the Court argued that since the German system was built in a way where nobody had any way of knowing if they were surveilled because no notification would be given when the surveillance was over. Since it meant that anyone could have been surveilled, all were potential victims since, as we remember the Court saying, the effect directly affects all users of postal and telecommunication services in the State. It seems rather obvious that data retention, which covers every single user of electronic communications, would make it possible for anyone to bring a case to the Court. Undeniably, every single citizen has been monitored. Furthermore, the *Malone* case concerned metering of telephone activities, where the information would be much the same as the part of the retained data concerning telephone communications. Here we found the Court saying that the information which was gained from metering constituted an integral part of the communications made by telephone, and that such a recording thusly constituted an interference. It seems clear that retention pursuant to the Directive far exceeds, interference wise, the intrusion that the metering constituted in the *Malone* case.

[443] Jacobs *et al*, *The European Convention on Human Rights* (5th edn, Oxford University Press, New York, 2010) p. 374
[444] Jacobs *et al*, *The European Convention on Human Rights* (5th edn, Oxford University Press, New York, 2010) p. 377-388

Here follows an account on what I believe to be the issues the Court may focus on in an assessment of data retention as an interference, and possibly a violation, of the rights under Article 8. Here I will use the steps set out in chapter 8.1.1 on the delimitations of Article 8, and in each step I try to predict what the Court may or may not approve of.

10.2.1.1 In Accordance With the Law?

As we recall, the first step of the test on accordance with domestic law is to ask oneself whether the interference has any basis in national law. When, or if, the proposition is passed by the parliament in 2012, the interference would be regulated in the Electronic Communications Act. This means that the simple fact question can be answered with a simple 'yes'.

The second and third part of the test was the accessible and foreseeable. The Swedish government proposes a rather detailed regulation on what data to retain. It is my belief that had the regulation in this regard been regulated in a more detailed way, it would become obsolete more quickly than is desirable. This was also the governments basis for having more exact details regulated in regulations issued by the government. A comparison between the suggestion of the Traffic Data Investigation and the final proposition shows that there has been a substantial upgrade in accessibility and foreseeability in this regard. In the Traffic Data Inquiry, the committee held that all further information on what type of data to retain should be accounted for in regulations issued by the government, rather than having any detail at all in the legislation.

One might think that the technical terminology in the legislation would mean that it is not foreseeable for the individual, but as we learnt in chapter 8.1.1.1, it is allowed that the individual may need proper advice in order to foresee the consequences.

There is one part of the proposed legislation that may raise concern in this context: the regulations on the access to the traffic data. Again, in chapter 6 Article 16(c) of the Electronic Communications Act refers to two different Articles already existent in Swedish law: one of the Articles is in the Electronic Communications Act, and the other in the Code of Judicial Procedure. While the Code of Judicial Procedure is sufficiently clear in this regard on whom the police may issue secret tele-monitoring, the referred to Article in the Electronic Communications Act might not be if the Court was to look at the case. The legislation seems to be clear in that it requires a suspicion of a crime of a certain magnitude. But as we saw in the chapter comparing the two separate regulations on access to the data, one of the negative aspects of the Electronic Communications Act is that it does not require any actual suspects. It seems as though the individual not only will have their traffic data retained without any suspicion of having done anything, the data may also be accessed without any suspicion of having done anything. It is thusly unforeseeable in that the individual will have no idea what conduct, *i.e.* communications with whom, may lead the law enforcement authorities to look up your data and putting together the puzzle

of your life for the last six months. Another issue in this regard is the possibility of a 'base station depletion'. Here the individual is left with absolutely no possible way of foreseeing that the data on her will be accessed. It is not even a matter of being at the wrong place at the wrong time, but a matter of being in the wrong larger area at the wrong time. The *Huvig and Kruslin* cases showed us that the Court considered necessary, *inter alia*, a clear definition of people liable to have their telephones tapped by a judicial order. Now, while all citizens will be under the general surveillance that is the data retention, not all of us will be victims of the second interference where the data is accessed. An issue for the Swedish legislation here is that there is no clear definition, as discussed above, on the people liable to have their data accessed by the authorities.

We may note the *Malone* case, where the violation was found under the test of 'in accordance with the law'. The case concerned metering of telephone communications, which is part of the data which will be retained pursuant to the Directive. Here the Court found a vast array of legislation which together compiled the entire picture, thusly making it impossible for the individual to predict or foresee the scope and manner of the exercise of interferences. Clearly, this constituted a violation of rights under Article 8. However, another violation of rights under Article 8 was found because of the lack of obligation for the police to have a subpoena before requesting the data from the Post Office – the Court was clearly not satisfied with the lack of legal rules concerning the scope and manner of the exercise of the discretion enjoyed by public authorities and would most likely not be satisfied with the Swedish situation under the Electronic Communications Act. While the rules of the Code of Judicial Procedure clearly requires a court decision before requesting the data, Article 16c of chapter 6 of the Electronic Communications Act requires no such thing. The police may go to the service provider without any prior control necessitated by the legislation.

