FRA and the European Convention on Human Rights
- A Paradigm Shift in Swedish Electronic Surveillance Law

Mark Klamberg
Doctoral Candidate
Stockholm University, Faculty of Law
mark.klamberg@juridicum.su.se

Dag Wiese Schartaum (editor), *Overvåking i en rettstat* in the series Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology), Fagforlaget, Bergen 2010, pp. 96-134

Kapittel 5

FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law

Mark Klamberg[1] is a doctoral candidate in public international law at the Faculty of Law at Stockholm University. He has served as a legal clerk at the district court of Blekinge and at the International Criminal Court. Klamberg lectures on international criminal law, human right law, public international law and electronic surveillance law.

[1] I owe gratitude to several people who provided helpful comments on the manuscript or parts thereof at various stages in its development: Simon Andersson, Petter Asp, Janne Flyghed, Christopher Kullenberg, Mikael Nilsson, Cecilia Magnusson Sjöberg, Karol Nowak, Anna Petersson, Peter Wahlgren and Sören Öman. As far as shortcomings are concerned, they are all attributable to the author.

1. Introduction

Electronic surveillance is an important tool for law enforcement. Video cameras, wire-tapping and bugs can be used to detect, prevent and investigate criminality. **(p. 96)** It can also be used to collect intelligence about foreign powers or agents of foreign power, which shows that electronic surveillance is not necessarily connected to law enforcement.

Electronic surveillance law is subject to a paradigm shift where traditional principles are reconsidered and the notion of privacy has to be reconstructed. This paradigm shift is the result of four major changes in our society with regard to 1) technology; 2) perceptions of threats, 3) interpretation of human rights and 4) ownership over telecommunications.

First, the technological development has made the Internet an increasingly important part of our lives. Furthermore, messages are to lesser extent travelling by satellite, microwave relay link and more in fibre optic cable. While satellite and microwave relay links are leaking communication making these modes of communication relatively accessible with an antenna, interception of communication in a fibre optic cable is more problematic. Normally, the cable has to be accessed with the knowledge and consent of the communications service provider (CSP) at certain points where the communication is routed.[2]

Second, with the fall of the Berlin Wall and the dissolution of the Soviet Bloc the perceived threats have changed, shifting the focus from military threats towards non-state actors such as terrorists and criminal networks. There is a trend that countries redefine their view of national security which involves an expanded conceptualization of security. This has led to a shift towards more proactive, preventive measures against threats such as terrorism, in other words preemptive intelligence. A large number of measures involving interference with privacy has been taken to counter such threats.[3]

Third, constitutional courts as well as human rights courts have clarified the standards that state agencies have to meet in order to conduct surveillance. For example, article 8 of the European Convention for the protection of Human Rights requires that any individual measure of surveillance has to comply with strict conditions and procedures set out in statute law. **(p. 97)**

Finally, many European states have towards the end of the 20th century privatized previously state-owned CSPs. In the previous era of state monopolies the State could through secret decrees order their CSPs to hand over communication. Private CSPs are less willing to do the same without a statute creating such an obligation.

The abovementioned changes have created a need to reform both the tools of electronic surveillance and domestic legislation. Surveillance that was previously kept secret is now subject to public debate. There is also a fear that tools created for legitimate purposes such as crime control can also be used for increased or total social control. Does the ends justify the means?

Even if the state does not aim at total social control and the actual surveillance is legitimate, the mere possibility of mass surveillance may lead to self-censorship and inhibition.[4] The option for legislators who do not wish to close down several surveillance

---

[2] Johnson, Loch K., *Introduction*, Johnson, Loch K. (Ed.), Handbook of Intelligence Studies, 1-14, Routledge, London and New York, 2009, p. 6; Richelson, Jeffrey T., *Technical Collection in the Post-September 11 World*, Treverton, Gregory F. & Agrell, Wilhelm (Eds.), National Intelligence Systems, 147-175, Cambridge University Press, Cambridge, 2009, p. 163.

[3] Flyghed, Janne, *Crime-Control in the Post-Wall Era: The Menace of Security*, Journal of Scandinavian Studies in Criminology and Crime Prevention, vol 6, 2005, pp. 165-182, pp. 166-168, 178-179; Omand, David, *The Limits of Avowal: Secret Intelligence in an Age of Public Scrutiny*, Treverton, Gregory F. & Agrell, Wilhelm (Eds.), National Intelligence Systems, 235-264, Cambridge University Press, Cambridge, 2009, pp. 238 and 241.

[4] Solove, Daniel J., *A Taxonomy of Privacy*, University of Pennsylvania Law Review, vol 154, 2006, pp. 477-560, p. 493.

systems is to proceed by making the legislation transparent. Some may argue that this would fatally erode the necessary secrecy that need to surround such activity. It is also argued that some of the once-overriding reasons for secrecy have lost their original force while others still remain valid.[5]

I will first discuss the privacy discourse and provide the essential insights in the electronic surveillance law in Sweden.[6] However, the main focus of this article is the signal intelligence operations of the Swedish National Defence Radio Establishment (Försvarets Radioanstalt or FRA). This study is founded on the assumption that FRAs interception of the content of messages is relatively narrow compared to its large-scale collection and storage of traffic data which through further processing may reveal who is communicating with whom. Does this assumption have any basis in the actual legislation and what consequence will it have for our perception of privacy? **(p. 98)**

2. Sociological and Technological Aspects on the Privacy Discourse

2.1 Disintegration of Geographical and Functional Boundaries

There is a disintegration of the traditional boundaries previously set by geography and the functional mandates between different state agencies. Electronic surveillance of domestic communication is normally carried out by law enforcement agencies that have the power to order CSPs to hand over communication. Often such orders require authorization in a warrant issued by a judge, but not always as will be explained. The CSPs extract the relevant message or data and hands over it to the law enforcement agency. States may also introduce law which requires that CSPs must retain necessary data which at a later stage can be accessed by law enforcement agencies.

International communications is more problematic. For example, how can a law enforcement or intelligence agency in country A intercept an e-mail message from a terrorist suspect in country B whose e-mail account is administered by a CSP outside the territorial jurisdiction of country A? The law enforcement or intelligence agency in country A only knows that the message it wishes to intercept is destined for an unknown recipient in country A or is in transit through the territory of country A to a destination in country C. It is held that CSPs without significant investments do not have the technical capacity to intercept such messages. Furthermore, if the object of surveillance is an agent of a foreign power, intelligence agencies are very reluctant to disclose the target of the surveillance to private and in some cases foreign owned CSPs.[7] How can this dilemma be solved? Several countries have created signal intelligence agencies for this purpose, such as the National Security Agency (NSA) in the USA, Government Communication headquarters (GCHQ) in the UK, Bundesnachrichtendienst (BND) in Germany and the FRA in Sweden. Instead of having the CSP extracting the relevant message or data, all international communication is made accessible to the intelligence agency which collect, process and store the relevant information. The information made accessible to the State in this way is on a totally different scale than the narrow warrants used in a pure domestic setting. As indicated, this development is problematic from a privacy perspective. Increasingly more of everyday communication has an

[5] Omand, 2009, p. 246.

[6] Methods of surveillance which do not concern electronic communication, such as secret camera surveillance and the use of covert listening devices (bug), is outside the scope of this article. For rules on these methods, see Code of Judicial Procedure, chapter 27 section 20(a); Act on Covert Listening Devices (2007:978.

[7] National Defence Radio Establishment, Opinion on the Memorandum on Additional Protection for Privacy in Connection with Signal Intelligence (Ds 2009:1), 27 February 2009, pp. 2-3.

international character. The Internet does not distinguish between **(p. 99)** pure domestic communication and international communication, messages between two persons in the same country can be routed all across the world. The mandate of agencies such as the NSA, GCHQ, BND and FRA is no longer restricted to surveillance of foreign state powers but also include the activities of non-state actors involved in terrorism or gross international criminality. Differences between domestic and international communication, threats from state and non-state actors are becoming blurred.[8]

2.2 Content and Traffic Data

Surveillance of electronic communication is often associated with wire-tapping where the police listen in on a phone conversation. However, such surveillance has its limitations. Modern phone and internet communication involves increasing use of encryption and ever increasing volumes of messages. Law enforcement and intelligence agencies will not be able to store and analyse the content of all the messages. This development is essential in understanding why law enforcement and intelligence agencies are focusing less on traditional wire-tapping, more on retention of traffic data and traffic analysis of communication patterns.

As opposed to the content of a message, traffic data is the information used by the communication network to deliver the message to or from the user. In a telephone network, traffic data will reveal the number dialed ("to"), the originating number ("from"), the time of the call, and its duration. In the internet context, traffic data will similarly reveal the "to" and "from" e-mail address, the instant message to and from account names, and the other administrative information the computers generate in the course of delivery.[9] I will use the terms "content data" and "traffic data".[10] For the most part, it is easy to classify what is content or traffic data. However, in some cases it remains difficult, such as URLs for websites. Daniel J. Solove has made the observation that since a URL points to the location of particular information on the Internet, it can reveal the specific content of a website that people are viewing.[11] **(p. 100)**

Encryption of the content of the message will not offer protection against traffic analysis of traffic data.[12] In this way law enforcement agencies may identify the communication patterns of and the network of criminal groups. Intelligence agencies may find agents communicating with foreign governments without ever reading or listening to any messages. Traffic analysis is also used in military intelligence to identify the chain of command, higher staff functions, divisions, brigades and units.[13] Considering that traffic data can be used to identify what content a person is viewing at the internet, membership of groups and networks, it is submitted that such data may in certain contexts be as sensitive as content data. The question is if the law should offer the individual identical protection of his or her traffic data as is afforded to content data.

---

[8] Omand, 2009, p. 2004.

[9] Kerr, Orin S., *Applying the Fourth Amendment to the Internet: A General Approach*, Stanford Law Review, Forthcoming, pp. 21-22.

[10] Other, similar terms are used. Orin Kerr makes the distinction between "content" and "envelope" information, ibid, p. 21. One may also find references to "metadata" (data about data), which in this context also signifies non-content data or "envelope information", Government Bill 2006/07:63 Adapted Defence Intelligence Operations, p. 72.

[11] Solove, Daniel J., *Reconstructing Electronic Surveillance Law*, Geo. Wash. L. Rev., vol 72, 2003-2004, pp. 1264-1305, p. 1287; see also Kerr, 2009, p. 23.

