REGERINGSKANSLIET

Ministry for Foreign Affairs
Sweden
Department for International Law,
Human Rights and Treaty Law (FMR)

Stockholm, 27 April 2012
UDFMR2012/144/ED

IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application no. 35252/08

Centrum för rättvisa

v.

Sweden

OBSERVATIONS OF THE GOVERNMENT OF SWEDEN ON ADMISSIBILITY

I. Introduction

1. These observations on the admissibility of the application introduced by Centrum för rättvisa are submitted on behalf of the Swedish Government in response to the invitation of the Court dated 16 November 2011.

II. The Facts

Circumstances of the case

2. The statement of facts prepared by the Registry of the Court consists essentially of the applicant firm's description of domestic law and practices concerning signals intelligence. For its own part, the Government would like to give the following description thereof.

Background

3. The applicant firm complains that Swedish state practice and legislation concerning intelligence work in the form of signals intelligence have violated and continue to violate its rights under Article 8 of the Convention. It also complains that it has had no effective domestic remedy through which to challenge this violation. The applicant firm's allegations concern the following three time periods: a) from the establishment of the applicant firm in 2002 to the entry into force of the Signals Intelligence Act (2008:717) on 1 January 2009 (the first period), b) from 1 January 2009 to the entry into force of the amended Signals Intelligence Act on 1 December 2009 (the second period) and c) from the entry into force of the amended Signals Intelligence Act on 1 December 2009 and onwards (the third period).

4. At the outset, the Government would like to give some background on foreign intelligence and signals intelligence, as well as an overall description of current work and regulations in this field. A more detailed presentation of relevant domestic law and practices will follow with reference to the three time periods.

5. Foreign intelligence work is conducted in support of Swedish foreign, defence and security policy, and to identify external threats to the country. Foreign intelligence work also includes Sweden's participation in international security cooperation. Sweden's foreign intelligence activities developed after the Second World War in response to the threat scenario that totally dominated during the Cold War – namely an external military threat from another state or group of states. Legislation on foreign intelligence was introduced in 2000 with the Foreign Intelligence Act (2000:130).

6. The agencies responsible for foreign intelligence work are the Swedish Armed Forces (*Försvarsmakten)*, the National Defence Radio Establishment (*Försvarets radioanstalt)*, the Swedish Defence Materiel Administration (*Försvarets materielverk*) and the Swedish Defence Research Agency (*Totalförsvarets forsknings-institut*). These agencies had, and continue to have, the task of identifying at an early stage, and reporting on or warning about, changes in the international situation that may give reason for a political decision to adjust the total defence. In the short term, the agencies are to continuously provide information to serve as a basis for such decision-making, so that there is time to adapt the defence organisation's military capacity before a potential attack. However, providing information on changes in the international situation that may motivate decisions on longer-term adaptation is also part of the task. This is a matter of being able to predict conflicts, process collected data and communicate assessments about security policy and military conditions. Response forces also require information about security and operations when they are in the field.

7. Since the end of the Cold War the threat scenario has changed considerably. Although any form of direct armed military attack on Sweden by another state is unlikely in the foreseeable future, the risk of armed conflicts, incidents and violations of Sweden's territorial integrity cannot be ruled out. Monitoring military developments in our region therefore remains an important task for Swedish foreign intelligence. Another central and increasingly important task for foreign intelligence is to provide the Government with background material for decisions on foreign, defence and security policy issues. Security policy is a broad part of and name for the measures taken by the Government within the context of foreign and defence policy to protect against external threats to the country and to safeguard the country's peace and independence. Developments in security policy over the past decade have raised a number of issues. The concept of security has acquired broader implications. Various non-traditional threats and risks must now be given greater attention in security policy and thus also in intelligence work. These threats and risks include terrorism, proliferation of weapons of mass destruction, large-scale international crime of a sophisticated nature, e.g. the smuggling of arms, drugs or human beings and threats to the technical infrastructure, in particular electronic communications and data-processing systems.

8. The hallmark of these types of risks and threats is that they more often than not originate from non-state actors and are of a transnational and non-military nature. The threat scenario is often complex and concerns several sectors of society. The knowledge required for an effective national policy to combat

these threats and risks is spread over a larger number of agencies than before and involves broader points of contact and cooperation between agencies than has traditionally been the case.

9. Furthermore, Sweden's traditional involvement in international peace support and humanitarian operations, as well as Sweden's membership of the EU, lead to increasing demands for active Swedish participation in civilian and military crisis management abroad. This in turn increases the need for foreign intelligence to provide information that is relevant to decisions on Swedish participation and to the protection of Swedish personnel. This often involves geographical areas far from our region and functional areas that are relatively new for foreign intelligence, such as medical intelligence or organised crime of a nature and scale that may have consequences for security policy.

10. The term 'external threat to the country' means that the threat must be of such a sophisticated nature that it can be considered to be targeted at the security of the realm or at structures that are vital to the functioning of society. International crime thus largely falls outside the mandate of foreign intelligence work. Section 4 of the Foreign Intelligence Act clarifies where the line is drawn between foreign intelligence work and police crime prevention (cf. para 15).

11. Limiting foreign intelligence work to foreign circumstances means that the aim of this work is typically to collect, process and communicate information on phenomena and circumstances in other countries, so as to provide Swedish decision-makers with better data for decisions and assessments in matters of foreign, security and defence policy, or to protect Swedish personnel participating in international operations. It deserves to be stressed that foreign intelligence must, for obvious reasons, be protected by strict secrecy. It goes without saying that there is very limited scope for giving outside parties an insight into the activities, even in the very long term. The need to keep secret both the methods and the results applies for a very long time, and the work is organised in a compartmentalised way.

12. The Government determines the tasking directives for foreign intelligence. Within the context of these tasking directives, agencies appointed by the Government can issue more detailed tasking directives.

13. Signals intelligence is a special form of intelligence collection used in the context of foreign intelligence work. Signals intelligence is conducted by intercepting electronic signals. One of the purposes of signals intelligence is to give advance warning of circumstances in the international environment that may

affect the country from a security policy and military perspective, e.g. an armed attack or violation of Sweden's territorial integrity.

14. Signals intelligence within foreign intelligence is conducted by the National Defence Radio Establishment. The National Defence Radio Establishment is a civilian agency that was formed in 1942 with the main task of conducting signals intelligence services. Signals intelligence work is traditionally divided into communications intelligence (COMINT) and electronic intelligence (ELINT). COMINT targets signals that carry some form of communications content, whereas ELINT targets non communicative electromagnetic emissions, e.g. radar signals.

15. Foreign intelligence does *not* include law enforcement or crime prevention operations. Hence, signals intelligence may not be used to collect information for use in investigating crime. This is clear from Section 4 of the Foreign Intelligence Act. For the sake of clarity, the Government would like to point out that measures for the investigation of crime, for example covert interception and surveillance of electronic communications, are regulated in other legislation. Under Chapter 27 of the Swedish Code of Judicial Procedure, covert interception and surveillance of electronic communications may be used in preliminary investigations relating to certain serious offences.

16. During the Cold War, the signal environment was characterised by a low pace of change. The publicly available services for international communication were essentially limited to telephone, fax and telex. The capacity for international communication (e.g. the number of simultaneous calls abroad from a given country at any one time) was limited. Foreign military and state actors normally had specially built communication solutions at their disposal (e.g. shortwave and satellite systems) that were not used by anyone other than the actors themselves. In the area of encryption, there were few solutions available to the public, which is why encryption was normally used in military or state contexts at the time. Altogether, this meant that the traffic that was relevant at the time for signals intelligence was easier to distinguish and identify, which is why the risk of collecting irrelevant traffic of a private nature was minor. The need for a statutory regulation of signals intelligence based on privacy protection aspects was thus not as pronounced at that time.

17. Today's signal environment is characterised by a high pace of change with regard to new ways of exchanging information over long distances. Similarly, today's commercial mass market technologies – such as the Internet and mobile telephony – are also used by the kinds of actors that would traditionally have

used specially built communication solutions (e.g. foreign military actors). The fact is that commercial mass market technologies are currently used by *all* types of actors operating within the phenomena against which signals intelligence is targeted. This is also why it is absolutely essential for a modern signals intelligence organisation to be able to target these communication methods. The collection of signals in international electronic communications cables is also necessary as current traffic is mainly transmitted through these. However, all this has meant that a need has arisen to regulate signals intelligence to take account of privacy protection, as the collection that is conducted today runs a greater and more obvious risk than during the Cold War of touching on irrelevant traffic of private nature.

18. Signals intelligence work within the National Defence Radio Establishment is intended to generate intelligence in accordance with the detailed tasking directives given by those commissioning the intelligence on the basis of their precise intelligence requirements. This intelligence refers to information that may be useful to those commissioning the intelligence in formulating Swedish foreign, security and defence policy, and in identifying external threats to the country. Signals intelligence exclusively targets *foreign situations*, even though some of these may have ramifications in Sweden (e.g. when following the espionage operations of a foreign power targeting Sweden). The purposes for which the National Defence Radio Establishment is permitted to conduct signals intelligence are further clarified by law. Signals intelligence at the National Defence Radio Establishment may *not* target domestic traffic or domestic circumstances. Claims about "intensive mass interception of all Swedes' traffic" are incorrect and do not correspond to the National Defence Radio Establishment's mandate as regulated by law, the tasking directives or – as is described in more detail below – the way in which signals intelligence is conducted.

19. The more detailed tasking directives of signals intelligence must be accommodated within the framework of the Government's tasking directives for all foreign intelligence work and the special purposes for which signals intelligence is permitted. Signals intelligence at the National Defence Radio Establishment is conducted exclusively on the basis of detailed tasking directives from those commissioning the intelligence and who are entitled by statute to determine the detailed tasking directives of signals intelligence. The detailed tasking directives of signals intelligence may currently be determined by the Government, the Government Offices *(Regeringskansliet)* and the Swedish Armed Forces. The National Defence Radio Establishment does not conduct signals intelligence for its own intelligence needs. However, the National Defence Radio

Establishment is allowed to collect signals for the purpose of the technical and continuing professional development necessary for foreign intelligence. A permit procedure is in place according to which the National Defence Radio Establishment is only allowed to collect electronic signals after obtaining a permit from the Foreign Intelligence Court *(Försvarsunderrättelsedomstolen)*.

20. The signals intelligence process, which is described in more detail below (para. 22), is governed by the tasking directives determined by those commissioning the intelligence, on the basis of their precise intelligence requirements, permits from the Foreign Intelligence Court, collection plans for various types of signals, the exact formulation and use of selectors, etc. Therefore, contrary to what is claimed in the complaint, it is not a matter of 'chance' which signals are collected. The fact that signal traffic can take various paths, via cable or wireless, and can thus appear random is another matter entirely. It deserves to be stressed that signals intelligence work is conducted with limited resources; hence there is a constant effort to subject only relevant traffic to human scrutiny (cf. para. 37). The regulations cover intelligence collection via both cable and wireless.

21. With signals intelligence, electronic signals are collected, processed and analysed. The results of this work are reported to the relevant agencies. The collection that takes place is regulated by Section 1 of the Signals Intelligence Act. The descriptions below are technically neutral, i.e. they are suitable for signals intelligence targeting terrestrial or satellite radio communications as well as cable traffic.

22. The signals intelligence process can be broadly divided into six stages:

1) Firstly, a choice is made as to which parts of the signal environment (e.g. frequency bands for satellite communications) are the most relevant to be collected at any given time, with regard to the permits issued for signals intelligence at that time, the detailed tasking directives from those who have commissioned the intelligence and that reflect their precise intelligence requirements, and also with regard to the practical limitations of the National Defence Radio Establishment's collection capacity.