In fact, the Electronic Communications Act lack several of the minimum safeguards set out by the Court in the *Huvig and Kruslin* cases, later referred to in the *Valenzuela* case, while the regulations of the measures in the Code of Judicial Procedures satisfies all the requirements. The Electronic Communications Act does have a limit on the duration of the telephone tapping, at least indirectly since the data is only to be stored for six months. And indeed, it does regulate the nature of the offences which may give rise to access to the data, but it does not require that a judicial order is issued. Furthermore, it does not regulate a definition of people liable to have their communications and habits mapped out through use of the retained data by a judicial order, there are no procedures for summary reports containing intercepted communications and there are no regulations on how to transmit the data to the requesting authority. This is a consequence of the lack of regulations in the Directive on how the data may be accessed. One may note that at the time the Framework and the Directive were drafted, there was still the distinction between the first and third pillar of the EU, which since has been eliminated pursuant to the Lisbon Treaty. This, along with the

history of the telecommunications market going from state monopoly to a private market, is the reason why the Electronic Communications Act lacks several of the minimum safeguards which the Court requires. The only reasonable solution for Sweden,is to make use of the BRU inquiry and make the Code of Judicial Procedure the only gateway to the retained data.

From the case law, we saw that the Court is inclined to find violations under this first test, meaning that one will not often find a case concerning the necessity of measures in a democratic society. If a Swedish case on this issue ever gets to the Court, it thusly seems that we run the 'risk' of having the Court finding a violation of rights under Article 8 based on a failure to show that the measures are in accordance with the law. This would in a sense be unfortunate, since the really interesting topic is the one on whether the measure is necessary in a democratic society.

10.2.1.2 Legitimate aim?

Should the Court be satisfied with the foreseeability of the legislation, it will move on to looking for a legitimate aim.

There seems to be little analytical relevance to this test, since the Court is usually short in their assessment of this aspect. Furthermore, applicants seldom question the aims that the State claims to pursue. We therefore must simply find the connection between the interference and one of the specified aims in the Article. The matter is simple: blanket retention of electronic communications traffic data has as its aim to investigate and prevent serious crime. There is thusly a legitimate aim which is acceptable under Article 8.

10.2.1.3 Neccessary in a Democratic Society?

Being satisfied that there is a legitimate aim, the Court will assess the necessity of the retention.

In summary, there are several steps to this test in the case law.

- Is there a pressing social need?
- Is the measure proportionate to the legitimate aim pursued? This means balancing opposing interests of the individual to have her privacy intact, and the State's interest in investigating crime.
- Does the measure fall within the State's margin of appreciation?

One must also have in mind when arguing, that being 'necessary' is not synonymous with being 'indispensible', nor does it mean that the measure may merely be 'useful', 'desirable', 'admissible', etc. While on the subject, it should be pointed out that through the critique from the EU level, as presented in chapter 5.4, it seems as though the evidence on data retention as a necessary tool in the fight against 'modern' criminality has not adequately proven the point of necessity. Rather, it seems as though the Commission's report only shows that it is 'useful' and that States appreciates having the tool.

On the issue of a 'pressing social need', we noted in chapter 8.1.1.3 that the need served by the State's interference will be more easily justified in matters of national security than in other matters. The Swedish government did not press on national security as a reason for the retention, but rather the need for law enforcement authorities to use retention as a vital tool in the fight against serious crime, such as world encompassing organized crime. However, if the argument is that States face modern threats, such as organized crime and terrorism, and need new tools in order to fight these new types of threats, then the State could pass this part of the test.

We now move on the proportionality test, within which the discussion of the margin of appreciation would fall. We must balance the State's interest of using surveillance measures to reach the legitimate aim of investigating serious crime, against the individual's interest of respect for her private life. We noted in chapter 8.1.1.3 that the State will give a slighter margin when it is an issue of personal security or well-being, compared to when the State interference would not constitute an obstacle to the applicant's leading a private life of her own choosing. One could argue that the retention of traffic data would not create obstacles in how the applicant may lead her private life. The data is already 'created' through our normal communications. It does not hinder anyone from communicating, nor does it interfere with the content of the communication. As we learned from the case law, monitoring communications is an interference on the same level as looking at the content at the communication, meaning that while one might instinctively think that since the content is protected the surveillance is not as intrusive, in fact the Court would look at it as surveillance nonetheless. Furthermore, it is very well arguable that the retention of traffic data indirectly creates obstacles in the way a person conducts her life, since there are indications that people avoid calling e.g. marriage counselors or suicide hotlines once they are aware that there communications are being logged. This would reduce the margin of appreciation for the State. On the other hand, if the State would claim that the measure is needed for reasons of national security, rather than the general category of fighting crime, the margin would again be rather wide. There has been no talk of national security so far though, only the fight against serious crime. Again, on a third note in this matter, we find that in the *Klass* case, the Court noted that States did enjoy a wide margin of appreciation in the way the system of surveillance is operated, but that the Court must be satisfied that the system contains adequate and effective safeguards. If one considers this statement carefully however, it does not seem to mean that any type of surveillance is permitted as long as there are adequate safeguards – it merely suggests that it is completely up to the state to decide what safeguards to use and how to build up the system of safeguards. It does not imply that States enjoy a wide margin of appreciation in their choosing of measures of surveillance.