[12] SOU 2007:76 Data Retention for Law Enforcement Purposes, Report by the Inquiry on Data Retention, Stockholm 2007, p. 132; Wirtz, James J., *The American Appraoch to intelligence studies*, Johnson, Loch K. (Ed.), Handbook of Intelligence Studies, 28-38, Routledge, London and New York, 2009, p. 36.

[13] Agrell, Wilhelm, *Konsten att gissa rätt - Underättelsevetenskapens grunder*, Studentlitteratur, Lund, 1998, pp. 97, 120 and 121; Wirtz, 2009, p. 36.

2.3 Defining Privacy

Privacy may be perceived as an umbrella term, referring to a wide and disparate group of activities. It is argued that privacy is not only an individual right but also a constitutive element of civil society. The consequence of this pluralistic approach to privacy is that the value of privacy is different depending upon the particular problem or harmful activity. I will focus on three basic groups of harmful activities: 1) information collection, 2) information processing, and 3) information dissemination.[14]

Information processing may involve *aggregation* as well as *identification*. Modern techniques of electronic surveillance often involve data mining, where large quantities of data are collected, aggregated, linked to individuals (identification) and disseminated. *Aggregation* involves the combination of various pieces of information about a person. We might not find that these pieces are sensitive and worthy of concealing, but when aggregated they may reveal information we wish to conceal. Such aggregated data may reveal to government agencies patterns in our daily lives and interaction with other people that we ourselves are not aware of.[15] One may also use the term *information fusion* which is an activity that seeks to increase the value of disparate **(p. 101)** but related information above and beyond the value of the individual pieces of information.[16] Information can be aggregated without being associated with a specific person. For example, an electronic surveillance measure may target a phone number or an IP address without knowing which specific person is using the service. In such a case individuals communicating to each other are reduced to anonymous nodes in a larger network. The initial surveillance is carried out without knowing the true identity of all the targets. I submit that it is difficult or even impossible to carry out the initial stages of such surveillance involving *collection* and *aggregation* with the requirement that is shown that someone is reasonably suspected of an offence in relation to all the nodes. Possibly one could require before an activity involving aggregation is taken that reasonable cause of suspicion is shown in relation to an initiating node where the identity of the subscriber is known. *Identification* is linking the information to particular individuals.[17] Following collection and aggregation the intelligence agency may wish to focus even further on some of the nodes. For this purpose the node is linked to an individual. For example, when the intelligence agency has found that certain phone numbers and IP addresses are relevant, they may order the CSPs to disclose the identity of the subscriber of that phone number or IP address. It is clear that all of the abovementioned measures constitute acts which interfere with privacy. The question is how to minimize such interference. In section 5.1 of this article I will discuss aggregation and identification because they are key in designing and determining both how invasive and how efficient an intelligence-gathering program is.

2.4 Data Mining Techniques

Public authorities as well as private parties hold transactional records, for example 1) applications for passports, visas, work permits and drivers' licenses; 2) credit and debit card transactions; 3) automated teller machine (ATM) withdrawals; 4) airline and rental car reservations; 5) in the context of this article: Internet access, records of phone calls and e-mail messages. The fact that all of the data in question are in digital form means that increasingly

---

[14] Solove, 2006, pp. 485-488; Solove, Daniel J., *I've Got Nothing to Hide and Other Misunderstandings of Privacy*, San Diego Law Review, vol 44, 4, 2007, pp. 745-772, pp. 756-764.
[15] Solove, 2006, p. 490; Solove, 2007, p. 766.
[16] National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, National Academies Press, Washington, DC, 2008, p. 188.
[17] Solove, 2006, p. 490.

powerful tools - such as automated data mining - can be used to analyze it.[18] **(p. 102)** Data mining is a technology of analysis rather than collection, and thus they are intended to help analysts find patterns of interest in all of the available data.[19]

Data mining often work well in commercial settings, for example for detection of fraud in relation to credit cards, where they are applied to highly structured databases and are improved through constant use and learning. Data mining algorithms might also be used as components of a data-supported counterterrorist system, helping to perform functions, such as helping to detect aliases, or combining all records concerning a given individual and his or her network of associates, or clustering events by certain patters of interest. Automated identification of terrorists or other criminal activity through data mining may be problematic because it 1) conflicts with privacy and 2) there is likelihood of false positives. First, using large databases filled with transaction data on actual individuals presents a serious privacy issue. Almost all of these individuals will have no connection to terrorism or crime, and the use of such data in this context means that their private personal information will be compromised. Second, these systems will produce false positives, i.e. innocent persons are identified as suspect.[20] If a credit card company contacts a client because they believe that somebody through fraud is using the client's credit card is less problematic than if the Secret Service believes that a person is involved with terrorism.

It should be emphasized that many of the groups that are targeted for surveillance have a high security counsciousness. They will make calculated efforts to conceal their identity and mask their behaviors through the use of strategies such as encryption, code words, and multiple identities to obfuscate the data they are generating and exchanging. Such deliberate manipulation of the system may generate false positives against innocent individuals.[21]

In a report from the U.S. National Research Council the following definitions on two different data mining techniques are provided. *Subject-based data mining* uses an initiating individual or other datum that is considered, based on other information, to be of high interest, and the goal is to determine what other persons or financial transactions or movements, etc., are related to that initiating datum. This data mining technique simply expands and automates what a police detective or intelligence analyst would carry out with sufficient time.[22] *Pattern-based data mining* looks for patterns (including anomalous data patterns) that might be associated with terrorist activity **(p. 103)** —these patterns might be regarded as small signals in a large ocean of noise. In its report, the National Research Council Such presents the conclusion that automated terrorist identification is not technically feasible because the notion of an anomalous pattern - in the absence of some well-defined ideas of what might constitute a threatening pattern - is likely to be associated with many more benign activities than terrorist activities. It is argued that the utility of pattern-based data mining is found primarily if not exclusively in its role in helping humans to prioritize attention and deploy scarce investigative resources.[23]

3. The European Convention on Human Rights

This section will provide the European Legal Context, focusing on the European Convention for the protection of Human Rights and Fundamentals Freedoms (ECHR).

---

[18] National Research Council, 2008, pp. 32-33 and 241; Pollard, Neal A., *On Counterterrorism and Intelligence,* Treverton, Gregory F. & Agrell, Wilhelm (Eds.), National Intelligence Systems, 117-146, Cambridge University Press, Cambridge, 2009, pp. 143-144.
[19] National Research Council, 2008, p. 20.
[20] ibid, pp. 3-4, 81, 188-189; Pollard, 2009, p. 145.
[21] National Research Council, 2008, pp. 2 and 40; Richelson, 2009, p. 161.
[22] National Research Council, 2008, pp. 17 and 21.
[23] ibid, pp. 17 and 79; Pollard, 2009, p. 144.

The EU Data Retention Directive is discussed in an other article of this yearbook. However, it is worth observing that the directive has not been implemented in Sweden within the prescribed period.[24] As a consequence the Court of Justice of the European Union has declared that Sweden has failed to fulfil its obligations under the directive.[25] The Minister for Justice has stated that Sweden will implement the directive. The Government has motivated the delay with the need to coordinate the implementation of the directive with an Government inquiry on law enforcement methods (henceforth *Inquiry on Law Enforcement Methods)* which,[26] *inter alia*, deals with the access for national authorities to traffic data.[27]

Turning to the ECHR, article 8 protects the individual's right to respect for his private and family life, his home and his correspondence. The European Court of Human Rights (ECtHR) has dealt with several complaints concerning electronic surveillance, including two complaints concerning signal **(p. 104)** intelligence or "strategic monitoring" directed against international communication, *Weber and Saravia v. Germany* and *Liberty and Others v. the United Kingdom* .[28] Prior to the examination by the ECtHR, strategic monitoring was under review by the Federal Constitutional Court in Germany. It held that certain provisions of the legislation were incompatible or only partly compatible with the principles laid down in the Basic Law (the constitution).[29] The law was modified and the ECtHR made its assessment on the law as interpreted and modified by the Federal Constitutional Court.[30]

What is the scope of the protection? The ECtHR has in its case law determined that communication by telephone, facsimile and e-mail are covered by the notions "private life" and "correspondence".[31] Moreover, activities of a professional or business nature are both included in the notion of "private life".[32]

3.1.1 Defining Interference

What is to be regarded as interference with the right to privacy under Article 8(1)? In *Klass and Others v. Germany*, the Court considered that the question whether surveillance measures had been ordered or implemented in respect of the applicants had no bearing on the appreciation of the applicants' status as "victims". The menace of surveillance in itself to restrict free communication through the postal and telecommunication services, constituted for all users or potential users a direct interference with the right guaranteed by Article 8 (art. 8). The Court found that each of the applicants is entitled to claim to be the victim of a

---

[24] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 , article 1.
[25] C-185/09, European Commission v Kingdom of Sweden, Judgment of 4 February 2010.
[26] SOU 2009:1 Improved Legal Safeguards in the Collection of Electronic Communication for Law Enforcement Purposes; see more on this inquiry in sections 4.2.1 and 4.2.4.
[27] *Regeringen skjuter på datalagring,* Svenska Dagbladet, 21 oktober 2009.
[28] Decision as to the Admissibility of Application no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany, ECtHR, 29 June 2006; Liberty and Others v. the United Kingdom, (Application no. 58243/00), Judgment, 1 July 2008.
[29] BVerfG, 1 BvR 2226/94 of 07/14/1999, paragraphs No. (1 - 308).
[30] *Weber and Saravia v. Germany*, paras. 12 and 63.
[31] *Klass and others v. Germany*, ECtHR, (Application no. 5029/71), Judgment, 6 September 1978, paras. 41; Malone v. the United Kingdom, (Application no. 8691/79), Judgment, 2 August 1984 para. 64; Kruslin v. France, (Application no. 11801/85), Judgment, 24 April 1990, para. 26; Kopp v. Switzerland, (13/1997/797/1000), Judgment, 25 March 1998, para. 50; Amann v. Switzerland, (Application no. 27798/95), Judgment, 16 February 2000, para. 44; *Weber and Saravia v. Germany*, para. 77; *Liberty and Others*, para. 56.
[32] Niemietz v. Germany, (Application no. 13710/88), Judgment, 16 December 1992, paras. 28-33; *Kopp*, Judgment, 25 March 1998, para. 50; Amann, para. 65; Rotaru v. Romania, (Application no. 28341/95), Judgment, 4 May 2000, para. 43.

violation of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance.[33] Similarly the Court stated in *Weber and Sara*- **(p. 105)** *via v. Germany* that "the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."[34]