2) The relevant traffic that is present in the relevant parts of the signal environment is then collected. When signals are collected automatically, selectors are used to identify the relevant traffic. Selectors are formulated with great precision with regard to the targeted foreign phenomena, and in accordance with the detailed tasking directives determined by those who have commissioned the

intelligence, on the basis of their precise intelligence requirements, the permits from the Foreign Intelligence Court, and purposes ultimately decided by the Riksdag.

3) The traffic collected is processed in order to refine the information and make it more usable from an analysis perspective. Examples of processing include cryptanalysis and language translation. This refinement can be done automatically or manually.

4) The processed information is analysed.

5) A report is submitted to those who commissioned the intelligence and other agencies concerned.

6) Feedback is given to all parts of the process. Feedback can take place through internal processes and from those who commissioned the intelligence.

Relevant domestic law and practices

23. Domestic provisions of relevance to the present case are found in a number of acts. Certain constitutional provisions regarding fundamental freedoms and rights found in the Instrument of Government provide the starting point. Foreign intelligence and signals intelligence is regulated in a number of acts, which will be described in more detail below. Other domestic provisions of relevance are found in, *inter alia*, the laws and regulations governing the work of the Parliamentary Ombudsmen *(Riksdagens ombudsmän)* and the Chancellor of Justice *(Justitiekanslern)*. Regulations and case law concerning damages are also of relevance.

Constitutional provisions

24. Under Chapter 2, Article 6, first paragraph of the Instrument of Government everyone shall be protected in their relations with the public institutions against, for example, examination of mail or other confidential correspondence, and against covert interception and recording of telephone conversations or other confidential communications. "Public institutions" here means both public executive bodies and legislative bodies, when they make decisions on provisions of public law that are onerous for individuals (Govt. Bill 1975/76:209, p. 86).

25. What the constitutional provision is protecting is the confidentiality of communications between individuals. The protection does not cover communications taking place in public gatherings, for example, or in radio

broadcasts, since the communication cannot be considered confidential in the sense of the provision. The same applies in principle in regard to radio communication that is transmitted openly over the air. Nor does the protection include postal items that can easily be read by others, such as postcards.

26. The preparatory materials for the Instrument of Government show that it goes without saying that protection for fundamental rights and freedoms can be claimed not only by natural persons but also by legal persons, in the cases this seems natural (Govt. Bill 1975/76:209, p. 141). It may be regarded as natural that the right to protection for confidential communications applies to both natural and legal persons.

27. Under Chapter 2, Article 20 of the Instrument of Government, protection for confidential communications among other things may be restricted in law. It follows from Article 21 of the same chapter that such restrictions may only be imposed to satisfy purposes acceptable in a democratic society. A restriction may never go beyond what is necessary with regard to the purposes for which it was imposed, nor may it extend so far that it represents a threat to freedom of opinion, which is one of the fundaments of democracy. No restriction may be imposed solely on grounds of political, religious, cultural or other beliefs. In addition, such provisions may not imply discrimination of persons belonging to a minority group or the unfavourable treatment of a person on the grounds of gender (Chapter 2, Articles 12 and 13 of the Instrument of Government).

28. It does not directly follow from this regulation that rules should be enshrined in law when it comes to how and to what extent public institutions may use information obtained through restrictions in the protection of confidential information. However, it has been considered most in line with the purpose of the protection of privacy in the Instrument of Government to provide basic provisions on use in this context in the form of law (Riksdag Committee on Justice JuU 1976/77:20 p. 48 f.).

29. Under the Act concerning the European Convention for the Protection of Human Rights and Fundamental Freedoms (1994:1219) (hereinafter the European Convention Act), this Convention is applicable as amended by Protocols 11 and 14, and supplemented by Protocols 1, 4, 6, 7 and 13, as law in Sweden. Hence, under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter the European Convention) everyone has the right to respect for his or her private and family life, his or her home and his or her correspondence. This right may not be restricted by public institutions other than under the provisions of law and if

necessary in a democratic society with regard to certain given purposes, including national security, public safety or for the prevention of disorder or crime. Moreover, under Article 13, everyone whose rights and freedoms as set forth in the Convention are violated shall have an effective remedy before a national authority, notwithstanding that the violation has been committed by persons acting in an official capacity.

30. It follows from Chapter 2, Article 19 of the Instrument of Government that no act of law or other provision may be adopted which contravenes Sweden's undertakings under the European Convention and the Protocols to the Convention that Sweden has ratified and that have come into force. This provision was introduced when the Convention was incorporated into Swedish law and signifies that the Convention has special significance but without giving it constitutional status (Govt. Bill 1993/94:117, p. 53). This provision is primarily directed at the legislator, but can also be cited by courts and managing authorities in support of setting aside a legislative provision in accordance with the rules of judicial review in Chapter 11, Article 14 and Chapter 12, Article 10 of the Instrument of Government.

31. The provisions on judicial review mean that courts and other public bodies that find that a provision conflicts with a rule of fundamental law or other superior statute may not apply that provision. The preparatory materials point out that the person applying the law must first and foremost resolve any conflicts between the European Convention Act and other laws in accordance with normal principles of interpretation of law. The preparatory materials provide support for the person applying the law, in applying the principle of interpretation in conformity with the Convention, then giving the European Convention particular weight – due to its special nature – in cases of conflict with provisions of domestic law (Govt. Bill 1993/94:117, p. 38). If, despite this, a real conflict of laws is considered to exist, the person applying the law may need to consider applying the rules of judicial review in the Instrument of Government in the individual case.

Signals intelligence

32. The regulatory framework that steers the National Defence Radio Establishment's signals intelligence work within foreign intelligence aims to clarify the purposes of signals intelligence and the methods used, and to safeguard privacy protection. Based on the requirements on the signals intelligence work conducted by the National Defence Establishment, and on privacy protection aspects, the regulations have been developed in the area over

the three periods. In many respects, however, signals intelligence work has been conducted in a similar fashion during all three relevant time periods – it has always been a matter of collecting, processing and analysing electronic signals and reporting the results to relevant agencies. During all three periods, the work has exclusively targeted foreign circumstances. The differences that have been relevant between the three periods have mainly involved the forms of the tasking directives, the agencies that may determine the detailed tasking directives of signals intelligence, the arrangements for permits, the scope of the obligation to destroy information and the forms of supervision. In addition, there have of course also been differences purely related to the technology and methods used, caused by changes in the signal environment (e.g. new communications services), as well as the development of new signals intelligence tools.

33. During the first and second periods, the mandate of the National Defence Radio Establishment was limited to signals intelligence targeting wireless traffic. Signals intelligence targeted foreign or international traffic transmitted by terrestrial or satellite radio communications systems.

34. The second period saw the addition of comprehensive regulations that were intended to protect privacy, while the description of what foreign intelligence is allowed to involve was narrowed down and the dividing line against law enforcement was clarified. The purposes for which it was permitted to conduct signals intelligence were regulated by statute. There was no collection from cable traffic during this period as the obligation on the part of the cable owners to pass on signals that cross the Swedish border did not enter into force until the third period.

35. From the start of the third period, the National Defence Radio Establishment's mandate to conduct signals intelligence was broadened to the extent that electronic signals may also be collected from international electronic communications cables that cross the Swedish border. The expansion of the mandate was not brought about by any change in the overall tasking of the National Defence Radio Establishment; instead, it is a result of fibre optic cables gradually and increasingly replacing communications satellites to convey international communications. Hence, it is essential for a modern signals intelligence organisation to collect signals in international electronic communications cables (cf. para. 17). The third period also saw the addition of even greater privacy protection.

36. For the National Defence Radio Establishment to gain access to signals in cables crossing the nation's borders, a decision is required from the Foreign

Intelligence Court. Such decisions refer to specific optical fibres in the international telecables that are to be made available to the National Defence Radio Establishment. The optical fibres are called 'signal carriers' *(signalbärare)* in the legislation. The cable-bound signals contain the same types of traffic as signals carried via radio communications systems (e.g. satellites), which is why the expanded mandate has primarily called for new capabilities with regard to collection rather than processing and analysis. This is because signals in optical cables have in certain respects different technical characteristics compared to radio signals.

37. The expansion of the National Defence Radio Establishment's mandate during the third period has meant that it has gained access to a larger *proportion* of the total volume of traffic carried between various countries throughout the world. As staff numbers at the National Defence Radio Establishment have remained relatively constant over the three periods, the increased access to traffic has also meant that the Establishment has had to make its data reduction even more efficient. This is done through the automated process which, by using selectors, identifies individual pieces of information that may eventually be subjected to human scrutiny, and not least through making the selectors used even more precise. Although it may seem paradoxical, access to a larger *proportion* of traffic actually means that fewer individuals run the risk of having their traffic manually scrutinised by an employee at the National Defence Radio Establishment. The reason for this is that access to a larger *proportion* of traffic means that the collection of information, with better chances of achieving favourable results, can be targeted directly at the core of phenomena referred to in the permits from the Foreign Intelligence Court.

38. Signals intelligence work is conducted with limited resources and has to be done as efficiently as possible, not least through the constant effort to subject only relevant traffic to human scrutiny. The parliamentary committee that was given special instructions by the Government to review the National Defence Radio Establishment's signals intelligence work (the Signals Intelligence Committee) also highlights in its conclusions from February 2011 that the National Defence Radio Establishment is striving – for reasons of efficiency – to limit the collection to specific material that is relevant from an operations perspective and that efficiency and privacy protection interests coincide in this respect. The committee also notes that this is something that is built into the work and that this benefits privacy protection, irrespective of legislation (SOU 2011:13).

39. After this general background on relevant domestic law and practices concerning signals intelligence, the regulatory frameworks applicable during the periods in question are described in more detail below.

From the establishment of the applicant firm in 2002 to the entry into force of the Signals Intelligence Act on 1 January 2009 (First period)

(1) General provisions on signals intelligence

40. The signals intelligence conducted by the National Defence Radio Establishment during the period 2002 – December 2008 was mainly regulated in the Foreign Intelligence Act and the Foreign Intelligence Ordinance (2000:131), the Electronic Communications Act (2003:389) and the Ordinance containing instructions for the National Defence Radio Establishment (2007:937).

41. Under the Foreign Intelligence Act, foreign intelligence was to be undertaken to identify *external military threats to the country* and to support foreign, defence and security policy. Foreign intelligence included involvement in Swedish participation in international security cooperation and, in accordance with what the Government decided, involvement in supporting society in the event of serious peacetime emergencies. The Government decided the more detailed tasking directives of foreign intelligence. Foreign intelligence was to be conducted by the Swedish Armed Forces and the other agencies determined by the Government (Section 1).

42. Foreign intelligence was conducted through the collection, processing and analysis of information. Analyses of threats and assessments in intelligence matters were to be reported to the Government Offices and other agencies concerned (Section 2). The agencies that were to conduct foreign intelligence might, in accordance with specific instructions from the Government, establish and maintain cooperation in intelligence matters with other countries and international organisations (Section 3). Under Section 4, foreign intelligence should not involve tasks that, under the law and other regulations, lie within the scope of the law enforcement and crime prevention work of the Swedish Police *(Polisen)* and other agencies. Foreign intelligence was not allowed to include the carrying out of activities that involve police powers, such as preliminary investigation measures under the Swedish Code of Judicial Procedure or the use of coercive methods under the Police Act (1984:387) and other legislation (cf. para. 15). However, the foreign intelligence agencies were permitted to assist other agencies in accordance with specific instructions from the Government. For example, the technical knowledge or equipment of an agency active in signals intelligence within foreign intelligence was, if requested by the Government, to

be used in support of the exercise of public authority for which another agency was responsible. Under Section 5, a special board under the Government was to monitor the foreign intelligence work, as specifically prescribed by the Government (cf. paras. 49-52).