It seems from the case law presented in this thesis that the effect of the necessity test has been to guarantee that all states have comprehensive legislation on its surveillance measures. This is a frustrating approach for anyone who is interested in the actual proportionality assessment between

the opposing interests of the State to surveil in order to gain intelligence on criminal activities and the individual's interest of having her private affairs undisturbed. It seems as though Court has settled for an approach where the proportionality between the two interests are adequately addressed if the domestic legislation provides safeguards of a certain adequacy and effectiveness in domestic legislation or other regulations. Let us therefore look at the safeguards in the case law which satisfied the Court and later look at the way the Swedish legislation provides safeguards. This will be an answer with two parts, since we have two separate ways of gaining access to the data and thusly two separate ways of safeguarding the individual's interest. The analysis will concern Sweden and not the Directive itself, because the EU cannot, as of yet, be brought to the Court since the changes envisioned by the Lisbon Treaty are still in process.

We learned from the *Klass* case that the Court approved of a system where written applications had to be made on which a Federal Minister had to make a decision after having been empowered to do so be the Chancellor. The implementation of the decision was then under the control of an official who qualified for judicial office and the Parliament had subsequent yearly controls over the measures. There was no violation of Article 8 since the Court was satisfied with the control prior to the surveillance as well as the subsequent controls. The fact that the individuals could not be notified was due to the covert nature of surveillance; as long as there are adequate safeguards decreasing the potential for abuse the Court could find no violation. Sweden would have to base their arguments on the fact that surveillance is of a covert nature, wherefore access to the data via the Electronic Communications Act will not motivate any notifications to the individual; Sweden is already notifying individuals subsequent to secret tele-monitoring as stipulated by the Code of Judicial Procedure. There are no reasons why the same should not be the case for the accessing of data which is retained pursuant to the Directive, since the nature of the data is the same.

In the *Leander* case the Court found no violation of Article 8 after having made a necessity assessment. The Court gave Sweden a wide margin of appreciation based on the fact that the surveillance system was instituted in the interest of national security, which is not an argument under the retention of traffic data. Even though we speak of serious crime, we speak of crime nonetheless and not national security. It is important to make this distinction, so as to not make two separate discussions one and the same which would result in the State enjoying a wider margin of appreciation than it should. In the *Kennedy* case, the Court clarified that, as it at held in the *Klass* case, surveillance is a field where the potential for abuse is so easy in the individual cases and may have detrimental consequences for the democratic society as a whole; therefore it is important to have some supervisory control before a surveillance measure is implemented, preferably by a judge. The Court was satisfied with the safeguard, which included the IPT. One should also remember the concurring opinion by Judge Pettiti in the *Malone* case, where he wrote that the possibilities that

new technology brings to map out an individual's life through systematic interceptions of communications means that there must be instituted an impartial, independent and judicial control. Otherwise, the system is disproportionate to the aim pursued. An individual in Sweden will have recourse to judicial control subsequent to interferences under the Code of Judicial Procedure. She will not have such possibilities prior or after the traffic data is accessed pursuant to the regulation in the Electronic Communications Act.

In conclusion, Sweden is, as the legislation stands today, in breach with its Convention obligations. The Code of Judicial Procedure stands its ground well; it is the Electronic Communications Act which falters. This is a fact which does not depend on the implementation of the Directive, however the implementation would make the possible consequences more severe as there will be more available data. It is strongly advisable that Sweden makes use of the BRU inquiry prior to any implementation of the Directive, in order to reduce the possible consequences for the individual.

10.2.2 Article 13

It was stated in chapter 8.2 that an analysis on the right to effective remedy is necessary due to a statement from one of the judgments by the Court where it held that since it had been satisfied with the safeguards in domestic legislation under its assessment on Article 8, an analysis under Article 13 must be made to see whether the there exists a domestic machinery whereby the individual can secure that the laws scrutinized under Article 8 are being followed. Even if the State is found to violate Article 8 due to a lack of safeguards, an analysis of compliance with Article 13 will still be made, albeit shorter than had there been adequate safeguards in legislation.

Naturally, covert surveillance will raise some issues as regards remedies. The nature of surveillance is often brought up, wherein it being 'secret' is vital to it being valuable. When making an assessment on whether the remedies are effective, it is important to keep in mind that surveillance measures requires special consideration.

The individual will have little use of available remedies, no matter how effective they are when applied, if there is no notification subsequent to when the surveillance measure has been carried out. In the *Klass* case, the State had not breached Article 13 when it did not give notifications. One should remember that there were several other remedies available, of a quality which satisfied the Court, and that the Court concluded that a lack of notification had not been considered a breach of Article 8 wherefore it could not constitute a breach of Article 13 either since the Convention must be read as a whole. However, as has been noted in the analysis on Article 8, Sweden already gives notifications under procedure regulated in the Code of Judicial Procedure – it would be hard for Sweden to argue that it deemed it necessary to give notifications in one case of surveillance measures, but not

in the other. Especially since secret tele-monitoring basically gives the same data as will be retained pursuant to the Directive.

As deduced from the comparison between the Electronic Communications Act and the Code of Judicial Procedure, the individual is left with two possible remedies if she suspects her data has been illicitly accessed pursuant to the Electronic Communications Act: the Parliamentary Ombudsmen and the Chancellor of Justice. Remembering the case of *Segerstedt-Wiberg*, we can assume these two bodies will not be considered as effective enough remedies: not in and of themselves and not in the aggregate. They have no judicial authority, except the Chancellor who may award compensations with possibilities for judicial appeal should the compensation claim be dismissed.