The ECtHR distinguishes between content and traffic data, but both categories of information are protected by Article 8.[35] In *P.G. and J.H. v. the United Kingdom* the applicants argued that the requirement on accessibility and foreseeability was not fulfilled in their case, as there were insufficient safeguards in place concerning the use, storage and destruction of records of billing information. The ECtHR found that use of the information would be strictly limited. Disclosure to the police was permitted under the relevant statutory framework where it was necessary for the purposes of the detection and prevention of crime, and the material was used at the applicants' trial on criminal charges to corroborate other evidence relevant to the timing of telephone calls. The lack of statutory governing storage and destruction of such information did not offend Article 8.[36] The Court's finding on storage and destruction has been superseded by the minimum requirements set out in later case law.[37] Metering does not *per se* offend against Article 8 if, for example, if its is done by the telephone company for billing purposes.[38]

Some of the measures discussed later in this article involves the retention of large amounts of traffic data. Such data is included by the notion personal data.[39] In *S. and Marper v. the United Kingdom* the Court stated that "the **(p. 106)** mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data".[40]

---

[33] *Klass and others v. Germany*, paras. 37-38, 41.
[34] *Weber and Saravia v. Germany*, para. 78; *Liberty and Others*, para. 56.
[35] *Malone v. the United Kingdom*, para. 84: By its very nature, metering is … to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).
[36] *P.G. and J.H. v. the United Kingdom*, (Application no. 44787/98), Judgment, 25 September 2001, para. 44-48.
[37] *Weber and Saravia v. Germany*, para. 95; *Liberty and Others*, para. 62; see also Lagerwall, Anders, *Privacy and Secret Surveillance from a European Convention Perspective*, Stockholm University, Fall 2008, p. 27, para. 157.
[38] *P.G. and J.H. v. the United Kingdom*, 25 September 2001, para. 42.
[39] Data Protection Directive, article 2(a); Privacy, Transparency, Information Technology SOU 1997:39, pp. 113 and 341.
[40] *S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment, 4 December 2008, para. 121.

3.1.2 Legitimate Interference

When is interference legitimate under article 8? Interference is permissible only if the measure is 1) "in accordance with the law"; 2) pursues certain interests; and 3) is "necessary in a democratic society".[41]

First, interference must be "in accordance with the law", which requires that the measure should have some basis in domestic law. It also refers to the quality of the law in question, requiring that it should be 1) accessible to the person concerned, who must, moreover, be able to 2) foresee its consequences for him, and 3) compatible with the rule of law.[42]

Publication of the law is a way to fulfil the requirement that the law is accessible.[43] In *Liberty and Others* the United Kingdom argued that arrangements under section 6 of the 1985 Act provided safeguards for individuals' rights.[44] The Court observed, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.[45] In its conclusion that the law did not fulfil the requirement "in accordance with the law" under article 8 the Court in particular noted that that the U.K. law did not meet the requirements of the Court's case-law. The 1985 Act did not set out in a form accessible to the public any indication of the procedure to be followed for selecting, examination, sharing, storing and destroying intercepted material.[46] **(p. 107)**

With the requirement on foreseeability follows that the norm has to be formulated with sufficient precision to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to measures of surveillance.[47] Any individual measure of surveillance has to comply with the strict conditions and procedures laid down in the legislation itself.[48] However, there is no absolute right for persons concerned by secret surveillance measures to be notified subsequently once surveillance has ceased.[49] As a compensatory measure, there should be an independent control mechanism in the form of a court or equivalent body vested with sufficient powers and competence to exercise an effective and continuous control.[50]

It is contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[51] Aspects relevant for the requirement on foreseeability may also be relevant for the assessment whether a measure is in accordance with the rule of law.

In *Weber and Saravia* the Court summarized the requirements on the quality of the law in the following way:

---

[41] European convention for the Protection of Human Rights and Fundamental Freedoms adopted 4 November 1950 as amended by Protocol No. 11, article 8(2).

[42] *Sunday Times v. the United Kingdom*, (Application no. 6538/74), Judgment, 26 April 1979, para. 49; *Malone v. the United Kingdom*, para. 66; *Kruslin*, para. 27; *Kopp*, Judgment, 25 March 1998, para. 55; *Amann*, para. 50; *Leander v. Sweden*, (Application no. 9248/81), Judgment, 26 March 1987, para. 50; *Rotaru*, para. 52; *Foxley v. the United Kingdom*, (Application no. 33274/96), Judgment, 20 June 2000, para. 34; *Weber and Saravia v. Germany*, para. 84; *Liberty and Others*, para. 59.

[43] *Rotaru*, para. 54; *Leander v. Sweden*, paras. 52-53.

[44] *Liberty and Others*, paras. 27 and 48-51.

[45] ibid, para. 66.

[46] ibid, para. 69.

[47] *Malone v. the United Kingdom*, para. 68; *Kruslin*, para. 33; *Kopp*, paras. 64 and 72; *Amann*,, para. 56; *Weber and Saravia v. Germany*, para. 93.

[48] *Klass and others v. Germany*, para. 43.

[49] ibid, para. 58; *Leander v. Sweden*, para. 66; *Weber and Saravia v. Germany*, para. 135.

[50] *Klass and others v. Germany*, paras. 55–56; *Rotaru*, para. 59; *Weber and Saravia v. Germany*, paras. 117–118.

[51] *Malone v. the United Kingdom*, para. 68; *Leander v. Sweden*, para. 51; *Weber and Saravia v. Germany*, para. 94; *Liberty and Others*, para. 62.

> In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: [1] the nature of the offences which may give rise to an interception order; [2] a definition of the categories of people liable to have their telephones tapped; [3] a limit on the duration of telephone tapping; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed. [52] **(p. 108)**

The second requirement under article 8(2) calls for that the interference must pursue certain listed interests in order to be legitimate: national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health or morals, or the protection of the rights and freedoms of others.[53] The Court rarely challenges the aim referred to by states.[54] The disputes more often concern whether the measure has a legal basis and/or is "necessary in a democratic society". In comparison, the Federal Constitutional Court in Germany holds that collected data must be marked to make it possible to track the object of protection throughout the remaining steps of processing. Data that is not destroyed or deleted is bound to the objective that justified the collection of data in the first place.[55] This would be in conformity with the finality principle, i.e. that personal data shall be collected and recorded for specific, explicit legitimate purposes and used in a way that is not inconsistent with the said purposes.[56]

Finally, an interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient".[57] While it is for the national authorities to make the initial assessment in **(p. 109)** all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention.[58] A margin of appreciation is left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors including

---

[52] *Weber and Saravia v. Germany*, para. 95. The Court applied the same principles in the subsequent case, *Liberty and Others*, para. 62-64.
[53] ECHR, article 8(2).
[54] *Klass and others v. Germany*, para. 46; *Leander v. Sweden*, para. 49; *Weber and Saravia v. Germany*, paras. 103-104; see also Lagerwall, 2008, p. 17.
[55] BvR 2226/94 of 07/14/1999, paras. 248 and 255; *Weber and Saravia v. Germany*, para. 116.
[56] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, CETS No.: 108, article 5(b) and (e); Balboni, Paolo, *Video Surveillance and Related Privacy and Data Protection Issues: the Italian Experience*, Nouwt, Sjaak, De Vries, Berend R. & Prins, Corien (Eds.), Reasonable Expectations Of Privacy?: Eleven Country Reports On Camera Surveillance And Workplace Privacy, 285-322, T • M • C Asser Press, The Hague, 2005, p. 306; SOU 2008:3 Protection of Privacy, Memorandum of the Committee on Protection of Privacy, p. 141.
[57] *Silver and Others v. United Kingdom*, Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, European Court of Human Rights, Judgment 25 March 1983, para. 97; A example where the Court found a measure disproportional is *S. and Marper v. the United Kingdom*, paras. 125-126. The Court found that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, failed to strike a fair balance between the competing public and private interests. Consequently, the United Kingdom had overstepped the acceptable margin of appreciation with that result that the measure was in violation of article 8; Ovey, Clare & White, Robin C.A., *The European Convention on Human Rights*, Oxford University Press, Oxford, 2006, p. 232.
[58] *Coster v. The United Kingdom*, Application no. 24876/94, European Court of Human Rights, Judgment 18 January 2001, para. 104; *S. and Marper v. the United Kingdom*, para. 101.

the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights.[59] National Security is an area where States are allowed a wide margin.[60] However, the Court has affirmed the risk that a system of secret surveillance in the struggle against terrorism, espionage and for the protection of national security may undermine or even destroy democracy under the cloak of defending it. Therefore the Court must be satisfied that there exist adequate and effective guarantees against abuse.[61] The Court's approach in this regard indicates that it perceives privacy not only as an individual right but also a constitutive element of civil society.

4. Swedish Law

4.1 Relation to the ECHR and Constitutional Protection

Sweden was among the first states to ratify the ECHR and the treaty entered into force 3 September 1953.[62] It was incorporated 1995 into Swedish law by an act.[63] A constitutional provision was also included in the Instrument of Government which provides that no act of law or other provision may be adopted which contravenes Sweden's undertakings under the ECHR.[64] **(p. 110)**

In the Swedish Constitution there is a similar privacy protection as is provided under article 8 of the ECHR.[65] The scope of this protection may be restricted by statutory law and "only to satisfy a purpose acceptable in a democratic society. The restriction must never go beyond what is necessary having regard to the purpose which occasioned it, nor may it be carried so far as to constitute a threat to the free formation of opinion as one of the fundaments of democracy. No restriction may be imposed solely on grounds of a political, religious, cultural or other such opinion."[66]

4.2 Electronic Surveillance of Domestic Communication by the Police and the Secret Service

Having established that electronic surveillance constitute interference with the right to privacy, the surveillance of communications by the Police and the Secret Service will be analysed in four steps: 1) collection; 2) processing; 3) dissemination; and 4) monitoring. Such surveillance mainly concerns domestic communication due to the fact that some international communication, for example transit communication, is beyond the effective surveillance traditionally used by Police and Secret Service.[67]

---

[59] *Klass and others v. Germany*, para. 49; *Leander v. Sweden*, paras. 59 and 67; *Weber and Saravia v. Germany*, para. 106; *S. and Marper v. the United Kingdom*, para. 102; Clare & White 2006, p. 233.
[60] *Klass and others v. Germany*, para. 48; *Leander v. Sweden*, para. 59; Clare & White 2006, p. 237.
[61] *Klass and others v. Germany*, paras. 49-50; *Leander v. Sweden*, para. 60; *Weber and Saravia v. Germany*, paras. 106 and 116-118.
[62] Chart of signatures and ratifications, Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 005, Status as of 11 September 2009.
[63] Act (1994:1219) on the European convention for the Protection of Human Rights and Fundamental Freedoms.
[64] The Instrument of Government (1974:152), chapter 2, article 23.
[65] ibid, Chapter 2, article 6: "Every citizen shall be protected in his relations with the public institutions against any physical violation also in cases other than cases under Articles 4 and 5. He shall likewise be protected against body searches, house searches and other such invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications."
[66] ibid, chapter 2, article 12.
[67] This is explained in sections 2.1 and 4.3.