43. In the Foreign Intelligence Ordinance, the Government had specified that the Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Defence Materiel Administration and the Swedish Defence Research Agency were the agencies to conduct foreign intelligence work (Section 2). The agencies that conducted foreign intelligence work could only cooperate on intelligence matters with other countries and international organisations on condition that the purpose of the cooperation was to serve the Swedish central government leadership and the Swedish total defence. The information passed on by agencies to other countries must not be detrimental to Swedish interests (Section 3).

44. Under the Ordinance containing instructions for the National Defence Radio Establishment, the task of the Establishment was to conduct signals intelligence in accordance with the tasking directives provided by the Government, the Swedish Armed Forces and other commissioning entities (Section 1). The National Defence Radio Establishment was, if necessary in order to conduct signals intelligence in the long term, also to survey changes in the signal environment, follow the development of communication services and encryption methods, continuously develop the technology and methods needed for conducting signals intelligence and conduct mathematical assessments of encryption systems for the total defence (Section 2).

45. In this context, it is also relevant to mention that Chapter 6, Section 17, point 3 of the Electronic Communications Act states that it is permitted to use a radio receiver to intercept or in some other way gain access to a radio-communicated electronic message that is not intended for the interceptor or the general public. In Sweden, it has generally been considered that the interception of radio frequency transmissions over the air is permissible. The fundamental premise is that "the airwaves are free" and that anyone can, in principle, listen to radio messages using a suitable receiver (cf. para. 25). This stance has also formed the basis of Swedish legislation and has found its expression in the abovementioned provision.

46. The processing of personal data was regulated until June 2007 in the Personal Data Act (1998:204), the Personal Data Ordinance (1998:1191) and the Ordinance on certain processing of personal data within the Swedish Armed

Forces and the National Defence Radio Establishment (2001:703). From 1 June 2007, the processing of personal data by the National Defence Radio Establishment has been regulated in the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment (2007:259) and the associated ordinances.

47. The National Defence Radio Establishment is permitted to process personal data in its foreign intelligence activities if this is necessary for conducting foreign intelligence as stated in the Foreign Intelligence Act. Information about a person may only be processed if the person is related to the detailed tasking directives of foreign intelligence and the processing is necessary to fulfil those objectives (cf. paras. 53-54).

(2) Supervision and legal remedies

48. The mechanisms in place for protecting the privacy of individuals consisted, during this period, mainly of general control functions that primarily worked independently and supervised that no other data was being processed than that which was relevant to foreign intelligence, and that data was not retained for longer than necessary.

49. The task of monitoring the intelligence services within the Swedish Armed Forces and the other agencies conducting foreign intelligence work – i.e. the National Defence Radio Establishment, the Swedish Defence Materiel Administration and the Swedish Defence Research Agency – was the responsibility of the Swedish Intelligence Commission *(Försvarets underrättelsenämnd)* during this period. This was stated in Section 1 of the Ordinance containing instructions for the Swedish Intelligence Commission (2007:852). The Swedish Intelligence Commission was established on 1 July 1976. The purpose of the Commission was to be the Government's insight and control function with the task of continuously monitoring the foreign intelligence services and submitting proposals generated by its scrutiny.

50. In particular, the Commission was to:
– monitor compliance with the Foreign Intelligence Act and the Foreign Intelligence Ordinance;
– supervise that foreign intelligence was conducted in accordance with the specified objectives;
– pay attention to the units within the Swedish Armed Forces and the National Defence Radio Establishment that collected intelligence using special methods;
– scrutinise the means and methods used for collecting intelligence;
– supervise how the registers needed for foreign intelligence were set up and

maintained; and
– review the principles for the recruitment and training of staff (Section 2).

51. The Swedish Intelligence Commission was to present the Swedish Armed Forces and the other agencies conducting foreign intelligence with the views and proposals for measures generated by its inspection activities. If necessary, the Commission was also to submit proposals for measures to the Government. The Swedish Intelligence Commission was to present, no later than 1 March each year, a report to the Government on the previous year's inspection activities (Section 3).

52. The Swedish Intelligence Commission was made up of six members, including a chair, all of whom were appointed by the Government for a set period. The Commission had a secretary. The Commission convened at least four times a year following a summons by the chair (Section 8). The Commission was entitled to obtain from other agencies the information and assistance required for its activities (Section 11).

53. In this context it should also be mentioned that the National Defence Radio Establishment is obliged, once per calendar year, to provide information free of charge to every individual who applies, about whether or not personal data concerning the applicant is being processed. If such data is being processed, written information must also be provided about what data is being processed concerning the applicant, where this data has been collected, the purposes of processing the data and which recipients or categories of recipients the data has been disclosed to. This does not apply if secrecy prevents the information being disclosed to the person whose personal data has been recorded (cf. paras 46-47).

54. Pursuant to the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment, the Establishment is also obliged, at the request of the person whose data has been recorded, to correct, block or delete at the earliest opportunity such personal data that has not been processed in accordance with the legislation or regulations issued (Chapter 2, Section 4). A decision by the National Defence Radio Establishment on disclosure of information or rectification can be appealed to an ordinary administrative court (Chapter 6, Section 3). A decision by the National Defence Radio Establishment not to disclose a public document, with reference to domestic legislation on secrecy, can also be appealed to the Administrative Court of Appeal in Stockholm (*Kammarrätten i Stockholm)*.

From 1 January 2009 to the entry into force of the amended Signals Intelligence Act on 1 December 2009 (Second period)

(1) General provisions on signals intelligence

55. The increasingly complex threat scenario, technical developments and Sweden's growing involvement in international peace support operations made certain adaptations of the regulatory framework for foreign intelligence necessary (cf. paras. 7-9, 17 and 35). Amendments were thus, from 1 January 2009, introduced concerning the legal regulation of working methods and society's control. A certain adaptation of the mandate for foreign intelligence was also made. The Foreign Intelligence Act was amended and the Signals Intelligence Act was introduced. Further, a special permit procedure was introduced and a new court-like permit authority was established concerning signals intelligence in foreign intelligence – the Signals Intelligence Board *(Signalspaningsnämnden)*.

56. To cover the full complexity of the spectrum of threats, with significant elements of non-military and non-armed threats, foreign intelligence was defined as being able to identify *external threats to the country*, irrespective of their nature or origin (Section 1 of the Foreign Intelligence Act). This included, as previously, military threats to the country, but also other threats such as terrorism and the proliferation of weapons of mass destruction. The hallmark of these latter types of risks and threats is, as stated above, that they more often than not originate from non-state actors and are of a transnational and non-military nature. The threat scenario is often complex and concerns several sectors of society. However, the threat must be so extensive that it is considered to threaten the country's security or structures that are vital to the functioning of society.

57. As stated in para. 32, foreign intelligence has always targeted foreign circumstances. The legislator now found it appropriate to clarify the law on this point. Accordingly, foreign intelligence was expressly limited to foreign circumstances only (Section 1 of the Foreign Intelligence Act). Foreign intelligence was intended to collect, process and report information on foreign phenomena and circumstances in order to provide Swedish decision-makers with better material for decisions and assessments in foreign, security and defence policy issues or to protect Swedish personnel participating in international peace support operations.

58. The new Signals Intelligence Act entered into force on 1 January 2009. The Act covers signals intelligence for foreign intelligence purposes, irrespective of how the signals are transmitted. However, as mentioned above (para. 35), collection from cables was not possible until after 1 December 2009, i.e. from

the third period, when the regulation concerning the obligation on the part of the cable owners to make traffic available entered into force. According to the new Act, signals intelligence is to be conducted in accordance with the tasking directives decided by the Government or by agencies designated by the Government (Section 1).

59. Under the Act, the Government can decide tasking directives that may also refer to purposes that are not included in foreign intelligence, but that are a prerequisite for being able to conduct foreign intelligence in the long term. Signals may thus be collected to survey changes in the signal environment, follow the development of communication services and encryption methods. Signals intelligence may also be collected to continuously develop the technology and methods needed to conduct foreign intelligence in accordance with the Act (Section 1). A corresponding right was previously contained in the Ordinance containing instructions for the National Defence Radio Establishment (cf. para. 44).

60. The tasking directives of signals intelligence may not refer to a certain natural person only. Signals intelligence does indeed have to concern individuals' communications in certain cases so as to make it possible to monitor a certain phenomenon that is relevant to the objectives of signals intelligence work. However, it must not target a specific individual only. Before a decision on the tasking directives of signals intelligence, the Government must consult the Signals Intelligence Board (cf. Sections 4 and 6 of the Signals Intelligence Act and Section 1 of the Ordinance with Instructions for the Signals Intelligence Board [2008:924]).

61. A permit is required for the agencies designated by the Government in order to decide on the detailed tasking directives of signals intelligence. However, the permit requirement did not apply during this period to the Government's or the Government Offices' tasking. The Signals Intelligence Board was established as a new agency responsible for issuing permits. The organisation and operations of the Board were regulated in the Signals Intelligence Act and the Ordinance with Instructions for the Signals Intelligence Board. The members were appointed by the Government for a fixed period of at least four years. The chair and vice chair were to be, or have been, permanent judges. The other members were appointed from a list of persons proposed by the party groups in the Riksdag.

62. A permit is valid for a maximum of six months and may be extended for a maximum of six months at a time after renewed examination. The scope of the

renewed examination must be adapted to what the permit covers, the results so far of the collection of signals and any new circumstances of relevance to the examination. Moreover, the tasking directives have to concern a phenomenon or circumstance that is relevant with regard to the purposes for which the signals intelligence is conducted. Furthermore, the tasking directives must also in other respects be compatible with the Foreign Intelligence Act. A permit may only be issued if the purpose of the aim clearly outweighs the infringement upon personal privacy that the intelligence collection – in line with the tasking directives – could cause, and if this purpose cannot be fulfilled in a less intrusive manner. Consequently, the permit authority is to conduct a proportionality assessment based on the information provided by the applicant agency. As has been mentioned, permits may not be issued for tasking directives that refer to a natural person only. This must be examined in connection with the issue of the permit (Section 5).

63. As mentioned above, however, signals intelligence may concern individuals' communications if necessary for monitoring a certain phenomenon that is relevant to foreign intelligence work. If the agency determining the tasking directives can provide selectors that are intended for use initially, these must also be included in the consideration of the permit application. The examination of such selectors must cover whether they have been formulated and are used in such a way as to limit as far as possible any intrusion into personal privacy, and must entail that they are not directly attributable to a certain natural person, unless this is of exceptional importance for the objectives of foreign intelligence.

64. The obligation to obtain a permit does not apply to urgent cases. This means situations in which waiting for a permit would result in serious consequences for essential national interests. If detailed tasking directives have been determined without a permit, this must be reported immediately to the Signals Intelligence Board, which will examine the permit issue. If the permit authority finds that there are no grounds for a permit, the National Defence Radio Establishment is to be informed and the collection of signals must cease immediately (Section 5). The Signals Intelligence Control Delegation can at the same time decide that the collected signals are to be destroyed (Section 10) (cf. para. 69).

65. Recordings or notes of data collected in accordance with the law are to be destroyed immediately if the content of the recordings or notes concerns a certain natural person and it is considered that it lacks importance for foreign intelligence requirements. Of course, this applies regardless of whether signals have been collected with the help of automated processing or with manual

methods. One example of recordings or notes that typically lack importance are those concerning communication that falls entirely outside the framework of the purpose of foreign intelligence, e.g. because they concern domestic circumstances. The requirement to destroy recordings or notes also applies to recordings or notes that include information that is subject to the duty of confidentiality under Chapter 3, Article 3 of the Freedom of the Press Act or Chapter 2, Article 3 of the Fundamental Law on Freedom of Expression, or that is covered by the enquiry prohibition in Chapter 3, Article 4 of the Freedom of the Press Act or Chapter 2, Article 4 of the Fundamental Law on Freedom of Expression. The recordings or notes of information in messages referred to in Chapter 27, Section 22 of the Swedish Code of Judicial Procedure, i.e. between a suspect and his or her defence counsel, must also be destroyed. The obligation to destroy recordings or notes applies to all copies of the recordings or notes in question. There is besides this a prohibition against the reporting of superfluous information concerning individuals and that lacks relevance from a foreign intelligence perspective.