The *Leander* case came earlier, and also concerned Sweden. Herein the Court had, yet again not been satisfied with the Parliamentary Ombudsman or the Chancellor of Justice in and of themselves, but since there were two other remedies the Court remained satisfied that the State had not breached Article 13. As the government noted in its reply to the critique from the bodies of referral, there will be a supervisory body who will control the conduct of the service provider and ensuring the technological aspects of the retention. However, in the words of the dissenting opinions of Judge Pettiti and Russo in the *Leander* case: ineffective remedies cannot amount to an effective remedy, even if they are combined, when they in no way cancel out each other's shortcomings. In the case of access to data pursuant to the Electronic Communications Act, the shortcomings of the available remedies are cumulative: there is nowhere for the individual to turn in order to get a satisfactory judicial examination ensuring that her rights have been respected in the retention of her communications traffic data. This should be compared to the rules under the Code of Judicial Procedure: the individual will somehow receive notification and has the opportunity to turn to her local court or to a supervisory authority (*i.e.* the Commission on Security and Integrity Protection). The Parliamentary Ombudsmen and the Chancellor will only be extraordinary bodies in this sense, and will add value the remedy system. In the case of the Electronic Communications Act, they will constitute the remedy system. Clearly this will not satisfy the Court.

Once again, Sweden is in breach of its obligations and, once again, the easiest way for Sweden to ensure compliance with the Convention is to instigate legislation as per the suggestions made in the BRU inquiry. The remedy system already exists; it is simply a matter of using it for all measures of surveillance.

10.3 Final Words

The standard of protection for the right to respect for private life can be said to be the one set out by the European Court of Human Rights. As we have seen in chapter 10.2.1 and 10.2.2 , I believe that the blanket retention of

traffic data violates Article 8, and that the Swedish system of remedies violates Article 13.

I argue that it is not sufficient to merely look at the safeguards that the domestic regulations provide, but now more than ever it is important to initiate the idea of looking at surveillance as a whole and the ensuing consequences. We have gone from surveillance being used only on people who are suspected of illicit conduct to everyone having their communications and whereabouts monitored regardless of suspicion. Lyon criticizes the notion that if we have done nothing wrong we have nothing to hide from the State and therefore have nothing to fear in terms of consequences from the surveillance. This then is the wrong way to go about things since the consequence we should fear is the fact that surveillance is a form of social control where people are being clustered into groups and categorized as potential lawbreakers. The problem for us as individuals is that we will most likely not know that we are part of such a group which according to Lyon makes all the difference. This is especially the case with access to data pursuant to the Electronic Communications Act: the data on your communications may be accessed without you having been suspected of a crime. You may be a relative to 'the wrong person' or perhaps you happened to end up at a social gathering with 'the wrong people' without realizing it. Since there are no suspicion conditions, there is no way of conducting your habits and communications in a way that you, a non-criminal, can ensure that data on your communications will not be accessed.

One may refer to the Chancellors opinion in the matter, when he wrote that had the bodies for referral had the opportunity to have a gathered look at all of the propositions and inquiries currently circulating, they would have had a more negative approach when assessing the consequences that surveillance measures has on personal integrity. I argue that the same goes for the Court. It is desirable, from a human rights law point of view, to start taking into account the entire picture. A privacy advocate could argue that the opposing interests are not assessed properly through looking at whether the legislation provides safeguards for the individual's privacy. Instead, a full analysis is required, at least once, where we look at all surveillance measures available to the state authorities, and what their gathered impact on the individual's interests are. Separately, the surveillance measures will easily appear necessary. Put together, the assessment may render the opposite result. Are all the available surveillance measures necessary? Are there really no alternatives to blanket retention of data which is more suitable, considering that the surveillance that the individual already is subjected to? Has the State ever done an adequate assessment on the gathered effect on privacy that their surveillance measures do have on the individual? It may be argued that it is a difficult feat to asses such impacts – then again, if the Sweden feels it has done adequate assessments in each and every single piece of proposition for surveillance measures, then surely it should not be an impossible feat to make a gathered analysis. If the State benefits from the full framework on surveillance that exists domestically and has the possibility to use information from each measure in an

investigation on one person, then surely the full impact of all of these measures on the individual should be taken into consideration. The Court said itself in the *Klass* case that the reasons for the delimitations of Article 8 were instituted to ensure that society would not "slide imperceptibly towards totalitarianism". Also in the inspiring concurring opinion by Judge Pettiti in the *Malone* case from nearly 20 years ago, where he warned against disregarding the possibility that new technology brings for authorities to shape a complete picture of the "life style of even the 'model' citizen".

Nevertheless, if Sweden wishes to comply with its obligations under the Convention when it decides to implement the Directive, it should make sure that the changes proposed by the BRU inquiry are carried through before such an implementation. As long as there is such a major discrepancy in what could be expected by Sweden as a democratic State and the safeguards it actually provides for its citizens, Sweden is in direct breach of their obligations under Article 8.

