REGERINGSKANSLIET

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

Stockholm, 8 May 2015
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 AND MERITS

I. Introduction

1. These observations on the admissibility and merits 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 24 October 2014.

II. The Facts

2. The statement of facts prepared by the Registry of the Court consists essentially of the applicant firm's description of domestic legislation concerning signals intelligence. For its own part, the Government has submitted a thorough description of domestic legislation concerning signals intelligence in its observations on the admissibility of the present application, dated 27 April 2012 (hereinafter 'the Government's observations on admissibility'). The Government does not reiterate that description in full in the present observations, but would like to make some clarifications, amendments and supplements to that description, and will essentially do so in connection to its observations on the merits. However, the Government would, at this point, like to make a minor correction of the Government's observations on admissibility, as well as briefly respond to the third party observations submitted by ICJ-Norway on 11 February 2009 (hereinafter 'the third party observations').

3. As regards the correction, the reference to the Act on the processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment (2007:259) in para. 109 of the Government's observations on admissibility should rightly be to *Chapter 2*, Section 5 of that Act (and not simply to Section 5 of the same Act).

4. Concerning the third party observations, the Government firstly notes that they were submitted to the Court during the second time period, and hence before the legislation concerning the third time period was adopted. Accordingly, the third party observations are essentially relevant with regard to the Court's examination of the complaint concerning the second time period. In this connection it is important to reiterate that collection from cables was not possible until after 1 December 2009, i.e. as from the third time period, when the regulation concerning the obligation on the part of the cable owners to make traffic available entered into force.

5. ICJ-Norway's contention that individuals in Norway are deprived of legal rights in comparison with individuals in Sweden (see para. 4 of the third party observations) is incorrect. An individual who wants to make an application to

any of the authorities responsible for supervising the signals intelligence conducted by the National Defence Radio Establishment (*Försvarets radioanstalt*) obviously has the right to do so irrespective of citizenship or geographical location (see Government Bill 2006/07:63, p. 87; see also para. 91 of the Government's observations on admissibility).

6. ICJ-Norway further contends, *inter alia*, that Swedish legislation allows the National Defence Radio Establishment to secretly monitor, intercept, review and store the contents of *all* electronic communication passing Sweden's borders (see paras. 12 and 13 of the third party observations). In response to those contentions, the Government refers to paras. 13–22 and 145–151 of its observations on admissibility. Moreover, the Government would like to clarify that during the second time period, the mandate of the National Defence Radio Establishment was limited to signals intelligence targeting wireless traffic. The Government would also like to underline that both the legal and practical limitations on the conducting of signals intelligence within foreign intelligence contradicts allegations about collection of all electronic communication.

7. As regards paras. 20–21 of the third party observations and the internal Government document referred to in those paragraphs, the Government finds it pertinent to clarify the following. The internal Government document in question is a PowerPoint presentation, seemingly written before the third time period. Furthermore, it is evident from the document that it contains an enumeration of possible proposals for legislative amendments. The Government finds it appropriate to stress that as from the third time period, *all* signals intelligence collection conducted by the National Defence Radio Establishment requires a permit from the Foreign Intelligence Court (*Försvarsunderrättelse-domstolen*) and that there are no exceptions to this precondition (see para. 77 of the Government's observations on admissibility). Accordingly, ICJ-Norway is incorrect in alleging that the obligation to obtain a permit in order to use selectors attributable to a specific natural person only applies in relation to Swedish residents (see para. 76 of the Government's observations on admissibility).

8. To the extent that the contentions submitted by ICJ-Norway have not been commented upon at this stage, the Government refers to its observations on admissibility and to its observations on the merits below. However, the fact that not all the issues raised by ICJ-Norway in its observations are commented upon should not be taken to mean that the Government accepts those parts of the observations that have not been addressed.

III. On the Admissibility

9. 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, and that it has not had access to an effective remedy under Article 13 of the Convention. The applicant firm has not alleged any actual interception of its communications. It may therefore be concluded that the applicant firm complains about the signals intelligence regime in itself. Against this backdrop, the Government has previously been asked by the Court to address the following question in separate observations on admissibility:

> *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)?*

10. Initially, the Government wishes to raise the concern that the use of the words "state practice" in the Court's question seems to suggest that the signals intelligence conducted by the National Defence Radio Establishment may have been unregulated during one or more of the time periods concerned. The Government wishes to underline that the signals intelligence at issue in the present case has been regulated by laws and ordinances during all three time periods (see paras. 40–47, 55–65 and 72–87 of the Government's observations on admissibility as well as paras. 68–69 below).

11. In its observations on admissibility and in response to the Court's specific question, the Government held that the applicant firm cannot claim to be a victim of a violation of the Convention during any of the three time periods. The Government would like to clarify that it maintains that the aggregate of the control mechanisms, the supervisory elements and the remedies available during each of the three time periods constitute sufficient safeguards against abuse of the National Defence Radio Establishment's competence to conduct signals intelligence. The Government furthermore maintains that the risk that the applicant firm has been subjected to signals intelligence 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 legislation concerning signals intelligence within foreign

intelligence (see paras. 120–158 of the Government's observations on admissibility and paras. 51–53 of the Government's further observations on the admissibility of the present case, dated 25 January 2013; hereinafter 'the Government's further observations on admissibility'). It therefore follows that the applicant firm's complaint should be declared inadmissible *ratione personae* with respect to all three time periods.