4.2.1 Wiretapping and Tele-surveillance Prior or During a Preliminary Investigation

The applicable rules on collection of domestic communications may be examined according to two dimensions. The first dimension of rules relates to whether a preliminary investigation has been initiated. A preliminary investigation shall be initiated as soon as due to a report or for other reason there is cause to believe that an offence subject to public prosecution has been committed.[68] A second set of rules deals with electronic surveillance, outside the scope of a preliminary investigation, for the purpose of detecting or preventing crimes. In addition, the rules make a difference whether the collection relates to the content of messages or traffic data. **(p. 111)**

Electronic surveillance in the context of a preliminary investigation is defined as secret surveillance which include secret wiretapping (interception of the content of messages) and tele-surveillance (interception of traffic data). Such measures may concern sound, pictures, text, data or other information that are transmitted through radio, light or electromagnetic means.[69] In other words, such measures may concern communication by phone as well as by internet.

Chapter 27 of the Code of Judicial Procedure (*CJP*) provides that secret wiretapping may be used concerning 1) offences in respect of which a less severe penalty than imprisonment for two years is not prescribed for the offence; or 2) attempt, preparation, or conspiracy to commit such an offence if such act is subject to punishment.[70] CJP chapter 27 also allows secret tele-surveillance, i.e. interception of traffic data, which may be used concerning 1) offences in respect of which a less severe sentence than six months imprisonment is not prescribed; 2) other offences including breach of data secrecy, child pornography crime, narcotic offences and smuggling of narcotics; or 3. attempt, preparation, or conspiracy to commit the aforementioned offences and such an act is penalized.[71] Secret wire-tapping and secret tele-surveillance may only be conducted if someone is reasonably suspected of an offence and the measure is of exceptional importance to the inquiry.[72] Issues concerning secret wire-tapping and secret tele-surveillance are determined by the court upon the request of the prosecutor, i.e. a court warrant is required prior to use of such surveillance.[73] CSPs shall conduct their operations so a decision on secret wire-tapping and secret tele-surveillance can be implemented.[74] The rules in the Code of Judicial Procedure are quite rigid and additional acts have been adopted which increases the potential scope of surveillance and facilitate the authorization of such measures. For example, in the act on measures concerning certain serious crimes to society the Prosecutor may in situations of urgency, instead of a court, authorize surveillance in regard to crimes such as sabotage, terrorism and hijacking of aircraft.[75] This law only applies to cases when a preliminary investigation has been initiated. If the surveillance measure has been authorized by the Prosecutor, he or she must **(p. 112)** immediately report this decision to the Court who reviews and may cancel the surveillance.[76]

Surveillance measures outside the context of a preliminary investigation are addressed in the act on measures to prevent certain serious crimes. It concerns crimes such as sabotage, terrorism and hijacking of aircraft. In comparison with the act on measures concerning certain

---

[68] Code of Judicial Procedure, chapter 23, section 1.
[69] The Electronic Communications Act (2003:389), chapter 6, section 19.
[70] Code of Judicial Procedure, chapter 27, section 18.
[71] ibid, chapter 27, section 19.
[72] ibid, chapter 27, section 20.
[73] ibid, chapter 27, section 21.
[74] The Electronic Communications Act (2003:389), chapter 6, section 19.
[75] The Act on Measures Concerning Certain Serious Crimes (2008:854) , sections 1 and 4.
[76] ibid, section 6.

serious crimes to society, the difference is that surveillance may be used prior to the initiation of a preliminary investigation but a court warrant prior to the wire-tapping or secret tele-surveillance is required.[77] The prosecutor still has to show a "certain cause to believe that a person will commit an offence", but the evidentiary threshold is quite low. This is similar to the threshold of initiating preliminary investigations but lower than the requirement "if someone is reasonably suspected of an offence" in CJP chapter 27.[78] In an early draft of the law, it was suggested that the surveillance could be used against a person belonging to a group or organisation when there is cause to believe that group or organisation and not necessarily the person affected by the surveillance will commit an offence. This approach would have lowered the threshold for surveillance, but it was rejected.[79] In practice, the act on measures to prevent certain serious crimes has been used very seldom and when it has been used it has been under circumstances very close to a preliminary investigation, where the rules of CJP chapter 27 would be applicable. As a consequence, crime enforcement agencies and a Government rapporteur have asked for amendments of the law, lowering the threshold for surveillance.[80]

Electronic surveillance is also possible under chapter 6 section 22(3) of the Electronic Communications Act, henceforth ECA. It provides that communications providers shall, when there is suspicion of crime and on the request from law enforcement agencies, surrender traffic data in respect of offences when a less severe sentence than two years imprisonment is not prescribed. The provision does 1) not indicate the required standard of evidence, 2) no cause has to be shown in relation to a specific person and 3) such an order does not require a court warrant. In the *Inquiry on Law Enforcement Methods* it is stated that chapter 6 section 22(3) ECA has been interpreted to allow access to traffic data in two main situations: 1) during preliminary investigation when a suspect has not been identified and there is a need to identify such a person **(p. 113)** with the use of stored traffic data; and 2) outside the context of preliminary investigations for intelligence purposes.[81] This means that many of the safeguards set up in CJP chapter 27 and thereto associated acts can be circumvented in relation to traffic data. The *Inquiry on Law Enforcement Methods*, suggests that chapter 6 section 22(3) ECA should be deleted. Instead, it proposes 1) an amendment of CJP chapter 27 on tele-surveillance that would include all access to traffic data during preliminary investigation; and 2) a new act on access to traffic data for intelligence purposes. The latter act would not require a court warrant, but contain a caveat stipulating that a *post hoc* court order is required if the law enforcement agency wants to use the intelligence collected in a preliminary investigation and thus potentially also as evidence against an accused in a criminal trial.[82] In my view, the proposal will not change the patch-work character of the law and the wide powers of crime enforcement agencies in relation to access to traffic data for intelligence purposes. If court warrants are not required prior to the surveillance, compensating measures must be taken, such as an independent mechanism which reviews the surveillance measures after the surveillance has been carried out.

---

[77] The Act on Measures to Prevent Certain Serious Crimes (2007:979), sections 1 and 6.
[78] ibid, section 1.
[79] Government Bill 2005/06:177 Measures to Prevent Certain Serious Crimes, p. 52-57.
[80] SOU 2009:70 Evaluation of the Use of Covert Listening Device and Measures to Prevent Crimes, pp. 15-17, 169-172.
[81] SOU 2009:1, pp. 15, 17, 72-73, 103, 114 and 125-126. The actual practice of various branches of the law enforcements agencies is not consistent.
[82] Draft Act on Access to Certain Data on Electronic Communication in Intelligence Operations of Crime Enforcement Agencies; SOU 2009:1, section 7(3), pp. 136-137, 181.

4.2.2 Processing of Data Pursuant to the Police Data Act

The notion personal data has a wide scope. The preparatory works of the Personal Data Act (1998:204) explain that personal data may include apparently anonymous data that can through a so-called back-door be connected to an individual. The Personal Data Act is the Swedish implementation of the Data Protection Directive which provides the standard that it is enough that a person can be identified; the controller of the personal data does not alone have to be in possession of all the necessary data. Personal data is given a very broad definition, including data that directly or indirectly can identify a person such as phone numbers, so-called net node addresses and "electronic identities.[83] The Supreme Administrative Court affirmed in the case *Svenska Antipirabyrån v. the Data Protection Agency* a decision where the Stockholm Administrative Court of Appeal ruled that data, such as an IP-address, supplemented with information from the communications provider can be used **(p. 114)** to identify a person, i.e. a subscriber of the service. As a consequence, such IP-addresses should be regarded as personal data protected by the Data Protection Directive and the Personal Data Act.[84] Thus, it is submitted that phone numbers or IP-addresses that may identify the identity of a subscriber shall be regarded as personal data.

The Data Protection Directive does not apply to activities of the State in areas of criminal law.[85] The Police Data Act concerns processing of personal data used in law enforcement by the police and the Swedish Economic Crime Authority, for the purpose of preventing crime and disorder, collection of intelligence and investigation of crime.[86] Personal data has been given the same meaning in The Police Data Act as it has in the Personal Data Act,[87] which would mean that both of the acts provide that phone numbers or IP-addresses should be regarded as personal data. There are specific provisions concerning criminal intelligence databases and the Security Service database.[88] Automated processing for criminal intelligence purposes is only allowed if there are reasons to believe that certain serious offences have been committed or will be committed.[89] Turning to practice, the Security Service database is not used in the operative work, the rules on this database is instead applied to the more operatively used Central Database.[90] In addition to the Central Database, the Security Service uses analysis databases to process and analyze data collected through secret wiretapping and tele-surveillance governed by the general rules in the Police Data Act. The access to an analysis databases is limited to the agents working with the specific case. Information relevant for a wider range of agents may be transferred from analysis databases to the Central Database.[91]

Section 5(1) of the Police Data Act provides that it is prohibited to process data about a person solely on the basis of what is known about the person's race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life. However, section 5(2) provides that if data is processed about a person for reasons other than

---

[83] Data Protection Directive, article 2(a); SOU 1997:39, pp. 113 and 341. Article 3 provides that the Data Protection Directive does not apply to processing operations concerning public security, defence and the activities of the State in areas of criminal law. However, some definitions in the Data Protection Directive are also used in legislation related to law enforcement which will warrant some references to the directive.
[84] *Svenska Antipirabyrån v. the Data Protection Agency*, Case 3978-07, Decision 21 April 2009; Data Protection Directive; Personal Data Act (1998:204).
[85] Data Protection Directive, article 3(2).
[86] The Police data act (SFS 1998:622), section 1.
[87] ibid, section 3(7).
[88] ibid, sections 17-21 and 32-36.
[89] ibid, section 14; Government Bill 1997/98:97 The Police Records, p. 119.
[90] Processing of Personal Data by the Police for Law Enforcement Purposes, Ds 2007:43, p. 295.
[91] The Police data act, sections 1-9 and 13; Processing of Personal Data by the Police for Law Enforcement Purposes p. 295, 297-298, 620.

the aforemen- **(p. 115)** tioned, such data may be supplemented with the data mentioned in section 5(1), if it is indispensible necessary. This means that the police cannot chart the political opinion of the entire population, but if a person is involved with politically motivated criminality; such information may be added to his or her file.