As we all know, an individual has the option to exhaust all domestic remedies and take her case to the Court. However, the Court does not have the power to repeal an EU legislation. The individual could only win or lose a case in relation to her state. A decision by the Court would thusly not affect the Directive itself. As explained in chapter 4, there is an interface between the Member State, the EU and the Court of Justice of the EU, and the European Convention on Human Rights and its Court. While the General Court expressed that being directly concerned by an EU measure meant that a person is individually concerned when the measure affects her legal position in a manner which is both definite and immediate. One could again argue what 'definite' could mean, but it is of no use for this aspect of the thesis: the Court of Justice dismissed this approach by the General Court. So in the end, while the changes of the Lisbon Treaty make it theoretically possible for an individual to bring her claim even on general measures, in reality she will have a hard time arguing that she is directly concerned. The other way to reach the judgment of the Court of Justice would be to go through the domestic system, where the domestic court could refer the case to the Court of Justice in order to get an opinion on the compliance of the Directive with both the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. This is how the privacy advocacy group Digital Rights Ireland Limited got their case to the Court of Justice, so there will soon actually be a judgment from the Court of Justice on the compliance between the Directive and the rights under the Convention.

We have learnt that the Convention is intertwined with the EU in several ways. Furthermore, since the work on EU regulation on data retention started back in 2005, where Sweden was a vital part of the force for the framework, the status of the rights in the Charter have gained a stronger legal position in the EU. As for now, the Court of Justice will only be bound by the Charter of Fundamental Rights of the European Union, and the

Convention and its case law will merely serve as an 'inspiration' on the interpretation of the legal situation. The rights guaranteed by the Charter shall however be at least of the same level as the rights afforded by the Convention and its case law when there are corresponding rights in the Charter. This is the situation with Article 8 and the rights to respect for private life. This did not mean the same as the case law of the Court being binding for the Court of Justice, since this would produce a confusing, and, from the EU point of view but perhaps not from the human rights lawyer's point of view, undesirable hierarchy. What we are left with is a starting point, which says that the Court of Justice will aim to guarantee what the Court has guaranteed, without binding itself fully to such a commitment. There have been plenty of arguments from internal EU bodies on why the Directive itself does not, as it stands today, comply with the Convention, that the Court of Justice could not conceivable dismiss the Court's case law in the matter. It seems, albeit perhaps hopeful, that the Court of Justice would likely call for the Directive to be, if not repealed, at least amended. The Court of Justice should call for more conclusive evidence for the need of blanket traffic data retention, as per the EDPS' requests. If evidence of high enough quality is not presented in order to prove the necessity of the retention, then the Court could not, on good grounds, deem the Directive to be proportionate in the measures it takes to pursue its aim.

As for Article 13, it does not have any corresponding right in the Charter. This means that the Court of Justice does not have to take into consideration the Convention nor the Court's case law. There is no reason for the question on remedies to be taken to the Court of Justice. In any case, it is better addressed by the Court as the matter of available remedies for citizens is a domestic concern. It is my understanding that cases on the individual-state relationship should be taken to the Court. In cases on the suitability of e.g. the Directive, or other EU measures, it is better to put the means and the focus on getting the case to the Court of Justice, since this is where the real power to repeal measures is situated.

Perhaps the Commission will have finished its investigatory work and will propose amendments of the Directive before the Court of Justice has a chance of making a judgment in the matter. As of the entry into force of the Lisbon Treaty of 2009, the divide between the first and third pillar have been abolished. This means that the EU may regulate law enforcement activities, e.g. by adopting a new Directive which encompasses not only details on what data to retain, but also conditions as to how and for what reasons law enforcement authorities may access the data and how they may use it. If such regulations were put in, and if they were of a sufficient standard, it is possible that the blanket retention of traffic data may be assessed as proportionate and necessary. The Commission would only repeat its mistakes if it did not take this chance to regulate the entire matter of data retention, which includes how the data is to be accessed and used.

After having finished this thesis and taken part in studies carried out in the matter of the effectiveness of data retention pursuant to the Directive, I am

of the opinion the Directive should be repealed in favor of e.g. quick-freeze methods. One issue which this thesis has not looked further into, is what would happen with the already existing implementations in Member States: would a repeal simply mean that the legislation which have been passed now are left without any limitation to what data may be retained, for how long the data may be retained, and for what purposes? This was one of the issues that the Directive set out to address, the un-harmonized retention of traffic data. Regardless of the answer to that question, my opinion is that the retention pursuant to the Directive is counter-productive of the aim which it pursues, since it apparently increased the awareness and the will of criminals to 'hide' using available technological tools. We must find other ways of reaching the aim.

Supplement A

REMISSYTTRANDE

Datum
2008-03-04

Dnr
8771-07-80

Regeringen
Justitiedepartementet
Enheten för brottmålsärenden och
internationellt rättsligt samarbete (BIRS)
103 39 STOCKHOLM

BETÄNKANDET (SOU 2007:76) LAGRING AV TRAFIKUPPGIFTER FÖR BROTTSBEKÄMPNING

Departementets dnr JU/2007/95907BIRS

Inledning

Justitiekanslern har granskat förslagen i betänkandet utifrån de synpunkter som Justitiekanslern främst har att beakta. Genomgången ger inte anledning till några andra synpunkter än de som redovisas nedan.