(2) Supervision and legal remedies

66. The fact that the signals intelligence mandate was to be broadened to include the collection of cable-borne signals did not mean that the applicable regulations for the control of signals intelligence were fundamentally changed. The Swedish Intelligence Commission was entrusted with the task of reviewing the broadened signals intelligence mandate. Selectors, destruction and reporting were to be examined in particular. The members of the Commission were appointed by the Government for a fixed period of at least four years. However, a requirement was introduced stipulating that the chair and vice chair must be, or have been, a permanent judge. It was also made clear that the other members would be appointed from a list of persons proposed by the party groups in the Riksdag.

67. A significant part of the control function was to ensure traceability, i.e. that the collection of signals could be linked to a specific tasking directive and that no intelligence was processed without there being a tasking directive. The control function also covered, in particular, signals intelligence that could more obviously affect the privacy interests of individuals.

68. The scrutiny also included the selectors used by the National Defence Radio Establishment in its collection systems, in accordance with detailed instructions. As part of this control activity, the National Defence Radio Establishment was to continuously report the selectors used to the Swedish

Intelligence Commission. This procedure did not restrict the Commission's possibilities of conducting its controls in other ways it found appropriate, e.g. by examining the use of selectors on visits to the National Defence Radio Establishment. In its examination of selectors, the Commission was to supervise in particular that they were compatible with the purposes stated in the Signals Intelligence Act and that they had been formulated in a way that did not entail improper interference of individuals' personal privacy. The Swedish Intelligence Commission was also to supervise that data was destroyed to the extent required by law and that the reporting was compatible with the purposes of foreign intelligence as formulated in the Foreign Intelligence Act and the Signals Intelligence Act. These controls ensured that, throughout the intelligence process, continuous assessments were carried out concerning the relevance of the data and that the measures prescribed by law concerning the destruction of data and reporting of intelligence were conducted correctly. The feedback that the Commission was to provide with regard to its review was regulated in the Commission's instructions.

69. A special decision-making body at the Swedish Intelligence Commission was given the right to order certain types of measures to be taken if, during supervision of the National Defence Radio Establishment, it emerged that signals intelligence was not being conducted in line with the legislation or that it was otherwise violating individuals' rights in a way that was not in reasonable proportion to the purpose of the measures. The decision-making body was called the Signals Intelligence Control Delegation *(Signalspaningskontrolldelegationen)* and had a court-like composition, with a chair and vice chair who were or had been permanent judges, and other members appointed from a list of people proposed by the party groups in the Riksdag. The measures that the Delegation was authorised to order included that a specific ongoing collection process should be discontinued and that the recording or noting of data already collected should be destroyed. The Delegation was authorised to determine the scope of the measure in each individual case. A decision to discontinue signals collection could refer to everything from a prohibition of subjecting a certain phenomenon to monitoring in any way, to using certain selectors.

70. Decisions by the Swedish Intelligence Commission could be brought about in connection with ongoing supervisions on the Commission's own initiative or following special inspection measures in response to information provided, for example, by the privacy protection council established at the National Defence Radio Establishment (cf. para. 71). The Swedish Intelligence Commission was of course free to act on the basis of information irrespective of its source, which

could also include tip-offs from individuals. For the Swedish Intelligence Commission to be able to properly examine permit applications and conduct effective monitoring, it was reinforced with additional legal competence and extended office support. Rules concerning supervision, organisation and processing were also prescribed in more detail in the Commission's instructions. The Commission was given the right to access the information and to receive the assistance it needed for its activities from the agencies reviewed.

71. Beyond the control function for which the Swedish Intelligence Commission was responsible, a system was also created to ensure internal insight into, and follow-up of, the routines at the National Defence Radio Establishment that were intended to safeguard privacy protection. For this reason, a Privacy Protection Council *(integritetsskyddsråd)* was established at the National Defence Radio Establishment which had, and still has, a special responsibility within the context of the Establishment's work to prevent signals intelligence – irrespective of the directives – from being conducted in a way that is not compatible with the legislation. Its main task is to monitor how the Establishment's work is governed through internal regulations and routines. In doing so, the Council is to draw conclusions about whether the signals intelligence is compatible with the legislation and to inform the Establishment's management of the resulting observations. The responsibility for activities at the National Defence Radio Establishment lies with the management. Therefore, the Council does not have any decision-making function; instead, it fulfils its task by reporting its observations to the management of the National Defence Radio Establishment and, if the Council finds reason to do so, to the Swedish Intelligence Commission. The Commission, through the Signals Intelligence Control Delegation is, as stated above, authorized to order that the collecting of certain signals must be stopped or that material already collected must be destroyed. As previously mentioned, the Council still exists and its members are appointed by the Government for a certain period.

From the entry into force of the amended Signals Intelligence Act on 1 December 2009 and onwards (Third period)

(1) General provisions on signals intelligence

72. The introduction of the Signals Intelligence Act attracted a great deal of interest in the Riksdag, the media and public debate. In connection with its decision, the Riksdag announced that the Act would be furnished with additional legal security and control mechanisms. In September 2008, a political agreement was reached between the government parties on certain amendments to the Signals Intelligence Act. These amendments entered into force on 1 December

2009. At the same time, the Foreign Intelligence Court was established, replacing the Signals Intelligence Board. The Swedish Intelligence Commission was replaced by the Swedish Foreign Intelligence Inspectorate *(Statens inspektion för försvarsunderrättelseverksamheten)*.

73. According to the amended Act, permits for signals intelligence are issued by the new court – the Foreign Intelligence Court – upon application by the National Defence Radio Establishment. The rights of individuals have been strengthened, as an individual must be informed if, during signals intelligence, selectors have been used that directly pertain to him or her, unless secrecy applies to the information. Further, individuals have the right to report to the Swedish Foreign Intelligence Inspectorate if they consider they have been the subject of unlawful signals intelligence. The control agency is then obliged to investigate this (cf. para. 91).

74. Section 1 of the amended Signals Intelligence Act provides eight detailed purposes for which signals intelligence may be conducted within foreign intelligence: 1. external military threats to the country; 2. conditions for Swedish participation in international peace support and humanitarian operations, or threats to the safety of Swedish interests in the performance of such operations; 3. strategic circumstances concerning international terrorism and other serious international crime that may threaten essential national interests; 4. development of the proliferation of weapons of mass destruction, military equipment and products referred to in the Act on Control over Dual-use Products and over Technical Assistance (2000:1064); 5. serious external threats to society's infrastructure; 6. conflicts abroad with consequences for international security; 7. foreign intelligence operations against Swedish interests; or 8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy.

75. As stated above, the National Defence Radio Establishment's mandate to conduct signals intelligence was broadened as from the third period, to the extent that electronic signals may also be collected from international electronic communications cables that cross the Swedish border. Such signals may only be collected from cables owned by an operator and crossing the Swedish border (Section 2 of the Signals Intelligence Act). The operator refers to the person or entity that in some way or another has control over a public communication network or associated installation. For network configuration reasons, domestic traffic (signals between a sender and a recipient who are both located in Sweden) could also cross the national border. As it is not possible to fully separate such traffic automatically, the prohibition is supplemented with an obligation to

destroy recordings or notes of domestic traffic as soon as it is clear that it has such origins (Section 2a).

76. Cable collection must be done automatically. When signals are collected automatically, via cable or wireless, they must have been identified by selectors. Selectors are applied to specify one or more terms to search through a mass of information and find the items or constellations of data which a term matches. A selector may also contain parameters that exclude large volumes of information. Selectors are to be formulated and used in such a way that they involve as little infringement as possible upon people's personal privacy. Selectors may not be directly attributable to a specific natural person unless this is of utmost importance to the foreign intelligence objectives. To ensure that signals intelligence only targets relevant communications, access to signals via cable may only be given to the signal carriers covered by the permit (cf. paras. 78 and 80).

77. Only the Government, the Government Offices and the Swedish Armed Forces are permitted to decide the detailed tasking directives of signals intelligence (Section 4). Any signals intelligence conducted by the National Defence Radio Establishment requires a permit from the Foreign Intelligence Court. The permit process applies irrespective of the underlying intelligence requirements; there are no exceptions to this precondition. The Signals Intelligence Act states what an application must contain. The intelligence collection assignment forms the basis for the permit examination parameters. The design of an intelligence collection assignment varies depending on the intelligence requirements the assignment is intended to meet. The description must be sufficiently well defined to enable the court to carry out the examination. The collection assignment must also be related to the tasking directives that form the basis of the application (Section 4a).

78. The application must contain information about all of the signal carriers concerning signals via cables to which the National Defence Radio Establishment needs access within the scope of the relevant collection assignment. Signal carriers refer to the medium used for transmitting one or more signals. Regarding optical signals, the signal carrier is the same as an individual fibre. The signal carriers must be described in a way that can form the direct basis of enforcement. At the same time, adequate information about the signal carriers must be provided to make it possible to assess the extent of the interference of privacy that access to the carriers may entail. Information must be provided about the selectors or categories of selectors that will be used. The selectors should normally be given in categories enabling a proportionality assessment at an aggregated level, e.g. selectors that directly pertain to military

officials in a certain country. In some cases, a more detailed description of the selectors is required. Ultimately, it is up to the court to determine the level on which selectors must be described.

79. The National Defence Radio Establishment is to state the time needed to fulfil the intelligence collection assignment and any other circumstances being cited in support of the application. These may include previous collection assignments concerning the same phenomenon and their results, with the aim of clarifying the requirements for the new assignment. They may also include measures that the Establishment intends to take to limit interferences of privacy in connection with the signals collection.

80. The Foreign Intelligence Court is to examine whether the intelligence requirements referred to in the collection assignment correspond with the purposes permitted, as stated in the Foreign Intelligence Act and clarified in more detail in the Signals Intelligence Act. In addition, the examination is to ensure that the collection assignment is not in any way incompatible with the legislation. This includes controlling that tasking directives form the basis of the application. A permit is to state, among other things, the collection assignment for which signals intelligence is permitted, which signal carriers and selectors may be used, and which other conditions are needed to limit interferences of personal privacy.

81. A proportionality assessment is to be carried out, in which the value of the information expected from a collection assignment is to be placed in relation to the interference of privacy that it may entail. When assessing interference of privacy, the Court is to proceed from what is stated in the application about access to signal carriers and the use of selectors. The permit examination includes an assessment of whether the desired results of the collection may be achieved in a less intrusive way. Therefore, the National Defence Radio Establishment must describe the prospects of obtaining the information by targeting other sources. In many cases – particularly when the underlying intelligence requirements have been proposed by another Swedish intelligence agency with its own intelligence capacity – the point of departure should be that this agency has exhausted the practical possibilities of obtaining this information in another way (Section 5).

82. Beyond the fact that the selectors are a factor to be considered in the proportionality assessment, they must also be examined in relation to the relevant requirements contained in the legislation. As a rule, the examination should be based on the categories of selectors, but it may also focus on individual selectors if the Court finds this necessary.

83. As has been mentioned, a collection assignment may not focus on one natural person only. In such cases, a permit may not be issued by the Court. The Court may also issue other conditions that are needed to limit the interference of individuals' personal privacy. Which conditions are relevant depends on what the collection assignment refers to.