4.2.3 Dissemination of Data to Foreign States and International Organisations

Data can be surrendered to a foreign state authority or an international organisation for purposes of criminal investigation, if the surrender is based on an international treaty that subject to the acceptance of the parliament has been acceded by Sweden.[92] Furthermore, Sweden may offer legal assistance to other states in secret wire-tapping and secret tele-surveillance pursuant to the Act on International Legal Assistance in Criminal Matters. Such requests are executed by the responsible prosecutor. The prosecutor shall immediately consider if the prerequisites for the measure exist and in such case apply to the court for permission to undertake the measure.[93]

4.2.4 Monitoring the Use of Secret Surveillance and Processing of Data

Crime enforcement agencies using secret surveillance are subject to monitoring on how they process personal data. Such supervision is done after the data has been collected, which should be distinguished from prior judicial authorization in the form of court warrants.

Internal monitoring is performed by a personal data representative who shall independently assure that the personal data in the Secret Service analysis databases is processed in a correct and lawful manner. Data acquired from wire-tapping and tele-surveillance are kept in such databases [94]

External monitoring is carried out by two agencies, the Data Inspection Board and the Commission on Security and Integrity Protection (hereinafter, the Commission).[95] The Commission carries the responsibility to monitor **(p. 116)** the use by crime-fighting agencies of secret surveillance, associated activities and the processing of data by the Swedish Security Service under the Police Data Protection Act (1998:622), particularly with regard to Section 5 of that Act.[96] At the request of an individual, the Commission is obliged to check whether he or she has been the subject of secret surveillance or subject to processing of personal data as defined in Section 1 and whether the use of secret surveillance and associated activities or the processing of personal data was in accordance with laws and other regulations. The Commission shall notify the individual that the check has been carried out.[97] A problem in this context is that the access to traffic data under chapter 6 section 22(3) ECA is not defined as secret surveillance and as such outside the scope of the Commission's supervision.[98] The *Inquiry on Law Enforcement Methods*, suggests that the scope of the Commissions

[92] The Police data act, section 7.
[93] Act on International Legal Assistance in Criminal Matters (SFS 2000:562), chapter 4, section 25.
[94] Processing of Personal Data by the Police for Law Enforcement Purposes, pp. 297-298.
[95] ibid, pp. 331-332. Act on Supervision of Certain Crime-Fighting Activities SFS 2007:980, section 5 provides that the chair and vice chair of the Commission shall be, or have been, a permanent judge or have other equivalent legal experience. The other members shall be appointed from among the persons proposed by the party groups in the Riksdag (parliament).
[96] Act on Supervision of Certain Crime-Fighting Activities SFS 2007:980, section 1.
[97] ibid, section 3.
[98] SOU 2009:1, p. 154.

supervision should be expanded to include such measures as well.[99]

4.3 Electronic Surveillance of International Communication by the FRA

There are no rules which prohibit the law enforcement agencies to use measures under CJP Chapter 27 in relation to international communication. Thus, if it is technically feasible, CSPs should assist the police in the surveillance of such communication. The problem is that the police does not have enforcement jurisdiction outside Swedish territory and they can only issue their requests to CSPs in Sweden. These CSPs may have technical difficulties to intercept communication when the sender, receiver or both (transit communication) are outside of Sweden.

The FRA has the capability to intercept international communication crossing Swedish borders. It can collect intelligence about foreign powers as well as providing assistance to law enforcement agencies. However, the FRA is prohibited by the Defence Intelligence Operations Act to take measures that aim to solve tasks that are within the scope of the operations belonging to the police or other agencies involved with law enforcement and crime prevention. The FRA can not assume police powers and take investigatory **(p. 117)** measures under CJP Chapter 27 such as secret wiretapping and tele-surveillance.[100] However, the FRA may target the same kind of objects (for example information relating to terrorism) and the prohibition in Defence Intelligence Operations Act does not include collection for signal intelligence purposes.[101] It may also provide assistance to the law enforcement agencies.[102] The powers for law enforcement agencies to request FRA to conduct electronic surveillance through signal intelligence has temporarily been blocked due to political disagreement within the parliament's governing majority and the matter is under review.[103] Thus, at the present time only the Government, the Government office, and the Defence Forces have the authority to request the FRA to conduct electronic surveillance.

What is signal intelligence in the context of electronic surveillance of communications? The preparatory works of the Signal Intelligence Act explain that communications intelligence (COMINT), a sub-category of signals intelligence (SIGINT), consists of the steps 1) collection, 2) processing (traffic processing, cryptanalysis and content processing), analysis and 3) reporting (henceforth dissemination).[104] This means that the surveillance concerns content data as well as traffic data. The following sections will also discuss dissemination of communications to other State agencies and monitoring mechanisms.

The legislation differentiates between *defence intelligence operations* and *auxiliary operations*. *Defence intelligence operations* concern a small faction of all communication that is directly connected to external military threats, international terrorism and similar phenomena. Communication associated to such threats is examined in detail. In contrast the *auxiliary operations* concern a significant part of all communication but it is examined in a more shallow way. The preparatory works state that a purpose of the auxiliary operations "is

---

[99] Draft Act on Access to Certain Data on Electronic Communication in Intelligence Operations of Crime Enforcement Agencies, section 9; Act on Supervision of Certain Crime-Fighting Activities, draft amendment on section 2(2); SOU 2009:1, pp. 154-155.
[100] Defence Intelligence Operations Act (2000:130), section 4(1).
[101] Government Bill 2006/07:63, p. 41, 47-48 and 136.
[102] Defence Intelligence Operations Act, section 4(2).
[103] Signal Intelligence for Law Enforcement Purposes, SOU 2009:66 .
[104] Government Bill 2006/07:46 Processing of Personal Data by the Armed Forces and the National Defence Radio Establishment, p. 29; see also Richelson, Jeffrey T., *The technical collection of intelligence*, Johnson, Loch K. (Ed.), Handbook of Intelligence Studies, 105-117, Routledge, London and New York, 2009, p. 109.

to chart communication paths that may be of interest when collecting information relevant to the defence intelligence operations".[105] What does this mean? I will in the following sections show that collection of content data is done through the defence intelligence operations and the collection of traffic data and other meta data is done mainly in the context of the auxiliary operations. **(p. 118)**

4.3.1 All International Cable Communication is Transferred to the State

The first step involves a legal obligation for the CSPs to transfer all cable communication crossing Swedish borders to certain "interaction points", which may include communication where the sender or receiver is in Sweden.[106] The legislation and the preparatory works do not distinguish between the content data and traffic data, all communication shall be transferred to the "interaction points" which are the places where the CSP surrender the communication to the State. In the view of how modern telecommunication works, it is impossible at the transfer stage to sort out domestic communication that cross the border. It is an automated process how communication is routed. The person who communicates can not decide which medium or combination thereof will be used at a given point of time. It is not even certain that the shortest geographical way will be used. Communications which appear to be purely domestic can therefore take a detour through other countries. The route used is determined by pure economic considerations such as price and capacity. In other words, all cable communications, regardless if it is domestic or international, shall be transferred to "interaction points" which are controlled by the State.[107] The case law of the ECtHR indicates that this is interference with the right to protection of private life and correspondence, regardless if the communication is actually collected and processed.[108] The Council on Legislation (lagrådet) has with similar reasoning in its legal preview made the remark that the interference with individuals communications occurs already when the State gains access to the telecommunications and not only when a certain message subsequently is separated for analysis by the use of search concepts.[109]

4.3.2 Narrow Collection of Content Data and Broad Collection of Traffic Data

The CSP is not involved in any filtering of the communication or data.[110] Instead, the Inspection for Defence Intelligence grants the actual access to specified communication carriers,[111] and the filtering is carried out by the **(p. 119)** FRA when it collects the data from the "interaction points" with the use of certain search concepts in an automated procedure.[112] A communication carrier is the medium for transferring signals, for example a copper wire but more often an optic fibre. The purpose of involving the Inspection for Defence

---

[105] Government Bill 2006/07:46, p. 68.
[106] The Electronic Communications Act (2003:389), chapter 6, section 19(a); Government Bill 2006/07:63, p. 83; The Post and Telecom Agency, Opinion on the Memorandum Adapted Defence Intelligence Operations (DS 2005:30), 27 October 2005, pp. 3-4.
[107] Government Bill 2006/07:63, p. 85.
[108] *Klass and others v. Germany*, paras. 37-38, 41; *Weber and Saravia v. Germany*, para. 78; *Liberty and Others*, para. 56.
[109] Government Bill 2006/07:63, p. 172.
[110] National Defence Radio Establishment, Opinion 27 February 2009, pp. 2-3.
[111] Act on Signal Intelligence in Defence Intelligence Operations (2008:717), section 12(2); Government Bill 2008/09:201 Additional Protection for Privacy in Connection with Signal Intelligence, pp. 36-39.
[112] Signal Intelligence Act, section 3.

Intelligence at this stage is to add privacy protection by restricting FRA's access to communication to certain communication carriers.[113]

The scope of collection is indicated by section 1(1) of the Signal Intelligence Act which concerns *defence intelligence operations* and according to sub-paragraph (2) is restricted to the following purposes: 1) external military threats; 2) factors relevant for peacekeeping operations; 3) international terrorism and international organized crime; 4) the development and proliferation of weapons of mass destruction and arms control; 5) external threats against infrastructure (for example against information and communication technology); 6) conflicts outside of Sweden that effect international peace and security; 7) counter-intelligence; and 8) actions and aims of foreign powers of material interest for Swedish foreign-, security-, and defence policy.[114]

Sub-paragraphs (1) and (2) of section 1 of the Signal Intelligence Act does not distinguish between content data and traffic data which leads to conclusion that both can be collected. In addition, FRA may pursuant to the third subparagraph collect signals for other purposes which are not restricted to the purposes enumerated in the second sub-paragraph. This includes collection in order to 1) monitor changes in the signal environment, the technical development and signal protection, and 2) continuously develop the technique and methodology which is needed in order to carry out operations according to the law (henceforth *auxiliary operations* as opposed to *defence intelligence operations*). The preparatory works explain that collection in the context of *auxiliary operations* concerns metadata (data about data, i.e. channel number and carrier frequence). The *auxiliary operations* do not normally involve the content of messages between individuals. The preparatory works explain that the *auxiliary operations* include the collection of information **(p. 120)** concerning between who communication has occurred,[115] in other words traffic data. Considering that the limitations in sub-paragraph (2) does not apply to *auxiliary operations,* the scope of collection concerning traffic data can be very broad. What is the scope in practice? A TV news broadcaster (SVT's programme Rapport) disclosed in June 2008 that the FRA indiscriminately collects traffic data, including data relating to communication from or to Swedish citizens. The data is stored in the traffic database (*Titan*) for 18 months. The source of the information was a FRA employee who also disclosed a confidential document from a Q&A session held within the FRA supporting the claims made (henceforth the *FRA Q&A document*). The document discusses the scope of the collection and storage in the terms of "all available communication" and "large amounts of information".[116]

It has already been indicated that the collection is done with the use of search concepts in an automated procedure. Search concepts should not be confused with the narrower notion "key words", which would imply that words such as "bomb" or "al-Qaida" are used to screen the content of all messages. This would be improbable considering the huge amounts of communications and the increasing use of encryption. Instead, the preparatory works indicate that search concepts refer to technical parameters such as frequencies, e-mail addresses and

---

[113] Government Bill 2008/09:201, p. 35.