Dubbla regelverk avseende utlämnande av historiska trafikuppgifter

Enligt utredningens förslag får de uppgifter som operatörer ska vara skyldiga att lagra lämnas ut enligt både 27 kap. 19 § rättegångsbalken och 6 kap. 22 § första stycket 2 och 3 lagen om elektronisk kommunikation.

Utredningens förslag aktualiserar det faktum att utlämnande av historiska trafikuppgifter enligt gällande rätt kan ske med tillämpning av såväl RB 27 kap. 19 § som 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation. Beredningen för rättsväsendets utveckling (BRU) har i delbetänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38) föreslagit ändringar i rättegångsbalken och lagen om elektronisk kommunikation. Justitiekanslern har lämnat synpunkter på det betänkandet i ett remissvar den 8 december 2005, dnr 4667-05-80. BRU:s förslag bereds för närvarande inom Justitiedepartementet (dnr JU2005/4823/Å).

Justitiekanslern anser att det är otillfredsställande från rättsäkerhetssynpunkt att det finns två olika regelverk för utlämnande av historiska trafikuppgifter. Enligt Justitiekanslerns uppfattning är det därför angeläget att beredningen av det aktuella ärendet samordnas med beredningen av BRU:s förslag avseende utlämnande av historiska uppgifter. Vad gäller BRU:s förslag

Postadress
Box 2308
103 17 STOCKHOLM

Gatuadress
Birger Jarls Torg 12

Telefon (växel)
08-405 10 00

Telefax
08-723 03 57

E-post
registrator@justitiekanslern.se

hänvisar Justitiekanslern till de synpunkter som har framförts i det lagstiftningsärendet.

Ärendet har föredragits av föredraganden Nedim Salcic.

Göran Lambertz

Bilaga:
Justitiekanslerns remissvar, dnr 4667-05-80, avseende delbetänkandet SOU 2005:38

Bibliography

Primary Sources

The European Union

Primary Law

- Treaty of Lisbon amending the Treaty on the European Union and the Treaty establishing the European Community [2007] OJ C306/1
- Consolidated Version of the Treaty on the European Union [2010] OJ C83/13
- Consolidated Version of The Treaty on the Functioning of the European Union [2010] OJ C83/47
- Charter of Fundamental Rights of the European Union [2010] OJ C83/389

Secondary Law

- Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24 October 1995 [1995] OJ L208/31
- Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States [2002] OJ L190/1
- Parliament and Council Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L195/16
- Parliament and Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or public communication networks and amending Directive 2002/58/EC [2006] OJ L105/54

The European Council

- The European Convention on Human Rights and Fundamental Freedoms (1950)
- Protocol No. 14 to the European Convention on Human Rights and Fundamental Freedoms, amending the control system of the convention (2004)

Sweden

- The Code of Judicial Procedure – *Rättegångsbalk* (1942:740)
- Act on Copyright in literary and Artistic Works - *Lag* (1960:729) *om upphovsrätt till litterära och konstnärliga verk*

- The Penal Code – *Brottsbalk* (1962:700)
- The Instrument of Government – *Kungörelse* (1974:152) *om beslutad ny regeringsform*
- The European Convention on Human Rights Act – *Lag (*1994:1219) *om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna*
- Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet
- The Electronic Communications Act – *Lag* (2003:389) *om elektronisk kommunikation)*
- Förordning **(**2007:951) med instruktion för Post- och telestyrelse

Other Publications

The European Union

- Article 29 Working Party, 'Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]', 9 November 2004

- The European Commission 'Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC' COM(2005)438, 21 September 2005

- Article 29 Working Party , 'Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)', 21 October 2005

- Statement by the Council of the European Union, 5777/06 ADD 1 REV 1 Brussels, 17 February 2006

- Article 29 Working Party, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC', 25 March 2006
-
- Article 29 Working Party, 'Report 01/2010 on the second joint enforcement action Compliance at national level of Telecom Providers and ISPs with the obligations required from national

traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive' WP 172, 13 July 2010

- The European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' COM (2011) 225 final, 18 April 2011

- European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)', 31 May 2011

Sweden

Prop. 1983/84:85	*Om 1985 års folk- och bostadsräkning m.m.*
Prop. 1983/84:142	*Ändring i sekretesslagen (1908:100) m.m.*
Prop. 1988/89:124	*Vissa tvångsmedelsfrågor*
Prop. 1992/93:200	*En telelag och en förändrad verksamhetsform för Televerket, m.m.*
Prop. 1994/95:227	*Hemlig teleavlyssning och hemlig teleövervakning*
Prop. 1995/96:90	*Registerbaserad folk- och bostadsräkning år 2000 m.m.*
Prop. 2002/03:74	*Hemliga tvångsmedel - offentliga ombud och en mer ändamålsenlig reglering*
Prop. 2006/07:63	*En anpassad försvarsunderrättelseverksamhet*
Prop 2006/07:133	*Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.*
Prop. 2010/11:46	*Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG*

SOU 2005:38	*Tillgång till elektronisk kommunikation i brottsutredningar m.m.*
SOU 2006:98	*Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.*
SOU 2007:76	*Lagring av trafikuppgifter för brottsbekämpning*
SOU 2009:1	*En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen*
Skr. 2010/11:66	*Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2009*