84. The organisation and activities of the Foreign Intelligence Court are regulated in the Foreign Intelligence Court Act (2009:966) and the Signals Intelligence Act. The Court consists of a chair, one or at most two vice chairs and a minimum of two and maximum of six special members. The chair is appointed permanent judge by the Government following proposals by the Judges Proposals Board *(Domarnämnden)*. The vice chair and the special members are appointed by the Government for a four-year term. The chair and the vice chairs must be legally trained with experience of service as a judge. The special members are to meet the needs of the Court in terms of competence concerning intelligence work and privacy protection, among other areas. The Court has a secretariat with a head of administration and administrative staff. The Court comes under the supervision of the Parliamentary Ombudsmen, the Office of the Chancellor of Justice and the Data Inspection Board *(Datainspektionen)*. The Court's decision may not be appealed (Section 16 of the Foreign Intelligence Court Act and Section 13 of the Signals Intelligence Act).

85. During the examination of applications for signals intelligence permits, a privacy protection representative must be present to look after the privacy interests of individuals. The privacy protection representative does not represent any specific person, but individuals' interests in general in the proportionality assessment. The privacy protection representative is permitted to read all material associated with the case. The privacy protection representatives are appointed by the Government for a period of four years, following proposals by the Swedish Bar Association *(Sveriges advokatsamfund)* and the Judges Proposals Board. During this four-year period, additional persons may be appointed for the remaining time if necessary. A privacy protection representative must be, or have been, a lawyer or a permanent judge. In each individual case, the privacy protection representative is appointed by the Court. The duty of confidentiality applies for the privacy protection representative. In the course of his or her duties, the privacy protection representative regularly has access to extremely sensitive material (Sections 5–8 of the Foreign Intelligence Court Act).

86. Applications for permits are discussed during a hearing. The National Defence Radio Establishment and the privacy protection representative are to be summoned to the meeting. The Court may also summon another person who

can provide information that is relevant to the examination. This may mean, for example, that a representative of the agency whose objectives form the basis of the application should be given the opportunity to shed light on the intelligence requirements. In rare cases, a matter may be so urgent that there is no time to contact and summon a privacy protection representative without risking that the purpose of the measure is missed. For this reason, the Court may hold a meeting and take a decision in the matter without a privacy protection representative having been present or given the opportunity to give his or her opinion if the delay would seriously jeopardise the purpose of the decision. Regarding the secrecy protection for the information processed, it is generally not possible to allow the privacy protection representative to access the information and present his or her views in another way before the decision is taken if he or she is not able to get to the meeting. However, if a decision has been taken without a privacy protection representative expressing his or her opinion, the representative must be allowed access to the information afterwards (Sections 11–12). In cases where the privacy protection representative calls attention to irregularities, a natural consequence of his or her remit is to report this to the Parliamentary Ombudsmen or the Chancellor of Justice.

87. If it is clear from the application or other information from the National Defence Radio Establishment that making the hearing open to the public would result in information that is classified as secret being exposed, the chair of the Court may decide before the hearing begins that it must take place behind closed doors. Such a decision may be taken as soon as the conditions so require once the case has been initiated and up until the start of the hearing (Section 14).

(2) Supervision and legal remedies

88. As was mentioned above, the Swedish Intelligence Commission was replaced by the Swedish Foreign Intelligence Inspectorate as from 1 December 2009. The Inspectorate is a committee agency under the Government with the task of supervising that the foreign intelligence work conducted by the Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Defence Research Agency and the Swedish Defence Materiel Administration is in accordance with primary and secondary legislation (acts and ordinances). The committee of the Swedish Foreign Intelligence Inspectorate can have a maximum of seven members. The chair and the vice chairs must be legally trained with experience of service as a judge. The other members are nominated by the party groups in the Riksdag. The organisation and activities of the committee are regulated in the Foreign Intelligence Act, the Signals Intelligence

Act and the associated ordinances, and the Ordinance containing instructions for the Swedish Foreign Intelligence Inspectorate (2009:969).

89. The Swedish Foreign Intelligence Inspectorate is also responsible for controlling signals intelligence. The Inspectorate is to monitor, in particular, selectors, destruction of data and reporting. Furthermore, the Swedish Foreign Intelligence Inspectorate is to check at the request of an individual whether his or her communication has been collected in connection with signals intelligence. The Inspectorate also exercises a right of disposition over the signals that electronic communications cable owners are to submit to collaboration points under Chapter 6, Section 19a of the Electronic Communications Act. This right of disposition means that the National Defence Radio Establishment may only have access to the signal carriers for which there is a permit under the Signals Intelligence Act. The Inspectorate does not make any decisions of its own concerning the permit issued by the Court; it simply enforces it. Having said that, the Inspectorate is of course to ensure that the Court's decisions are followed.

90. The Swedish Foreign Intelligence Inspectorate is also to supervise the processing of data under the Act on processing personal data in the foreign intelligence and development operations of the National Defence Radio Establishment.

91. As stated above (para. 89), The Swedish Foreign Intelligence Inspectorate is to check at the request of an individual whether his or her communication has been the subject of signals intelligence. These checks must be carried out on the basis of information provided by the individual. Businesses and organisations may also request that checks be made. Following the check, the person who requested the investigation must be informed whether or not any improper signals collection has taken place. If the Swedish Foreign Intelligence Inspectorate finds evidence of improper signals collection, this must be reported to the individual as well as to the agencies responsible for the matter at hand, e.g. the Data Inspection Board, the Office of the Chancellor of Justice or the Office of the Prosecutor-General (*Riksåklagaren)* at the Swedish Prosecution Authority (*Åklagarmyndigheten)*. A request to perform checks must be made in writing and signed by the person whose communication it concerns.

92. Data that is of a superfluous nature is covered by the obligation to destroy data. Protection of individual privacy is thus safeguarded through the obligation to destroy data and supervision of compliance with this obligation.

93. The National Defence Radio Establishment is required to notify individuals about whether selectors have been used in signals intelligence that directly pertain to a certain natural person. It is only possible to provide notification to persons identified in advance as relevant to foreign intelligence. The contents of a notification must state when the signals collection referred to took place and its purpose.

94. Notification must be given as soon as possible without detriment to the objectives of foreign intelligence, but no later than one month after the end of the intelligence collection assignment. In some cases, an intelligence collection assignment ends when the permit for the remit expires without being extended. If processing and analysis continue after this time, however, the time at which the assignment ends is the time at which the last report associated with the assignment is submitted. However, notification to an individual is to be postponed during the period in which secrecy applies to the information. The National Defence Radio Establishment is to continuously examine whether secrecy still applies to the data or whether notification can be sent. The matter must also be examined if new circumstances arise, giving cause to review the secrecy issue. If one year has passed since the end of the intelligence collection assignment and it has not been possible to provide notification, there is no need to do so.

95. There is also an exception from the obligation to provide notification in matters concerning signals intelligence that exclusively refers to the circumstances of a foreign power or circumstances between foreign powers. This exception applies to information concerning, for example, a foreign state's military circumstances or political power structure, but not circumstances regarding individual aliens without there being a connection to any action on behalf of a foreign power. It is not considered that there is any noteworthy privacy protection interest in matters concerning such signals intelligence.

96. In connection with the legislative amendments of 1 December 2009, amendments were also introduced to the Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment (2007:261) to strengthen privacy protection. The amendments meant that personal data in the form of unprocessed raw material *must* be deleted no later than one year after the processing of the data began (Section 2). Previously, the time limit was three years, with the possibility of extension in certain circumstances. Moreover, the amendments specified that the deletion of this personal data is final (Section 12).

Other safeguards

97. This section of the present observations is limited to safeguards other than the control mechanisms, supervisory elements and remedies that are available in the context of signals intelligence. Unless stated explicitly, these safeguards have essentially been the same over the three time periods.

The Parliamentary Ombudsmen

98. It follows from Chapter 13, Article 6 of the Instrument of Government that the Riksdag elects one or more Parliamentary Ombudsmen who shall supervise the application of laws and other regulations in public activities. Courts of law and administrative authorities, as well as central or local government employees, are obliged to provide information and opinions at the request of an Ombudsman. The Ombudsmen are elected for a four-year period and may only be removed from office by the Riksdag (Chapter 8, Article 11 of the Riksdag Act).

99. The remit of the Parliamentary Ombudsmen includes ensuring in particular that in the course of their activities courts of law and administrative authorities observe the provisions of the Instrument of Government concerning objectivity and impartiality and that citizens' fundamental rights and freedoms are not encroached upon in public activities (Section 3 of the Act with Instructions for the Parliamentary Ombudsmen [1986:765]). The National Defence Radio Establishment and the Foreign Intelligence Court as well as their respective activities come under the supervision of the Ombudsmen. The supervision is conducted by means of examining complaints from the public and through inspections and other investigations. The examination of a matter is concluded by a decision in which the Ombudsman states his or her opinion on whether the measure of the authority contravenes the law or is otherwise wrongful or inappropriate. The Ombudsmen are entitled to have access to the minutes and other documents of the courts and the administrative authorities.

100. In the role of special prosecutor, an Ombudsman may initiate legal proceedings against an official who, in disregarding the obligations of his or her office, has committed a criminal offence. An Ombudsman also has the right to report that an official should be removed from his or her office because of a criminal act or repeated neglect of duty.

The Chancellor of Justice

101. Like the Parliamentary Ombudsmen, the Chancellor of Justice supervises those involved in public administration to ensure that they comply with laws and

other statutes and otherwise fulfil their obligations (the Act concerning the supervision exercised by the Chancellor of Justice [1975:1339]). Government agencies and government employees, contractors and others associated with the authorities are subject to the supervision of the Chancellor of Justice. The National Defence Radio Establishment and the Foreign Intelligence Court as well as their respective activities thus come under the supervision of the Chancellor of Justice. The supervision is conducted by means of examining complaints from the public and through inspections and other investigations. Courts of law and administrative authorities as well as their officials are obliged to provide information if requested by the Chancellor of Justice. The Chancellor of Justice is entitled to have access to minutes and other documents of the courts and administrative authorities (Section 9 of the Act concerning the supervision exercised by the Chancellor of Justice).

102. The Chancellor of Justice is also authorised to receive complaints and claims for damages directed towards the State. In addition, the Chancellor of Justice is entitled to decide that the State is to pay compensation for damage in such cases. This is elaborated on further below, see paras. 117-118. It may also be mentioned that the Chancellor of Justice has the same powers as the Parliamentary Ombudsmen in the role of special prosecutor (cf. para 100).

The Data Inspection Board

103. The Data Inspection Board is to act to protect individuals against violation of their personal privacy through processing of personal data. The Board is the supervisory authority under the provisions of the Personal Data Act and also supervises other statutes that govern the processing of personal data, including the Act on processing personal data in the foreign intelligence and development operations of the National Defence Radio Establishment. As part of its supervisory tasks, the Data Inspection Board may examine complaints by natural or legal persons. The Board is entitled for the purposes of its supervision to obtain access to personal data processed, as well as information about and documentation of this processing (Section 43 of the Personal Data Act). If the supervisory inspection shows that the data is processed or may be processed in an unlawful manner the Board shall, primarily by means of observations or in other ways, endeavour to obtain rectification. The Board can also bring legal action in a court of law to erase data processed in an unlawful manner.

Damages

104. In this context it is also relevant to reiterate that there are general provisions in Swedish law that regulate the liability for damages of public

institutions towards individuals. For damage caused through deficiencies in the exercise of public authority, the general liability for damages under the Tort Liability Act (1972:207) covers liability for costs for personal injury, material damage and pure financial loss. In some cases, compensation for non-material damage can also be paid. This assumes, however, that a criminal act entailing serious violation of the individual's integrity is involved.