[114] The preparatory works do not explain how signal intelligence can be sued to reveal the "actions and aims of foreign powers". With an international outlook, it is known that signal intelligence has been and is used to target diplomatic communications such as the exchange between a foreign ministry and its embassies or between countries, Johnson, 2009, pp. 111 and 115. This may come in conflict with obligations under article 27 of the Vienna Convention on Diplomatic Relations, 18 April 1961, 500 UNTS 95. However, the preparatory works provide that operations shall be conducted with the respect of Sweden's international obligations, Government Bill 2008/09:201, p. 30.

[115] Government Bill 2006/07:63, p. 72.

[116] FRA, 14 March 2007, Sveriges Television (Publ.), *Frågor & svar*, (16 November 2008), question 5; Struwe, Filip, Sveriges Television (Publ.), *FRA lagrar svenska telesamtal och mejl, 16 June 2008,* .

phone numbers. Different search concepts are used in various constellations.[117] The FRA has at its disposal a targeting database which contains "information on objects, which are targets of signal intelligence".[118] More detailed routines for determining and handling search concepts are defined in the FRA rules of procedure.[119]

A Defence Intelligence Court was established 2009 which authorises the data collection after an application from the FRA but prior to the commencement of collection activites. The application shall include information about 1) the collection operation sought and which needs it aims to fulfil; 2) which communication carrier(s) that FRA need to access; 3) the search concepts or **(p. 121)** categories of search concepts that will be utilized during collection; 4) the time period sought collection; and 5) other relevant circumstances.[120] A search concept is typically not related to a specific person.[121] Categories of search concepts do not relate to specific individual but may for example refer to military commanders in the armed forces of a foreign State or staff members of a nuclear program of a certain country.[122]

How much communication may a carrier of communication, i.e. an optic fibre, transport? The preparatory works indicate that the smallest communication carrier typically is a fibre optic core.[123] According to the CSP Bahnhof one such fibre optic core may transport 1.6 TB/s which is the equivalent of 800 000 households continuously using a 2 MB/s connection. Normally, fibre optics are in pairs to provide two-way communication which makes access to such communication carrier equal to 1.6 million households.[124]

In its opinion on the proposal to introduce a Defence Intelligence Court and restricting access to communication carriers, the Post and Telecom Agency (PTS) made the remark that it is plausible that at an "interaction point" FRA will pursue several collection operations, which would require access to all communication carriers. Against this background, PTS argues that restricting access to communication carriers does not in itself add any privacy protection.[125] I agree with that conclusion. In other words, the FRA will in the stage of collection have access to very large amounts of communication.

The value of introducing a judicial review on the implementation of policies on national security may be questioned. The preparatory works provides that the Defence Intelligence Court shall not take any standing on policy issues such as whether there is a need for collection through signal intelligence or not. The court has received the same instruction in relation to applications from the FRA for the conduct of *auxiliary operation*s.[126] With such instructions, the role of the court runs the risk of being reduced to the review of formalities. Evidence from countries which require prior judicial approval of surveillance warrants such as Canada and the USA does not suggest high rates of refusal. **(p. 122)** Ian Leigh perceives a danger that judges approving intelligence operations lose the qualities of independence and external insight through a process of acclimatisation. As a result the effectiveness of the protection of individual rights may decline. He suggests that there is little difference in the

---

[117] SOU 2003:34 Defence Intelligence and Security Service. Privacy - Efficiency, Memorandum of the Inquiry on Intelligence Data, Stockholm 2003 , p. 129; Government Bill 2006/07:63, pp. 76-77, 90.
[118] SOU 2003:34, p. 17 and 129. In the relevant decree the "targeting database" is designated "database with information on objects, which are targets of signal intelligence", Decree (2007:261) on processing of personal data in defence intelligence- and auxiliary operations of the National Defence Radio Establishment, section 6.
[119] Government Bill 2006/07:63, p. 78.
[120] Signal Intelligence Act, section 4(a).
[121] ibid, section 3(2) and 5(5); Government Bill 2008/09:201, pp. 24, 44, 46, 53.
[122] Signal Intelligence Act, p. 54.
[123] Government Bill 2008/09:201, pp. 36.
[124] Stockholm Faculty of Law, Opinion on the Memorandum on Additional Protection for Privacy in Connection with Signal Intelligence (Ds 2009:1), 24 February 2009, pp. 4-5.
[125] The Post and Telecom Agency, Opinion on the Memorandum on Additional Protection for Privacy in Connection with Signal Intelligence (Ds 2009:1), 23 February 2009, p. 2.
[126] Government Bill 2008/09:201, pp. 57-58

end result with the use of judicial approvals compared to approval within the agency itself or by a government minister. Leigh's conclusion is that there has to be other processes for handling accountability, such as complaints processes and inspectors-generals and monitoring.[127]

4.3.3 Processing through Content and Traffic Analysis

The preparatory works explain that processing involves traffic processing, cryptanalysis and content processing.[128] Content processing would mean to read or listen to a message. The preparatory works indicate that traffic processing involves the identification of who is communicating with whom and determining traffic patterns,[129] sometimes also referred to as traffic analysis,[130] charting and analysis of communications patterns.[131] In the *FRA Q&A document* the FRA methodology of processing data is in parts explained. From the aforementioned document the following information is known.[132]

1. The FRA stores large amounts of information which subsequently is searched through;
2. The FRA distinguishes between how it handles content data and traffic data;
3. In comparison with content data, traffic data is easier to store in large volumes;
4. Traffic data is a tool for targeting decisions and the possibility to determine new parameters for collecting data (for example if a target has changed his or her prepaid phone card);
5. The FRA is very anxious to use traffic data in the future; **(p. 123)**
6. With ever increasing use of encryption and volumes of messages the efficiency of traffic processing will increase in comparison with the traditional non-military content processing; and
7. Search concepts used for collection may include "Swedish parameters"

With reference to methods presented in Section 2.4, it is unknown whether the FRA uses "pattern-based data mining", "subject-based data mining", or both when it processes the traffic data.

A specific law regulates FRA's processing of personal data (henceforth the FRA Data Protection Act),[133] which appear to cover data mining techniques. Chapter 1, section 11(1) of the act specifically provides that personal data may not be processed based solely on what is known about a person' race or ethnic origin, political opinions, religious beliefs or philosophical convictions, trade union membership, health or sex life. However, subparagraph (2) and (3) provides that if data about a person is processed on another basis it may be supplemented with data referred to in the first subparagraph when it is absolutely necessary for the purpose of the processing. Data relating to a persons appearance shall always be treated in an objective manner with respect for the human dignity. This would mean that if the FRA has data on a person in its database, for example a terrorist, it may add information that the person is motivated to commit terrorist acts because of religious beliefs if it is absolutely necessary. A search, for example in a database, may only apply personal data which reveals

---

[127] Leigh, Ian, *The accountability of agencies*, Johnson, Loch K. (Ed.), Handbook of Intelligence Studies, 67-81, Routledge, London and New York, 2009, pp. 76-77; see also Manget, Fred F., *Intelligence and Judicial Intervention*, Johnson, Loch K. (Ed.), Handbook of Intelligence Studies, 329-342, Routledge, London and New York, 2009, p. 330

[128] Government Bill 2006/07:46, p. 29.

[129] ibid, p. 29.

[130] Agrell, p. 97.

[131] Signal Intelligence for Law Enforcement Purposes, p. 106.

[132] FRA "Frågor & svar", questions 5 and 24.

[133] Act on Processing of Personal Data in Defence Intelligence- and Auxiliary Operations of the National Defence Radio Establishment (2007:259).

race or ethnic origin, political opinions, religious beliefs and philosophical conviction, trade union membership, health and sexual life as search parameters if it is absolutely necessary for the purpose of the processing. This is similar to section 5 of the Police Data Act, mindful of the fact that the FRA Data Protection Act uses a more lenient threshold "absolutely necessary" in comparison with "indispensible necessary" used in the Police Data Act.[134]

The FRA has a number of databases which have a legal basis in the FRA Data Protection Act and are regulated more in detail in the FRA's Data Protection Decree.[135] The preparatory works of the FRA Data Protection Act describe the databases and indicate how the various databases are related with each other,[136] which is illustrated in the figure below.[137] **(p. 124)**