12. In addition, the Government finds it relevant to note that in previous cases concerning secret surveillance measures, the Court has not been consistent in how it has dealt with the question of an applicant's victim status. In some cases, the Court has dealt with this question when examining the admissibility of the application (see *Klass and Others v. Germany*, no. 5029/71,§ 38, 6 September 1978, and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 58–61, 28 June 2007), while in other cases the question of victim status was considered when examining the merits and as part of the assessment of whether there has been an interference of a certain Article of the Convention (*Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 56–57, 1 July 2008, and *Kennedy v. the United Kingdom,* no. 26839/05, §§ 118–129, 18 May 2010). For its part, the Government would like to stress that the question of victim status should rightly be dealt with when examining the admissibility of an application in accordance with the logic of the Convention, since victim status is a requirement for the Court to receive an application (Article 34; see *Klass and Others v. Germany*, § 38). In the present case, the Government finds no reason to depart from that principle, especially as the Court initially found it appropriate to request the parties' observations solely on the question of victim status.

13. Moreover, in the Government's observations on admissibility, the Government found that there could be reason to question whether the applicant firm had exhausted all domestic remedies available with respect to each of the three time periods concerned, but the Government limited itself to responding to the question put forward by the Court. The Government would like to clarify that it leaves for the Court to decide whether the applicant firm has exhausted all domestic remedies with respect to each of the three time periods.

14. Finally, with reference to what is submitted in connection with the observations on the merits below, the Government holds that the applicant firm's complaint regarding Articles 8 and 13 should be declared inadmissible *ratione materiae* or as being manifestly ill-founded.

IV. On the Merits

15. The Government has been asked to address the following questions in its observations on the merits:

> *1. Assuming that the applicant firm can claim to be a victim in the present case, has there been an interference with its rights under Article 8 § 1 of the Convention, and, if so, was that interference in accordance with the law and necessary in terms of Article 8 § 2?*
>
> *In particular, did such secret surveillance measures comply with the requirements of minimum legislative safeguards and of supervision of the regime as set out in the Court's case-law (see, for instance, Weber and Saravia v. Germany (dec.), no. 54934/00, § 95, ECHR 2006-XI, and Kennedy v. the United Kingdom, no. 26839/05, §§ 159–169, judgment of 18 May 2010) during each of the three time periods: a) before 1 January 2009, b) from 1 January to 30 November 2009, and c) as from 1 December 2009?*
>
> *2. Have the applicant's concerns about secret surveillance measures being applied to it required that it has access to an effective remedy within the meaning of Article 13 of the Convention? If so, has the applicant had an effective remedy at its disposal?*

The Government will limit itself accordingly.

Article 8

16. As stated above, the applicant firm complains that Swedish state practice and legislation concerning signals intelligence within foreign intelligence have violated and continue to violate its rights under Article 8 of the Convention.

17. The Court has asked whether, assuming that the applicant firm can claim to be a victim in the present case, there has been an interference with the applicant firm's rights under Article 8 § 1 of the Convention, and, if so, whether that interference was in accordance with the law and necessary in terms of Article 8 § 2. The Court has in particular asked whether such secret surveillance measures comply with the requirements of minimum legislative safeguards and of supervision of the regime as set out in the Court's case-law during each of the three time periods.

Domestic legislation concerning signals intelligence

18. Before responding to the Court's question, the Government will make some clarifications, amendments and supplements to the description of domestic

legislation concerning signals intelligence submitted in its observations on admissibility.

Signals intelligence within foreign intelligence

19. The Government finds it worth reiterating that the present case is limited to signals intelligence within foreign intelligence (cf., *inter alia*, *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, *Liberty and Others v. the United Kingdom*, cited above, and *Kennedy v. the United Kingdom*, cited above). It cannot be overemphasised that this activity is of a very special nature.

20. Foreign intelligence work is conducted in support of Swedish foreign, defence and security policy, and to identify external threats to the country (see further paras. 5–9 of the Government's observations on admissibility). Foreign intelligence work is limited to foreign circumstances, which 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.

21. The Government has the primary responsibility for satisfying Sweden's interests with respect to foreign, security and defence policy. Making accurate assessments of situations abroad and taking necessary decisions requires adequate background information. Foreign intelligence work, including signals intelligence, contributes to this. The Government's needs are of an overall strategic nature (see further paras. 24 and 65 below).

22. However, the fact that foreign intelligence work exclusively targets foreign circumstances, i.e. activities or phenomena that originate abroad, does not preclude that foreign intelligence may also concern certain domestic phenomena. Where the activities in question take place is not, therefore, the crucial factor. An example of a situation in which foreign circumstances must be considered to extend inside domestic borders is when activities constituting a threat to the country originate in another country but are conducted by representatives in Sweden or in some other way use resources in Sweden. It is then a matter of investigating the link between the foreign circumstances and Sweden in order to assess the threat to the country.