105. The liability for damages of the public institution that follows directly from the Tort Liability Act is limited to cases of unlawful actions. In other words it is assumed that there are "errors and omissions" on the part of the public institutions. Moreover, it is also required that the error is made "in the exercise of public authority", i.e. through or in close connection with measures on the part of a public institution that have legal effects for individuals and that give expression to the right of society to exercise authority over citizens. However, an action for damages cannot normally be brought concerning decisions made by the Riksdag, the Government or the highest courts.

106. Both natural and legal persons can bring a court action for damages and thus have their case heard. Chapter 3, Section 1 of the Tort Liability Act states that those who have employees in their service must pay for the costs of personal injury or material damage that the employee causes through errors or omissions in their duties, as well as pure financial loss that the employee causes in the course of their duties by committing a crime. Chapter 3, Section 2 of the Tort Liability Act contains provisions on the responsibility of public institutions in the event of the incorrect exercise of public authority. The central or local government is obliged to compensate an individual for personal injury, material damage or pure financial loss that the individual has suffered through errors or omissions in the exercise of public authority, for which the central or local government is responsible. Public institutions are also obliged to compensate an individual for a serious violation of their integrity through an offence involving an attack against his or her person, freedom, peace or honour if the offence involves errors or omissions in the exercise of public authority (Chapter 2, Section 3 of the Tort Liability Act). An individual thus has a right to compensation for the violation that he or she has suffered as a result of the exercise of public authority involving an illegal breach of postal or telecommunication secrecy or intrusion into a safe depository or unlawful interception. It is not necessary for someone to be convicted of the offence. It is sufficient that the act justifying the claim for damages constitutes an offence from an objective point of view.

107. An individual public official who, in the exercise of public authority, intentionally or through negligence, has disregarded the rules that apply to his or her duties is to be convicted of misconduct if the act is not insignificant. However, if the act is punishable under another provision, this provision is to be applied (Chapter 20, Section 1 of the Swedish Penal Code). This means that acts such as interception occurring with intent and without the support of the law are punishable under the penal provision on the breach of telecommunication secrecy (Chapter 4, Section 8 of the Swedish Penal Code).

108. A person who causes pure financial loss through an offence must pay compensation for the damage (Chapter 2, Section 2 of the Tort Liability Act). For damages that an employee causes through errors or omissions in his or her duties, he or she is only personally liable to the extent that there are exceptional grounds with regard to the nature of the act, the position of the employee, the interest of the injured party and other circumstances (Chapter 4, Section 1 of the Tort Liability Act). The idea is that the injured party is to be able to direct their demands for damages at the employer of the person having caused the damage.

109. There is also a possibility of damages under the provisions on personal data processing that apply to the operations. Under Section 5 of the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment, central government is to compensate the person whose data has been recorded for damages and interference of personal integrity caused by the processing of personal data in contravention of the law or regulations issued pursuant to the law. A corresponding right to damages is contained in Section 48 of the Personal Data Act.

Prosecution

110. Furthermore it should also be mentioned that natural or legal persons who consider themselves subjected to signals intelligence that go beyond the parameters established in the legislation can always report the matter for prosecution and have their case heard. Offences that may be relevant under Chapter 4 of the Swedish Penal Code include breach of postal or telecommunication secrecy (Section 8), intrusion into a safe depository (Section 9), unlawful interception (Section 9a) and data security breach (Section 9c).

Compensation for violations of the Convention

111. Finally, the Government would like to reiterate that Swedish tort law has been developed in case-law as regards compensation for actions involving

violations of fundamental rights and freedoms. Thus, in several cases, the Supreme Court (*Högsta domstolen*) has examined the issue of whether an individual, without direct support in the Tort Liability Act, can claim damages from central and local government in the form of non-pecuniary damages for violations of the European Convention on Human Rights, including violations of Article 8. It follows from established case-law that damages can be awarded without direct support in the Tort Liability Act if necessary to uphold the effective legal remedy requirement under Article 13 of the Convention. In practice, this principle means that a general court can oblige central government to pay both pecuniary and non-pecuniary compensation to an individual if there has been a violation of the Convention. The Chancellor of Justice can also order such damages. The case-law of the Supreme Court and the practice of the Chancellor of Justice are described below.

112. In a judgment of 9 June 2005 (NJA 2005 p. 462) the Supreme Court examined a claim for damages brought by an individual against the Swedish State, *inter alia*, on the basis of an alleged violation of Article 6 of the Convention on account of the excessive length of criminal proceedings. The Supreme Court held that the plaintiff's right under Article 6 to have the criminal charges against him determined within a reasonable time had been violated. Based on this finding – and with reference to Articles 6 and 13 of the Convention and the Court's case-law under these provisions (in particular the case of *Kudla v. Poland* [GC], no. 30210/96, ECHR 2000-XI) – the Supreme Court concluded that the plaintiff was entitled to compensation under Swedish law for both pecuniary and non-pecuniary damage. With respect to the level of compensation for non-pecuniary damage, the Supreme Court took note of the criteria established in the Court's case-law stating that the Court's practice constituted a natural point of departure in this regard.

113. In a decision of 4 May 2007 (NJA 2007 p. 295), the Supreme Court held that the principle concerning a right to damages established in NJA 2005 p. 462 also applied with regard to the rights contained in Article 5 of the Convention. The Supreme Court stated that the plaintiff's right to damages on account of a violation of Article 5 should be assessed in the first place under the Tort Liability Act and the Act on Compensation for Deprivation of Liberty and Other Coercive Measures (1998:714). To the extent necessary, the relevant provisions of domestic law should be interpreted in accordance with the Convention. If Sweden's obligations under Article 5 § 5 could not be met by such an interpretation, the domestic court should award compensation without the support of specific legal provisions. As regards the determination of the level of

compensation, the Supreme Court repeated that the Court's case-law is a natural point of departure. It also noted that account must be taken of the fact that different national conditions may lead to variations from one country to another in what should be regarded as a reasonable level of compensation.

114. In a judgment of 21 September 2007 (NJA 2007 p. 584), the Supreme Court held that the plaintiffs' right to respect for their private life under Article 8 had been violated. The reason was that a police authority's decision on a medical examination of some of them had not been "in accordance with the law". Having found that compensation for the violation could not be awarded immediately on the basis of the Tort Liability Act, the Supreme Court held that there was no reason to limit the scope of application of the principle established in NJA 2005 p. 462 and NJA 2007 p. 295 to violations of Articles 5 and 6. In view of this and with reference to Articles 8 and 13 of the Convention and the Court's case-law under these provisions, the Supreme Court concluded that the plaintiffs should be awarded non-pecuniary damages for the violation of Article 8. Furthermore, the Supreme Court found that the levels of compensation should not be too far removed from the levels that apply when awarding damages under the Tort Liability Act. Generally speaking, these levels should, however, be compatible with the case-law of the Court.

115. A further Supreme Court judgment of 28 November 2007 (NJA 2007 p. 891) concerned a claim for damages against the Swedish State on the basis of an alleged violation of Article 2 of the Convention relating to the plaintiffs' father's suicide while in detention. The Supreme Court concluded that the case revealed no violation of Article 2. However, in its reasoning leading to this conclusion, the Supreme Court noted that according to the Court's case-law there is a right to an effective remedy under Article 13 connected to the state's duty under the Convention to take measures to protect the lives of individuals in custody or who are otherwise deprived of their liberty. This right should, in principle, include a possibility of obtaining compensation for damages. The Supreme Court referred in particular to the judgment in *Keenan v. the United Kingdom* (no. 27229/95, § 130, ECHR 2001-III).

116. In another judgment of 3 December 2009 (NJA 2009 N 70), concerning claims for damages against the Swedish State on account of excessive length of tax proceedings, the Supreme Court once again ruled on a claim regarding compensation for a violation of the Convention. Referring to its case-law from 2007, the Supreme Court held that from that time it is a general principle of law that to the extent that Sweden has a duty to provide redress to victims of Convention violations through a right to compensation for damages, and this

duty cannot be fulfilled even by interpreting national tort law in accordance with the Convention (*fördragskonform tolkning*), compensation for damages may be ordered without direct support in law. Lastly, in a judgment of 16 June 2010 (NJA 2010 p. 363) the Supreme Court ordered compensation for non-pecuniary damage to be paid to an applicant whose damages proceedings against the State in the case previously mentioned (NJA 2009 N 70) had complied with neither the "reasonable time" requirement in Article 6 nor the right to an effective remedy in Article 13.

117. Finally, taking into account the Supreme Court's case-law referred to above and applying the principles established therein, the Chancellor of Justice has awarded compensation for violations of the Convention in several cases. For example, in a decision of 11 October 2007 concerning a claim for damages against the Swedish State, the Chancellor of Justice held that the right of one of the plaintiffs to a trial within a reasonable time under Article 6 had been violated on account of the excessive length of civil proceedings. Based on this finding, and with reference to NJA 2005 p. 462 and NJA 2007 p. 584, the Chancellor of Justice concluded that the individual was entitled to compensation from the State for non-pecuniary damage. With respect to the level of compensation, the Chancellor of Justice took note of the Court's case-law, in particular the case of *Ernestina Zullo v. Italy* ([GC], no. 64897/01, 29 March 2006). Since the autumn of 2007, the Chancellor of Justice has dealt with more than 1000 requests from individuals for compensation on the basis of violations of the Convention. Of those, at least 160 cases have concerned Article 8 of the Convention (see the Chancellor of Justice's comments on the report SOU 2010:87; *Remissyttrande över betänkandet Skadestånd och Europakonventionen*, no. 2250-11-80). If the Chancellor of Justice does not approve a claim for damages, the individual applicant has the option of bringing an action for damages in a court of law in accordance with the case-law described above.

118. With reference to the Supreme Court's case-law, the Chancellor of Justice has also dealt with claims from individuals in cases where the circumstances were similar to those examined by the Court in *Segerstedt-Wiberg and Others v. Sweden* (no. 62332/00, ECHR 2006-VII). In that judgment the Court found that the continued storage of information about four applicants in Swedish Security Service (*Säkerhetspolisen*) files constituted a violation of Articles 8, 10 and 11 of the Convention. Subsequently, about 130 persons applied to the Chancellor of Justice. They held that they had been subjected to the same kind of violation as the applicants in *Segerstedt-Wiberg and Others* and requested that compensation for damages be paid. When examining these claims, the Chancellor of Justice had

access to the case files at the Security Service concerning the applicants who appeared there. In a decision of 23 June 2009, the Chancellor of Justice found that one applicant had been subjected to similar violations as the applicants in the judgment previously mentioned (Articles 8, 10, 11 and 13 of the Convention) and awarded compensation for non-pecuniary damage (no. 7927-07-47). The decision aimed at providing a basis for assessing the remaining cases.

III. <u>On the Admissibility</u>

119. It may be reiterated that the applicant firm complains that Swedish state practice and legislation concerning intelligence work in the form of signals intelligence have violated and continue to violate its rights under Article 8 of the Convention. The applicant firm has not alleged actual interception of its communications. It may therefore be concluded that the applicant firm complains about the signals intelligence regime in itself. Against this background, the Government has been asked to deal in its observations with the following question:

Can the applicant firm claim to be a victim of a violation occasioned by the mere existence of Swedish state practice and legislation concerning secret surveillance measures within the meaning of Article 34 of the Convention? In particular, in each of the three time periods specified by the applicant firm, what remedies concerning secret surveillance measures were/are available to the public at the national level and what was/is the risk of such measures being applied to the applicant (see the recent authority Kennedy v. the United Kingdom*, no. 26839/05, § 124, 18 May 2010)?*

Although the Government finds that there may be reason to question whether the applicant firm has exhausted all domestic remedies available during each of the three time periods concerned, the Government will – in these observations – limit itself to the question put forward by the Court.