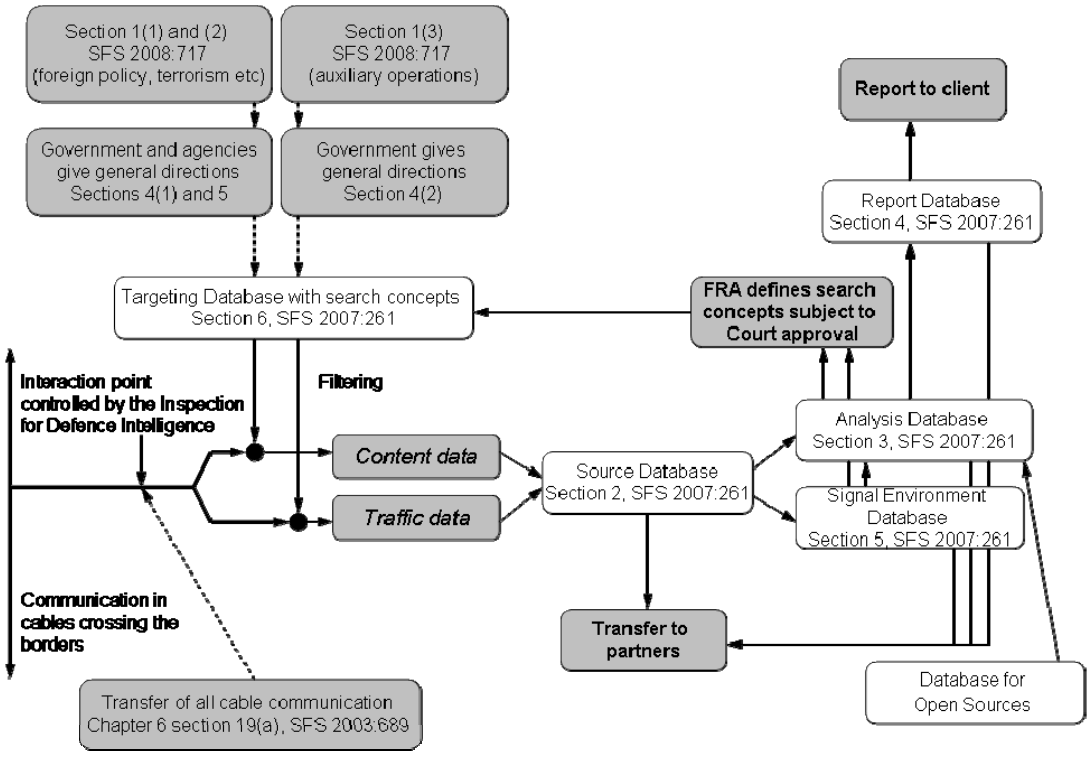

Figure illustrating how the FRA processes communication and information
Mikael Nilsson, Mark Klamberg and Anna Petersson, 2008

The Source Database is the main database for storage of the raw data that has been collected. It is a large database where the storage time varies.[138] The Signal Environment Database contains information and technical parameters relating to the signal environment.[139] Data collected from open sources such as newspapers, TV, radio and the publically available websites is stored in the Database for Open Sources. The collection concerns large amounts of data that are stored for a short time. If a piece of information is deemed relevant, it is transferred to the Analysis Database.[140] The Targeting Database contains information on

[134] Government Bill 2006/07:46, pp. 73-75, 124 and 132.
[135] FRA Data Protection Act, section 7; FRA Personal Data Protection Decree, section 2-6.
[136] Government Bill 2006/07:46, pp. 31-34.
[137] Compare with figure on p. 257 in SOU 2003:34.
[138] FRA Personal Data Protection Decree, section 2; Government Bill 2006/07:46, pp. 32-33.
[139] FRA Personal Data Protection Decree, section 5.
[140] Government Bill 2006/07:46, p. 33

planning and the targets of signal intelligence operations.[141] As indicated, data is transferred from the Source Database and the Database for open Sources to the Analysis Database for processing, cryptanalysis and other analysis. The Analysis Database is an interim storage place for working material before it is finalized into an intelligence report.[142] The finalized intel- **(p. 125)** ligence reports are stored in the Report Database. The reports sought may be accessed in the database by reference to client, date of the report and the subject of the report.[143]

A number of Government bodies and agencies have direct access to the Report Database, including the Government, the Government office, the Defence Forces, the Police, including the Security Service (SÄPO), the National Inspectorate of Strategic Products, the Swedish Customs Service, the Defence Materiel Administration Agency, the Defence Research Agency and the Civil Contingencies Agency.[144] There are no indications that entities outside of the FRA have any direct access to the other databases. This is important from a privacy perspective in regard to the Source Database and Signal Environment Database, because it is likely that the mentioned databases contain large amounts of sensitive "surplus information". This does not mean that raw data is outside the scope of exchange with other countries, but it is done without any external entity having direct access to the databases. Foreign States, their agencies and international organisations do not have direct access to the FRA databases.[145]

As already indicated, the legal framework distinguishes between collection for defence intelligence purposes which is fairly restricted and narrow in scope while auxiliary operations involves collection of information about communication in a much broader extent. Collection for defence intelligence purposes and auxiliary purposes have separate rules and, as illustrated in the next section, only defence intelligence operations generate reports to the clients of the FRA. The preparatory works provide that the auxiliary operations do not generate reports to the clients of the FRA.[146] This creates the impression that a wall has been erected where the large amounts of traffic data collected through the auxiliary operations is used purely for some abstract technical matters and not for intelligence purposes. This is a misconception. First, the preparatory works state that since the auxiliary operations "aim to facilitate the defence intelligence operations it would not be incompatible with the purpose for which the data is collected that the data is also used to some extent in the defence intelligence operations."[147] Second, reports to clients may involve extensive description of traffic patterns.[148] The- **(p. 126)** refore, it is submitted that while traffic data is collected with reference to auxiliary operations purposes, in the processing and dissemination stages the same data may also be used for defence intelligence purposes.

This may be problematic in relation to the finality principle. The text of the law separates the collection of data for intelligence and auxiliary purposes. Different sections of the preparatory works appear to contradict each other on how the data collected for auxiliary data can be used. One section suggests that the auxiliary operations do not generate reports to the clients of the FRA,[149] while an other section provides that data collected for auxiliary purposes may be used for intelligence purposes which in turn generate reports.[150] Is the collection of traffic data for auxiliary purposes in accordance with the requirements of article

[141] FRA Personal Data Protection Decree, section 6; Government Bill 2006/07:46, p. 32.
[142] FRA Personal Data Protection Decree, section 3; Government Bill 2006/07:46, p. 33.
[143] FRA Personal Data Protection Decree, section 4; Government Bill 2006/07:46, p. 34.
[144] FRA Personal Data Protection Decree, section 8.
[145] Government Bill 2006/07:46, p. 84.
[146] Government Bill 2006/07:63, p. 72.
[147] Government Bill 2006/07:46, p. 68.
[148] Signal Intelligence for Law Enforcement Purposes, pp. 59-60.
[149] Government Bill 2006/07:63, p. 72.
[150] Government Bill 2006/07:46, p. 68.

8 of the ECHR on foreseeability and that the law is formulated with sufficient precision? It is argued that such matters must be regulated in a less contradictory, more foreseeable and accessible manner in order to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to measures of surveillance.

4.3.4 Dissemination of Data to the Government, its Agencies and Foreign States

The FRA conducts defence intelligence on the order of the Government and its agencies. From this follows that after collection, processing and analysis FRA will deliver intelligence to the Government and the agencies concerned, henceforth referred to as clients. The intelligence reports are stored in a report database,[151] see figure 1. The auxiliary operations do not generate intelligence.[152] The clients have direct access only to the report database,[153] i.e. processed intelligence as opposed to raw data. A report can be very brief involves a single event (for example the content of a message or information about sender and receiver), or traffic charting (i.e. extensive description of traffic patterns). It may also concern reports of a more strategic nature on international matters and course of events.[154] **(p. 127)**

The FRA may subject to the Governments approval establish and maintain cooperation on intelligence issues with other States and international organisations.[155] The agency may also subject to the Governments approval establish and maintain cooperation concerning its auxiliary operations with other States and international organisations [156] and share processed personal data.[157] It is unknown to what extent such sharing is happening. Through leaks to the media it has been reported that Sweden share large amounts of raw data with the USA and the Baltic States.[158]

4.3.5 Monitoring the FRA

There are two agencies responsible for monitoring the FRA *ex post facto,* the Data Inspection Board and the Inspection for Defence Intelligence.[159] The Data Inspection Board has the main monitoring responsibility and the review by the Inspection for Defence Intelligence is a compensatory measure in regard to the confidentiality that hinders individuals from accessing information about themselves.[160] The Inspection for Defence Intelligence has the specific task to control the use of search concepts, destruction of certain data and reporting.[161] At the request of an individual, the Inspection for Defence Intelligence is obliged to check whether FRA has collected his or her communication, and such a case exists, the inspection shall control that the collection and processing was in accordance with the law. The inspection shall

---

[151] Defence Intelligence Operations Act, section 2; FRA Personal Data Protection Decree, section 4.
[152] Government Bill 2006/07:63, p. 80.
[153] FRA Personal Data Protection Decree, section 9.
[154] Signal Intelligence for Law Enforcement Purposes, pp. 59-60.
[155] Defence Intelligence Operations Act, section 3.
[156] Signal Intelligence Act, section 9.
[157] FRA Data Protection Act, chapter 1, section 17.
[158] NyTeknik, FRA:s metoder granskas efter ny avlyssningsskandal, 27 August 2008.
[159] FRA Personal Data Protection Decree, section 10; Government Bill 2006/07:46, p. 99; Processing of Personal Data by the Police for Law Enforcement Purposes pp. 333-334.
[160] Government Bill 2006/07:46, p. 102.
[161] Signal Intelligence Act, section 10(1). The agency is led by a board appointed by the government. The board members include a chairman and vice chairman who both are or have been judges. Additional members of the board are appointed among persons suggested by the parliamentary party groups, Signal Intelligence Act, section 10(3).

notify the individual that the check has been carried out,[162] but not whether he or she has been subject to surveillance. The inspection shall also monitor the processing of personal data.[163] It may conduct its monitoring through inspections and it reports to the Government.[164] **(p. 128)**

5. Reconstruction of the Notion of Privacy

5.1 Aggregation and Identification

As already indicated law enforcement and intelligence agencies are focusing less on traditional wire-tapping, more on retention of traffic data and traffic analysis of communication patterns. This involves the interception and storage of large amounts of information not only in relation to criminals but also law-abiding and innocent citizens.

If this trend is pursued by the policy-makers, safeguards must be adopted to minimize interference with the privacy of the average citizen and the occurrence of false positives which result in innocent persons being subject to measures such as targeted surveillance, detention and freezing of assets. The presumption of innocence must be upheld and the fact that a person is implicated through automated data-mining can not imply any reversal of the burden of proof. The retention of traffic data either by the CSPs or centrally by a state agency leads to unavoidable interference with the privacy of a large number of innocent citizens. The problem is compounded by the difficulty for a court to distinguish between the suspects and the innocents prior to the collection stage. The use of courts in such cases will simply be window-dressing.