- Riksdagens Protokoll 2008/09:139, 20 August 2008
- Riksdagens Protokoll 2010/11:73, 16 March 2011

Considerations on SOUs

- JK ”Remissyttrande över promemorian Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet” (Ds 2005:21)”, Dnr 3485-05-80, 30 September 2005
- JK ” Remissyttrande över delbetänkandet (SOU 2005:38) Tillgång till elektronisk kommunikation i brottsutredningar m.m.”, Dnr 4667-05-80, 8
- Säkerhets- och Integritetskyddsnämnden “Betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)”, Dnr 4-2008, 16 February 2008
- JK ”Betänkandet (SOU 2007:76) Lagring av trafikuppgifter för brottsbekämpning”, Dnr 8771-07-80, 5 March 2008, see Supplement A
- Datainspektionen ”Betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)”, Dnr 1673-2007, 6 March 2008
- Svea Hovrätt ” Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)”, Dnr 683/07, 13 March 2008
- JO ”remiss angående betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)”, Dnr 5927-2007, 14 March 2008
- Sveriges advokatsamfund – Dnr R-2008/0035, 14 March 2008

Secondary Sources

Books

Bennett, Colin J. — *The Privacy Advocates- Resisting the Spread of Surveillance* (MIT Press, Cambridge, 2008)

Mock, William B.T.; Demuro, Gianmaro — *Human Rights in Europe – Commentary on the Charter of Fundamental Rights of the European Union* (Carolina Academic Press, Durham, 2010)

van Dijk, P.; van Hoof, G.J.H. — *Theory and Practice of the European Convention on Human Rights* (3rd Edition, Kluwer Law International, The Hague, 1998)

Flaherty, David — *Protecting Privacy in Surveillance Societies* (The University of North Carolina Press, Chapel Hill, 1989), p.1

Hansson, Sven Ove — *Teknik och Etik* (KTHs filosofienhet, Stockholm, 2002)

Hermerén, Göran — *Kunskapens pris. Forskningsetiska problem och principer I humaniora och samhällsvetenskap* (Humanistisk-samhällsvetenskapliga forskningsrådet, Stockholm, 1996)

Jacobs, Francis G.; White, Robin; Ovey, Clare — *The European Convention on Human Rights* (5th Edition, Oxford University Press, New York, 2010)

Lyon, David — *Surveillance Society: Monitoring Everyday Life* (Open University Press, Buckingham, 2001)

Lyon, David — 'Surveillance Technologies: Trends and Social Implications' in OECDs *The Security Economy* (OECD, Paris, 2004) http://www.oecd.org/dataoecd/14/17/16692437.pdf Accessed 19 June 2011

Westregård, Annamaria J. *Integritetsfrågor i arbetslivet* (Juristförlaget i Lund, Lund, 2002)

Olsson, Anders R. *Efter 11 september 2001: Kan storebror hejdas?* (Teledok & Vinnova, Stockholm, 2006)

Zurei, Elia; Stalker, Lynda Harling; Lyon, David *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (McGill-Queen's University Press, Montreal, 2010)

Articles

Breyer, Patrick 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) *European Law Journal* vol. 11, pages

Corbet, Ronald; Marx, Gary T. 'Critique: No Soul in the New Machine: Technofallacies in the Electronic Monitoring Movement' (1991), *Justice Quarterly* vol. 8, pp. 399-414

Haggerty, Kevin D.; Ericson, Richard V. ' The Surveillant Assemblage' (2000) *British Journal of Sociology* 51, pp. 605-622

Lock, Thomas **'**The ECJ and the ECtHR: The Future Relationship between the Two European Courts' (2009) *The Law and Practice of International Courts and Tribunals* vol. 8, pp. 375-398

Lyon, David 'Bentham's Panopticon: From Moral Architecture to Electronic Surveillance' (1991) *Queens Quarterly* vol. 98, pp. 596-617

Lyon, David 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) *International Sociology* vol. 19, pp.135-149

McHarg, Aileen — ‘Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights’ (1999) *Modern Law Review* vol. 62, pp. 671 – 696

Mathiesen, Thomas — ‘The Viewer Society: Michel Foucault’s “Panopticon” Revisited’ (1997), *Theoretical Criminology* 1, pp. 215-234

Parent, W.A. — ’Privacy, Morality and the Law’, (1983) Vol. 12 *Philosophy and Public Affairs*, pp. 269-288

Taylor, Nick — ‘State Surveillance and the Right to Privacy’ (2002), *Surveillance and Society* 1, pp.66-85

Other

— Conclusions of the Nordic Conference on the Right to Privacy, International Commission of Jurists (1967) Geneva.

— ’Explanations Relating to the Charter of Fundamental Rights’ [2007] Official Journal of the European Union 2007/C 303/02

Collste, Göran — ’Personlig Integritet’; SOU 1997:39 Integritet – Offentlighet – Informationsteknik , bilaga 4, s 785-807

The Council of the European Union — 26226th meeting (Press Realease) 14894/04 (Presse 332), Brussels, 2 December 2004. http://www.consilium.europa.eu/uedocs/cmsUpload/14894_JAI_2.12.04.pdf accessed 20 June 2011

Kilkelly, Ursula — 'The right to respect for private and family life – A guide to the implementation of Article 8 of the European Convention on Human Rights', Handbook No.1 (Council of Europe, 2003). http://www.echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf Accessed 19 June 2011

The European Commission — "Data retention: Commission refers Sweden back to Court for failing to transpose EU legislation" (Press Release) IP/11/409. 6 April 2011. Brussels.