Can the applicant firm claim to be a victim of a violation of the Convention?

120. To begin with, the Article 8 rights at issue in the present case appear to be those of the applicant firm, not of its members. Hence, the Government does not contest that the applicant firm could claim to be a victim within the meaning of Article 34 of the Convention because there is not a sufficiently direct link between the firm as such and the alleged breaches of the Convention (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 61, 28 June 2007, and the authorities cited therein).

121. Furthermore, it may be reiterated that the Court has found that the mail and other correspondence of legal persons, which are at issue in the present case, are covered by the notion of "correspondence" which applies equally to communications originating from private and business premises. It therefore seems to be clear that the applicant firm is entitled to the protection afforded by Article 8 as far as it relates to its right to respect for correspondence. However, the Government holds that the Court's case-law does not support the conclusion that a legal person has a private life within the meaning of Article 8 (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, cited above, § 60, and the authorities cited therein). Consequently, the only Article 8 right at issue in the present case is the applicant firm's right to respect for its correspondence.

122. Moreover, the Court has consistently held in its case-law that its task is not normally to review the relevant law and practice *in abstracto,* but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention. However, in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision thereof, the Court has permitted general challenges to the relevant legislative regime (see, *inter alia, Klass and Others v. Germany,* 6 September 1978, § 33, Series A no. 28 and *Kennedy v. the United Kingdom*, no. 26839/05, § 119, 18 May 2010).

123. In assessing whether there has been an interference in cases raising a general complaint about secret surveillance measures, the Court has held that if an individual were to be deprived of the opportunity of lodging an application because, owing to the secrecy of the measures objected to, he cannot point to any concrete measure specifically affecting him, the efficiency for the Convention's enforcement machinery would be materially weakened. The Court has pointed out that where a state institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions. The Court has found it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violations (*Klass and Others,* cited above, §§ 34 and 36).

124. Furthermore, the Court has found that to the extent that a law institutes a system of surveillance under which all persons in the country concerned can potentially have their mail and electronic communications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification, it directly affects all users or potential users of the postal and telecommunication services in that country. The Court has therefore accepted that an individual may, under certain conditions, claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures (see, *inter alia, Klass and Others,* cited above, § 34 and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 58).

125. The principal reason justifying the Court's departure, in cases concerning secret measures, from its general approach which denies the right to challenge a law *in abstracto* is thus to ensure that the secrecy of such measures does not result in the measures being effectively unchallengeable and outside the supervision of the national authorities and the Court. In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court has, in its more recent case-law, clarified that regard must be had to the availability to the public of any remedies at the national level and the risk of secret surveillance measures being applied to him. The Court has pointed out that where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by the Court (*Kennedy,* cited above, § 124).

126. The Government would like to contend that a remedy in this context must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret measures. The measures must be considered as challengeable if there exists domestic machinery whereby, subject to the limitations of the context, compliance with the relevant laws can be secured (cf. *Leander v. Sweden*, 26 March 1987, §§ 78-79, Series A no. 116). In the Government's opinion, the Court's case-law suggests that such remedies are not only those which provide every person with the right to judicial scrutiny. What

seems to be important is that there are sufficient safeguards that secret surveillance powers are not being abused and also that the general public is assured that these powers are not being abused.

127. Furthermore, the Government submits that the remedies in this context do not have to satisfy the requirements of an effective remedy as set out in the Court's case-law on Article 13 of the Convention (cf. *Kennedy,* cited above). It may be reiterated that it is clear from the Court's case-law that Article 13 does not guarantee a remedy allowing a contracting state's laws as such to be challenged before a national authority on the ground of being contrary to the Convention or equivalent domestic norms. In addition, the Court does not require that an effective remedy within the meaning of Article 13 be provided by a judicial authority in the strict sense (see, *inter alia, Segerstedt-Wiberg and Others v. Sweden*, cited above, § 117). The Court has also held that the Convention is to be read as a whole and that the interpretation of the separate articles must be in harmony with the logic of the Convention (see *Kennedy,* cited above, § 197 and *Leander,* cited above, §§ 77 d and 78). In light of this, the Government contends that higher demands cannot be imposed on the remedies to be considered in this context than on remedies within the meaning of Article 13. Hence, the Government concludes that an applicant cannot claim to be a victim as a result of the mere existence of legislation permitting secret measures because the contracting state does not provide a remedy allowing a contracting state's laws to be challenged *in abstracto* or because the remedy is not provided by a judicial authority in the strict sense.

128. Turning to the present case and in response to the Court's question, the Government will elaborate first on the remedies available to the public at national level and then on the risk of secret surveillance measures being applied to the applicant firm.

Remedies available to the public at national level

From the establishment of the applicant firm in 2002 to the entry into force of the Signals Intelligence Act on 1 January 2009 (First period)

129. As is clear from the account of the Court's case-law above, one of the relevant circumstances in deciding whether an applicant can claim to be a victim of a violation occasioned by the mere existence of legislation permitting secret surveillance activities is if the secrecy of such activities results in the activities being effectively unchallengeable and outside the supervision of the national authorities and the Court.

130. As stated above (para. 48) the mechanisms in place during the first period for protecting the privacy of individuals consisted mainly of general control functions that primarily work independently. These independent control functions supervised that no other data was being processed than that which was relevant to foreign intelligence, and that data was not retained for longer than necessary. For example, the task of monitoring the intelligence services within the National Defence Radio Establishment was the responsibility of the Swedish Intelligence Commission (cf. paras. 49-52). Furthermore, any individual had (and still has) the right to apply to the National Defence Radio Establishment for information on whether or not personal data concerning him is being processed. The National Defence Radio Establishment is obliged to provide such information free of charge once per calendar year to every individual who applies, and to correct, block or delete at the earliest opportunity personal data that has not been processed in accordance with the legislation or regulations issued pursuant to the law. A decision by the National Defence Radio Establishment on disclosure of information or rectification can be appealed to an administrative court (see paras. 53-54 above).

131. In addition and as stated above, there are a number of other remedies available to the public, namely the possibility to apply to the Parliamentary Ombudsmen, the Chancellor of Justice or the Data Inspection Board, the possibility to bring an action for damages, the possibility to report a matter for prosecution and the possibility to bring a claim for compensation for violations of the Convention.

132. Both the Parliamentary Ombudsmen and the Chancellor of Justice have the competence to receive individual complaints and they may investigate such complaints in order to ensure that the relevant laws have been properly applied by the relevant authorities (cf. paras. 98-102 above). In their performance of these duties, both officials are entitled to have access to the minutes and other documents of the courts and the administrative authorities. Even if neither of the two officials, apart from their competence to institute criminal and disciplinary proceedings, have the power to render legally binding decisions, it deserves to be stressed that the opinions of the Parliamentary Ombudsmen and the Chancellor of Justice traditionally command great respect in Swedish society and are usually followed in practice (*Leander*, cited above, §§ 81-82 and *Segerstedt-Wiberg and Others*, cited above, § 118).

133. Furthermore, the Government would like to recall the supervisory tasks of the Data Inspection Board in this context (cf. para. 103 above). The Board may examine complaints by natural or legal persons. If an inspection shows that

certain personal data is being processed or may be processed in an unlawful manner, the Board shall endeavour to obtain rectification. In addition, the Board can bring legal action in a court of law to erase data processed in an unlawful manner. Moreover, the Government wishes to recall the possibility to bring a court action for damages and the possibility to report a matter for prosecution (cf. paras. 104-109 above).

134. Finally, the Court's attention is drawn to the case-law of the Supreme Court and the practice of the Chancellor of Justice as regards compensation for violations of the Convention, see paras. 111-118 above. Note should particularly be taken of the judgment of 21 September 2007 referred to in para. 114 above, whereby the Supreme Court awarded individuals compensation for non-pecuniary damage on account of violations of Article 8 of the Convention. In view of this case-law, it must, in the Government's opinion, be concluded that Swedish law provides a remedy in the form of compensation for both pecuniary and non-pecuniary damage in respect of any violation of the Convention, including cases where a violation of Article 8 has occurred.

135. The Government wishes to emphasise that the Supreme Court judgment of 9 June 2005 was pronounced more than three years before the application was lodged with the Court in the present case. Moreover, it deserves to be emphasised that the present case concerns Article 8 and that the first such case was considered by the Supreme Court in September 2007 (NJA 2007 p. 584), almost ten months before the application was lodged with the Court in the present case. Here, it needs to be stressed that the judgment in NJA 2007 p. 584 was made available on the Internet on the day it was delivered, i.e. 21 September 2007. Furthermore, it should be recalled that the Chancellor of Justice has dealt with more than 1000 requests from individuals for compensation on the basis of violations of the Convention since the autumn of 2007. A number of the requests handled by the Chancellor of Justice have concerned Article 8 of the Convention. Accordingly, the legal position on the possibilities under domestic law to obtain compensation for damages on account of violations of Article 8 must be considered to have been sufficiently clear at the time when the present application was introduced before the Court on 14 July 2008. The limitation period in respect of such a claim is ten years from the point in time when the damage occurred (Section 2 of the Limitations Act [1981:130]).

136. It is true that none of the above-mentioned authorities have the power to annul any of the provisions on foreign intelligence or signals intelligence if the provisions themselves were to be considered as incompatible with the Convention, or to discontinue state practice concerning signals intelligence.

However, bearing in mind the great respect that the opinions of the Parliamentary Ombudsmen and the Chancellor of Justice command in Swedish society, if either of these authorities delivered an opinion to the effect that the provisions on foreign intelligence or signals intelligence, or state practice concerning signals intelligence, were incompatible with the Convention, it could result in the provisions being annulled or amended or, in the latter case, that state practice concerning signals intelligence was being discontinued. Furthermore, such scrutiny as can be conducted by the Parliamentary Ombudsmen and the Chancellor of Justice could provide further elucidation of the applicable safeguards and of the general operation of the signals intelligence work conducted by the National Defence Radio Establishment, such as would assist the Court in its consideration of the compliance of these activities with the Convention (see *Kennedy,* cited above, § 110). The same could be said if the Chancellor of Justice or a court of law were to award compensation for damages because the provisions on foreign intelligence or signals intelligence, or state practice concerning signals intelligence, were considered to be incompatible with the Convention, and thus result in a violation of the Convention.

137. The Government contends that the control mechanisms, supervisory elements and remedies described above provided possibilities for the public to challenge the signals intelligence work conducted by the National Defence Radio Establishment during the first period. Hence, the secrecy of such activities did not result in these activities being effectively unchallengeable and outside the supervision of the national authorities and the Court.

From 1 January 2009 to the entry into force of the amended Signals Intelligence Act on 1 December 2009 (Second period)

138. Also during the second period, the Swedish Intelligence Commission was entrusted with the task of monitoring the intelligence services within the National Defence Radio Establishment. Some amendments were, however, introduced regarding the requirements on the chair and vice chair of the Swedish Intelligence Commission and regarding the appointment of the other members of the Commission. Moreover, it was made clear that the Commission should examine in particular selectors, destruction and reporting. Furthermore, the Swedish Intelligence Commission was reinforced with additional legal competence and extended office support. Rules concerning supervision, organisation and processing were also prescribed in more detail in the Commission's instructions. The Commission was given the right to access the information and the assistance it needed for its activities from the agencies reviewed. For further details, see paras. 66-70 above.

139. It should also be reiterated that a special decision-making body at the Swedish Intelligence Commission – the Signals Intelligence Control Delegation – was given the right to order certain types of measures to be taken if, during supervision of the National Defence Radio Establishment, it emerged that signals intelligence was not being conducted in line with the legislation or that it was otherwise violating individuals' rights in a way that was not in reasonable proportion to the purpose of the measure. The measures that the Delegation was authorised to order included that a specific on-going collection process should be discontinued and that the recording or noting of data already collected should be destroyed. A decision to discontinue signals collection could refer to everything from a prohibition of subjecting a certain phenomenon to monitoring in any way, to using certain selectors (see para. 69 above).