Aggregation of the data and identification of the data with individuals will amplify the interference. Thus, if it is difficult to use court warrants to minimize retention, law enforcement and intelligence agencies that have access to traffic data should minimize their aggregation and identification of the data. Aggregation and identification is done in sequenced procedures at the processing stage. Instead of only focusing on authorization through court warrants, it is submitted that emphasis should be on independent monitoring *ex post facto* in relation to aggregation and identification. Such monitoring and review should, *inter alia*, focus on 1) the amount of traffic data aggregated, 2) the number of persons identified, 3) the number of measures, such as targeted surveillance, detention and freezing of assets, undertaken as a result of the data mining and the 4) the ratio of false positives. In other words, an independent body should investigate the efficiency and interference in privacy of the electronic surveillance and regularly report its findings. This would require that the monitoring body conducts independent sampling of what data is stored, investigates the ways in which it is processed, including which mathematical algorithms are used, and checks what data is shared with others. Summaries of such reviews can be presented to policy-makers, experts and the general public, containing different levels of detail and confidentiality. If policy-makers want law enforcement and intelligence agency to collect and process large amounts of data in the pursuit of security, they must **(p. 129)** also make an effort to win the confidence of the general public that it is worth a limited, but still real sacrifice in privacy for all.

5.2 Evaluating Measures of Electronic Surveillance

When the ECtHR evaluate what is legitimate interference under article 8 of the ECHR, most of its attention is on the question whether a measure is in accordance with law but less on

[162] Decree (2007:852) with instruction for the Defence Review Committee, section 2(4); Signal Intelligence Act, section 10(a).
[163] Decree (2007:852), section 3.
[164] ibid, section 4.

whether it is necessary in a democratic society. The Court has stated that the national authorities enjoy a margin of appreciation. On the other hand, new methods of surveillance are not sufficiently analysed by national policy-makers before they are introduced and the measures are not sufficiently evaluated after their introduction. As already indicated, domestic legislator should assume the responsibility to evaluate measures of electronic surveillance in terms of necessity and efficiency. The ECtHR should adjust its standard on legitimate interference of privacy and require in-depth analysis on necessity and efficiency, especially in relation to systems of mass surveillance.

What is an adequate methodology for such analysis? Sometimes there is a lack of factual support for a certain perceived threat. In such cases law enforcement agencies may adopt misguided countermeasures to detriment of, due process, privacy and the general efficiency of crime control. In consequence, wrong prioritisation and faulty perceptions of threats may increase the number of victims of crime. The criminologist Janne Flyghed asserts that certain criteria must be fulfilled before new measures on surveillance and other intelligence-gathering activities are introduced, that may infringe upon the right to privacy. Otherwise there is a risk of an expansion of control and surveillance measures to the detriment of the right to privacy and without any gains to the effort of crime control. He suggests the following four criteria:[165]

1. The threat criterion. Are there data showing that new or old threats have become more immediate? Is there any reliable and verifiable evidence of this?
2. The damage criterion. If the threat is realized, will it produce substantial harm?
3. The effectiveness criterion. Is there evidence that the countermeasures are effective in relation to the relevant threat? And if so, is the level of effectiveness proportional to the cost?
4. The proportionality criterion. Is the interference with the individual's privacy threat and damage proportional in relation to the threat and the potential harm? **(p. 130)**

Janne Flyghed makes the observation that in the discussion relating to serious organized crime, terrorism and comparable acts, the damage criterion is the least problematic. If such threats become real and are carried out, there is no doubt that they will inflict serious damage. The perception of threats relates to future threats. Modern discussion on perception of threats relates to vague concepts such as "organized crime", "international crime", "cross-border crime" and "terrorism" crime.[166] The fact that threats sometimes are vague does not necessarily make them less dangerous. The explicit aim (external rationale) may relate to combating crime and maintaining public order. The creation of perceptions of threats may also have implicit interests (internal rationale), such as bureaucrats seeking budget maximation.[167] Other motives may include the interest of divert attention from other problems. Such implicit aims tend to lead to overestimation of threats. Janne Flyghed argues that the logic of threat analysis contributes to a *normalisation of the exceptional*, which entails the *normalisation of the perceived threats* and the *normalisation of the means of response*. The latter relates to policing methods.[168] Flyghed's conclusion is that if the answer is in the negative concerning the threat criterion, additional coercive measures should not be introduced. However, even if elements 1-3 may be answered in the affirmative, one has to consider whether the measure is proportional. For example, if it could be established that torture is an efficient method, it would still not be compatible with basic rules of law.[169]

---

[165] Flyghed, 2005, pp. 172-173.
[166] ibid, p. 168.
[167] Flyghed, Janne, *Normalising the Exceptional: the case of Political Violence*, Policing and Society, vol 13, 1, 2002, pp. 23-41, pp. 35-36.
[168] ibid, pp. 28-29.
[169] Flyghed, 2005, p. 173. Compare with the National Reasearch Council that also has presented twelve framework criteria for evaluating the effectiveness of information based programs, National Research Council, 2008, pp. 47-51 and 59

A problem in this context is that law enforcement and intelligence agencies may collect data with springboard or lead potential to other information or evidence without the intent to use the springboard data in a court or to reveal it in public through any other means. For example, the police may use wire-tapping in order to detect a crime and arrest the suspected criminals, but the evidence eventually presented in court is not from the wire-tap but instead in the form of tangible evidence collected at the time of the arrest. This is done to conceal the surveillance assets and methods of the agency. In consequence, it may be difficult to properly evaluate the actual surveillance measures, as they may appear inefficient, not being used in court.

Even though it is outside the scope of this article to determine the most appropriate methodology on how to evaluate measures of electronic sur- **(p. 131**) veillance, I submit that policy-makers and courts should pay greater attention to this matter.

5.3 Signals Intelligence and Preliminary Investigations in Criminal Cases

The legal framework regulating electronic surveillance is a patchwork which may be illustrated though the use of a table with four fields. The horizontal axis related to whether the law regulates 1) preliminary investigations or 2) intelligence measures. The vertical axis relates to whether the law "mainly" relates to electronic surveillance of 1) domestic communication or 2) international communication. I use the caveat "mainly" because laws whose main scope is domestic communication may also apply to international communication when only one of the parties is on foreign territory and the target is on domestic soil. In the table below, the Swedish legal framework on collection of communication is illustrated.

International Communication	• Not available	• Signal Intelligence Act
Domestic Communication	• Chapter 27 of the Code of Judicial Procedure • Chapter 6 section 22(3) of the Electronic Communications Act (2003:389) • Act on measures concerning certain serious crimes (2008:854)	• Act on measures to prevent certain serious crimes (2007:979) • Chapter 6 section 22(3) of the Electronic Communications Act (2003:389)
	Preliminary Investigation	Intelligence Measures

Table illustrating the legal framework regulating electronic surveillance

In a Government inquiry which included a comparative analysis of the legislation in Sweden and other countries, Anders Eriksson stated that the Swedish law uses the term "signal intelligence" to designate the surveillance measures covered by the Signal Intelligence Act. He argues that signal intelligence, secret wire-tapping and secret tele-surveillance are different terms to intercept the same type of communications. In other comparable countries, more general terms are used to denote surveillance of telecommunications, without taking into consideration the surveillance method, the agency conducting it **(p. 132)** and the purposes it

serves. The term "signal intelligence" is only used in the Swedish legislation, a fact which has caused confusion in Anders Eriksson's contacts with agencies in other countries. He suggests that surveillance of communications should be regulated in a more general manner where the purposes and limits of such surveillance are defined.[170] However, in his inquiry he still uses the term "signal intelligence" and to suggest a general framework was outside the mandate of the inquiry. In addition, Anders Eriksson suggests that signal intelligence towards international communication should be allowed for the purpose of a preliminary investigation.[171] I find the proposal problematic for the following reasons.

Data collected for the purpose of a preliminary investigation can be used in a court as incriminatory evidence. Sweden as many other countries have fair trial requirements and rules providing that the Prosecutor must disclose all evidence that he/she intends to use at trial[172] and allow the defence to inspect material in possession or under the control of the prosecution (*partsinsyn*).[173] Furthermore, the police and the Prosecutor must act impartially, which means that they must investigate incriminatory as well as exculpatory evidence.[174] This means in turn that all data collected through signal intelligence and that is relevant for the case must be disclosed or made available to the defence through inspection. Such disclosure would probably be impossible due to the sensitive nature of signal intelligence operations.[175] Thus, it appears difficult to meet fundamental fair trial requirements when using signal intelligence for the purpose of a preliminary investigation. **(p. 133)**

6. Conclusion

In academia mush attention has been given to electronic surveillance in the context of preliminary investigations while intelligence measures have to large extent been neglected. This is partly due to the fact electronic surveillance for intelligence purposes has not been legally regulated.

The concept of privacy has to be understood in a contextual manner where we acknowledge that interference in privacy may occur in different forms of activities, including collection, processing and dissemination. How do we compare the interception of the content of a single message targeted against an individual with indiscriminate collection of traffic data? The traditional approach has downgraded the interference involved with the collection of traffic data. I have attempted to explain that aggregation and analysis of traffic data may be more intrusive than interception of separate text messages.

Law-makers struggle with the question where to set the limits of the State's powers when at the present time technology allows near total social control. New surveillance measures have been introduced without earnest consideration of their consequences on due process, privacy and efficiency. Experience shows that the introduction of a requirement that surveillance has to be approved by a court does not solve all of the problems. Electronic surveillance law is a patch-work. This situation deserves earnest consideration, and it is time for legal scholars to do just that in order to expose the conflict between frequently opposing interests. Such work could provide useful information about how to create proper evaluation

---

[170] Signal Intelligence for Law Enforcement Purposes, pp. 39-40.
[171] ibid, pp. 126-128, see section 5 in the draft law on signal intelligence against foreign matters for law enforcement purposes.
[172] Code of Judicial Procedure, chapter 45, sections 4(4) and 9(2).
[173] ibid, chapter 23, section 23(4); Public Access to Information and Secrecy Act (SFS 2009:400), chapter 10, section 3(1).
[174] Code of Judicial Procedure, chapter 23, section 4; Office of the Prosecutor-General, Opinion on the Inquiry on Signal Intelligence for Law Enforcement Purposes, p.3; see also chapter 20, section 2(3) on the Prosecutor's power to make an appeal in favour of the defendant.
[175] Signal Intelligence Committee, Opinion on the Inquiry on Signal Intelligence for Law Enforcement Purposes, p. 5; Data Inspection Board, Opinion on the Inquiry on Signal Intelligence for Law Enforcement Purposes, p. 2.

tools and a more coherent and transparent body of law. Before new powers are given to law enforcement and intelligence agencies, we must consider whether it is really necessary in view of the already existing tools of surveillance. Balancing the security needs for surveillance against privacy interests may not always guarantee that the latter will triumph, but it should at least be in the scales. **(p. 134)**