The European Commission — 'Commission evaluates the Directive on retention of telecommunications data' (Press Release) IP/11/484, 18 April 2011. Brussels

Statistics Sweden — Background Facts, *Forty years of regional statistics from Statistics Sweden* (2006). http://www.scb.se/statistik/_publikationer/OV9999_2006A01_BR_X102ST0601.pdf Accessed 19 June 2011

UNESCO — 'The Protection of Privacy', (2007) Vol. XXIV No 3 International Social Science Journal 413

Web Material

'The European Union's Accession to the European Convention on Human Rights', Fact Sheet, http://www.coe.int/lportal/c/document_library/get_file?uuid=bc992d6f-f09b-4060-a9fe-4d36447cf118&groupId=10227 accessed 19 June 2011

Table of Cases

The European Court of Justice:
Sorted by date

- Case 25/62 *Plaumann v. Commission* [1963] ECR 95
- Case T-135/96 *UEAPME v. Council* [1998] ECR II-2335
- Opinion of General Advocate Jacobs delivered on 21 March 2002 in ECJ C-50/00 P – *Unión de Pequeños Agricultores* v *Council* [2002] ECR I-3357
- CFI 3 May 2002 – T-177/01 – *Jégo-Quéré and Cie SA* v *Commission* [2002] ECR II-2365
- ECJ C-263/02 *P Commission v. Jégo Quéré SA* [2004] ECR I –3452
- Case C-301/06, *Ireland v Parliament and Council* [2009] ECR I-593
- Case C-185/09, Judgment of the Court (sixth chamber), *European Commission v Kingdom of Sweden*, 4 February 2010

The European Court of Human Rights
Sorted by name

- Amann v Switzerland, (App. 27798/95), 16 February 200, (2000) 30 EHRR 842, ECHR 2000-II
- Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v Ireland, (App. 45036/98) 30 June 2005 [GC], (2006) 42 EHRR 1, ECHR 2005-VI
- Copland v.United Kingdom, (App. 3 April 200, (2007) 45EHRR 858, ECHR 2007-IV
- Demuth v Switzerland, (App. 38743/97), 5 November 2002, ECHR 2002-IX
- Halford v United Kingdom, (App. 11855/85), 21 June 1997, (1997) 24 EHRR 523, ECHR 1997-III
- Handyside v United Kingdom, (App. 5493/72), 7 December 1976, Series A No 24, (1976) 1 EHRR 737
- Huvig v France, (App. 11105/84), 24 April 1990, Series A, No 176-B, (1990) 12 EHRR 528
- Iordachi and others v Moldova, (App. 25198/02), 14 September 2009
- Kennedy v United Kingdom, (App. 26839/05), 18 May 2010
- Klass v Germany, (App. 5023/71), 6 September 1978, Series A No 28, (1979-80) 2 EHRR 214
- Kruslin v France, (App. 11801/850), 24 April 1990, Series A, No 176-B, (1990) 12 EHRR 547
- Kudla v Poland, (App. 30210/96) 26 October 2000 [GC], (2002) 35 EHRR 198, ECHR 2000-XI
- Larkos v Cyprus, (App. 29515/95), 18 February 1999 [GC], (2000) 30 EHRR 597, ECHR 199-I

- Leander v Sweden, (App. 9248/81), 26 March 1987, Series A No 116, (1987) 9 EHRR 433
- Liu v Russia, (App. 7508/02), 6 December 2007
- Malone v United Kingdom, (App. 8691/79), 2 August 1984, Series A, No 82, (1985) 7 EHRR 14
- Matthews v United Kingdom, (App. 24833/94) 18 February 1999 [GC], (1999) 28 EHRR 361, ECHR 1999-I
- Niemietz v. Germany (App. 13710/88), 16 December 1992, Series A No 251-B, (1993) 16 EHRR 97,
- Roche v United Kingdom, (App. 3255/96), 19 October 2005 [GC], (2006) 42 EHRR 599
- Segerstedt-Wiberg and Others v. Sweden, (App. 62332/00), 6 June 2006 (2007), 44 EHRR 14, ECHR 2006-VII
- Silver v United Kingdom, (Apps. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75), 25 March 1983, Series A No 61, (1983) 5 EHRR 347
- Soering v United Kingdom, (App. 14038/88), 7 July 1989, Series A, No 161, (1989) 11 EHRR 439
- Sunday Times v United Kingdom, (App. 6538/74) 26 April 1979, Series A No 30, (1979-80) 2 EHRR 245, para 49.
- Valenzuela Contreras v Spain, (App. 27671/95), 30 July 1998, (1999) 28 EJRR 483, ECHR 1998-V
- Vogt v Germany, (App. 17851/91), 26 September 1995, (1996) 21 EHRR 205

Other

- Ireland Ltd -v- Minister for Communication & Ors [2010] IEHC 221, 5 May 2010