140. Finally, the Government would like to recall the establishment of a Privacy Protection Council at the National Defence Radio Establishment. The Council had, and still has, a special responsibility to prevent signals intelligence from being conducted in a way that is not compatible with the legislation or the purpose of which cannot be deemed to be in reasonable proportion to the interference of privacy it would entail. The Council reports its observations to the management of the National Defence Radio Establishment and, if the Council finds reason to do so, to the Swedish Intelligence Commission. The Commission, through the Signals Intelligence Control Delegation is, as stated above, authorised to order that the collection of certain signals must be stopped or that material already collected must be destroyed (see para. 71 above).

141. In addition, the control mechanisms, supervisory elements and remedies that have been described in relation to the first period (see paras. 130-136) were also available during the second period. With the control mechanisms and supervisory elements introduced as from the second period, the possibilities for the public to challenge the signals intelligence work conducted by the National Defence Radio Establishment were consequently reinforced at that time. Hence, in relation to this period as well, the secrecy of such activities did not result in them being effectively unchallengeable and outside the supervision of the national authorities and the Court.

From the entry into force of the amended Signals Intelligence Act on 1 December 2009 and onwards (Third period)

142. As has been mentioned above, The Swedish Foreign Intelligence Inspectorate is responsible for the control of foreign intelligence as from the third period. The Inspectorate has the task of supervising that the foreign

intelligence work conducted by the relevant authorities is in accordance with the applicable legislation, and is also responsible for controlling signals intelligence. The Inspectorate is to monitor, in particular, selectors, destruction of data and reporting. For more details, see paras. 88-92 above.

143. Furthermore, the Swedish Foreign Intelligence Inspectorate is to check at the request of an individual whether his or her communication has been collected in connection with signals intelligence. Businesses and organisations may also request that checks be made. Following the check, the person who requested the investigation must be informed whether or not any improper collection has taken place. If the Swedish Foreign Intelligence Inspectorate finds evidence of improper signals collection, this must be reported to the individual as well as to the agencies responsible for the matter at hand, e.g. the Data Inspection Board, the Office of the Chancellor of Justice or the Office of the Prosecutor-General. The Swedish Foreign Intelligence Inspectorate is also to supervise the processing of data under the Act on processing personal data in the foreign intelligence and development operations of the National Defence Radio Establishment. For further details, see paras. 90-91 above.

144. In addition, the control mechanisms, supervisory elements and remedies that have been described in relation to the first and second periods (see paras. 130-136 and 138-140) were – with the exception of the control functions exercised by the Swedish Intelligence Commission – also available during the third period. With the control mechanisms, supervisory elements and remedy introduced as from the third period, the possibilities for the public to challenge the signals intelligence work conducted by the National Defence Radio Establishment were further reinforced at that time. In particular, note should be taken of the obligation on the part of the Swedish Foreign Intelligence Inspectorate to check, at the request of a natural or legal person, whether their communication has been collected in connection with signals intelligence and to report improper signals collection to the responsible agencies. Consequently, the Government holds that it is evident that also in relation to this period, the secrecy of the signals intelligence work conducted by the National Defence Radio Establishment does not result in these activities being effectively unchallengeable and outside the supervision of the national authorities and the Court.

Risk of secret surveillance measures being applied to the applicant

145. For the applicant to be able to claim to be a victim of a violation occasioned by the mere existence of state practice and legislation concerning

secret surveillance measures, there must also be a particular risk of such measures being applied to the applicant. In determining the risk of secret surveillance measures being applied to the applicant, it is relevant to reiterate the signals intelligence process as described above (paras. 20-22). In the following, the Government will elaborate further on different stages of that process.

146. Tasking directives for foreign intelligence work are initially established in an annual decision taken by the Government. The Government's tasking directives are sent to the National Defence Radio Establishment and the other agencies that have been designated by the Government to conduct foreign intelligence work, i.e. the Swedish Armed Forces, the Swedish Defence Materiel Administration and the Swedish Defence Research Agency. Since 1 December 2009, i.e. as from the third period, only the Government, the Government Offices and the Swedish Armed Forces are permitted to establish the detailed tasking directives of signals intelligence. During the first period, the Government was responsible for the tasking directives, and during the second period the agencies designated by the Government were also permitted to establish the detailed tasking directives of signals intelligence (Section 1 of the Foreign Intelligence Act). More detailed tasking directives provide the specific details of an overall need.

147. *Selectors* refer to a combination of technical data and various addressing details. From the previous description (paras. 20-22) it is clear that the use of selectors to identify traffic that is relevant to foreign intelligence work was effectively the same during all three time periods. The various components include for example frequencies, telephone numbers or IP addresses. The selectors are built up with great precision, which means that they consist of several components. By specifying selectors, the National Defence Radio Establishment can search through a signal and find the items in which the selectors appear. All parts must match to get a hit in the traffic collected. The selectors are intended to make searches accurate and to serve as a kind of filter to limit intelligence collection to what is relevant, as well as to prevent unlawful intelligence collection. This reduces the risk of unjustified infringement of personal privacy. Compared with a small number of less specific selectors, using a large number of justified selectors entails privacy protection for the people whose communications are not relevant to the foreign intelligence mandate.

148. The process of selecting signals with the use of selectors is conducted in two stages. In the first stage, data reduction at signals level is carried out, which means that only certain signals are chosen for further selection. This data reduction process is carried out on the basis of mainly technical parameters and

the National Defence Radio Establishment's knowledge of which signals may contain traffic that is relevant for foreign intelligence. Following data reduction, only a limited part of the traffic collected remains. In the next stage, data reduction is carried out at message level, which means that selectors are applied to the remaining traffic to sift out individual messages that are relevant to foreign intelligence. Information content is available to the National Defence Radio Establishment only after this process is complete.

149. Since 1 December 2009, the National Defence Radio Establishment has been obliged to obtain a permit from the Foreign Intelligence Court to collect electronic signals. The National Defence Radio Establishment's application for a permit refers to an intelligence collection assignment and contains a detailed account of the requirements underlying the application. The application further contains details of the link to the Government's annual tasking directives for foreign intelligence as well as to the detailed tasking directives of signals intelligence from the agency commissioning the intelligence (the Government, the Government Offices or the Swedish Armed Forces). All applications are presented to the head of the National Defence Radio Establishment for a decision. The Foreign Intelligence Court examines whether the intelligence collection assignment is reconcilable with the Foreign Intelligence Act and the Signals Intelligence Act, which means that it checks whether the application is relevant within the context of the tasking directives stated.

150. Selector management is to be done on the basis of the law and the Court's decision on which selectors or categories of selectors may be used. Based on the legislation, the National Defence Radio Establishment has established internal regulations concerning the management and design of selectors. These rules are intended to protect privacy and steer decision-making procedures and assessment criteria.

151. As stated above (para. 22), the signals intelligence process can be broadly divided into six stages. Traffic is not subjected to human scrutiny until the third or fourth stage, depending on whether the collected traffic is automatically or manually refined. As is clear from that description, the first stage of the signals intelligence process aims at limiting the traffic collected by choosing the relevant parts of the signals environment where traffic is to be collected. Consequently, not all traffic is collected and it is evident that claims about mass interception of all Swedes' traffic are incorrect. In the second stage the data collected is filtered (e.g., by using selectors to identify the relevant traffic that is present in the relevant parts of the signal environment) in order to further limit the data reaching the third stage. It is thus evident that not all traffic collected in the first

stage is subjected to human scrutiny. The traffic that is not scrutinised is automatically deleted after a certain time.

152. Turning to the present case, an initial prerequisite for the applicant firm's traffic to have been collected through signals intelligence in the first place is that the traffic occurred in the signals environment chosen for the collection of data (first stage). Furthermore, for the applicant firm's communication to have been sifted out at all in the filtering stage (second stage), it must have matched all the parameters of a selector. It must be borne in mind that the selectors that refer to the contents of the communication are designed, as has been described, with great precision as regards the foreign phenomena targeted by signals intelligence and on the basis of the purposes, as set down in law, for which foreign intelligence may be conducted. For the second and third period, the selectors were also in line with the Signals Intelligence Act and the detailed tasking directives provided by those who commissioned the intelligence based on their specific intelligence requirements.

153. From the description above it is thus clear that the risk that the applicant firm's traffic has been collected at all in the first and second stages of the signals intelligence process is very limited.

154. In any event, it is not until the third stage of the signals intelligence process that the information content is available to the National Defence Radio Establishment and this is the earliest stage that the traffic collected may be subjected to human scrutiny. It is consequently not until then that a secret surveillance measure can be considered to have been applied in relation to a natural or legal person. Traffic does not reach the third stage unless it is sifted out in the filtering stage, in principle only if it matches all the parameters of a selector. The likelihood that any part of the applicant firm's communication being sifted out and thus reaching the third stage of the signals intelligence process is virtually non-existent.

155. Consequently, the Government holds that the risk that a secret surveillance measure has been applied to the applicant firm during any of the three periods is virtually non-existent.

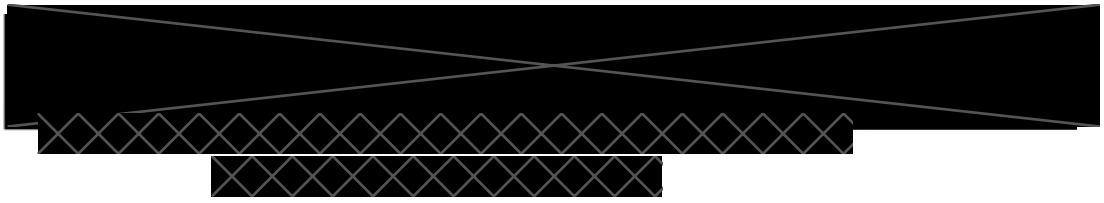
The Government's assessment and conclusions

156. The Court's task is not normally to review the contracting states' laws and practices *in abstracto*. However, in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision thereof, the Court has permitted general challenges to the relevant

legislative regime. The Court has therefore accepted that an individual may, under certain conditions, claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them. The principal reason, in such cases, justifying a right to challenge a law *in abstracto* is thus to ensure that the secrecy of such measures does not result in the measures being effectively unchallengeable and outside the supervision of the national authorities and the Court. In order to asses, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court has found that regard must be had to the availability to the public of any remedies at the national level and the risk of secret surveillance measures being applied to him.

157. Looking at the Court's case-law up until the *Kennedy* judgment, the Government draws the conclusion that the Court's main concern when assessing the remedies available to the public at the national level is that there exists domestic machinery whereby, subject to the limitations of the context, compliance with the relevant laws can be secured and that there are sufficient safeguards that secret surveillance powers are not being abused. For the applicant to be able to claim to be a victim of a violation occasioned by the mere existence of state practice and legislation concerning secret surveillance measures, there must also be a particular risk of such measures being applied to the applicant.

158. Turning to the present case, the Government contends that the aggregate of the control mechanisms, the supervisory elements and the remedies available during each of the three periods constitute sufficient safeguards against abuse of the secret surveillance powers in question. Furthermore, as submitted above, the Government holds that the risk that a secret surveillance measure has been applied to the applicant firm during any of the three periods is virtually non-existent. The Government therefore concludes that the applicant firm cannot claim to be a victim of a violation occasioned by the mere existence of Swedish state practice and legislation concerning secret surveillance measures within the meaning of Article 34 of the Convention.



Appendices

1. Agencies mentioned in the Observations
2. Acts and ordinances mentioned in the Observations