23. It is important to emphasise that the mandate of the agencies conducting foreign intelligence work is limited to intelligence gathering; all measures to tackle threats of a criminal nature that can be identified within the country are

reserved for the law enforcement agencies. There can, therefore, never be any question of the agencies that conduct foreign intelligence work devoting their attention to circumstances of a purely domestic nature, regardless of whether these fall within the responsibility of the law enforcement agencies or are entirely different in nature. Such circumstances fall entirely within the responsibility of other agencies.

24. Signals intelligence within foreign intelligence thus differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. Signals intelligence within foreign intelligence is not about identifying or mapping individuals, but about searching for *a priori* unknown foreign phenomena. Signals intelligence is hence proactive: it is about finding a danger rather than investigating a known danger. The purpose of the signals intelligence conducted by the National Defence Radio Establishment is to obtain strategic information and identify phenomena of relevance for foreign intelligence.[1] To date, the Court has only examined two cases related to strategic surveillance: *Weber and Saravia v. Germany* and *Liberty v. the United Kingdom*, both cited above. However, the case of *Weber and Saravia* concerned legislation that also permits surveillance for investigating crimes, and hence is in many respects incomparable with the present case. The case of *Liberty* concerned legislation aimed at strategic surveillance that did not permit intercepted material to be used in court. Nevertheless, the judgment is of minor relevance when examining the present case, for the following reason. In the case of *Liberty*, the Court found that the interference with the applicant's rights under Article 8 was not "in accordance with the law" since the procedure to be followed for examining, sharing, storing and destroying intercepted material had not been set out in a form accessible to the public. By contrast, the signals intelligence at issue in the present case was and is regulated by acts and ordinances that are accessible to the public.

Secrecy and the principle of public access to official documents

25. 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 (see para. 11 of the Government's observations on admissibility and paras. 28–29 below).

---

[1] Cf. the Venice Commission's report "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies", adopted by the Venice Commission at its 102nd Plenary session, 20–21 March 2015, paras. 85 and 92.

26. Nevertheless, it is important to keep in mind that the principle of public access to official documents also applies to foreign intelligence work, and thus to signals intelligence conducted by the National Defence Radio Establishment. The principle of public access to official documents means, among other things, that the public has a right of access to public administration. One way in which the principle is expressed is through regulations on the public nature of official documents. This means that individuals are generally entitled to access official documents. This is also enshrined in the Constitution of Sweden via the Freedom of the Press Act. The right of public access to official documents also guarantees the public's right of insight into the activities of government agencies, not least via media monitoring and scrutiny.

27. There are, however, exceptions to the right of public access to official documents. It is possible, under certain circumstances, to restrict the right to access official documents. The circumstances under which it is possible to impose such restrictions are outlined in the Freedom of the Press Act. The Act also states that any restrictions are to be specified in a special act of law. That act of law is the Public Access to Information and Secrecy Act (2009:400). Information can thus be kept secret through a secrecy provision in the Public Access to Information and Secrecy Act.

28. Under Chapter 15, Section 2 of the Public Access to Information and Secrecy Act, secrecy applies to information concerning activities to defend the country, and the planning or other preparation of such activities, and activities that otherwise concern the comprehensive defence strategy, if it can be assumed that disclosure of the information would damage the country's defence or endanger the security of the realm in some other way ('defence secrecy'). This provision was previously found in the old Secrecy Act (1980:100), which was replaced by the current Public Access to Information and Secrecy Act on 30 June 2009. Defence secrecy applies throughout all public sector activities.

29. Defence secrecy is intended to protect information concerning the organisation of Sweden's defence and security. Information concerning the country's intelligence activities is, naturally, of considerable importance to the security of the realm. Defence secrecy in intelligence activities is necessary to protect sources, methods and results. If information about these is divulged, there is a very great risk that the capabilities of Sweden's intelligence and security services will be reduced or lost entirely, and thus that access to information of crucial importance to the security of the realm will be lost. Methods and sources can be very costly to establish and take a long time to build up. At the same time, if a source or method is divulged, simple countermeasures can render it entirely

useless. See also para. 16 of the Government's further observations on admissibility.

30. Under the Freedom of the Press Act and the Public Access to Information and Secrecy Act, the general rule is that it is the agency where the document is held that determines whether or not a document should be released. This determination depends on whether or not the agency considers that any secrecy provision applies. As a main rule, a decision of an agency not to release a document can be appealed to the Administrative Court of Appeal (*Kammarrätten*), and subsequently to the Supreme Administrative Court (*Högsta förvaltnings-domstolen*).

31. The supervisory mechanisms that have been and are in place regarding foreign intelligence work are of course of the utmost importance as they, among other things, are to compensate for the necessary secrecy that surrounds this special form of state activity (see para. 122 below).

Tasking directives

32. It may be appropriate to reiterate that under the Foreign Intelligence Act (2000:130), the Government determines the tasking directives for all foreign intelligence work. This is done on an annual basis. Within the framework of these tasking directives, agencies appointed by the Government can issue more detailed tasking directives for signals intelligence (see para. 12 of the Government's observations on admissibility). The Government's tasking directives are therefore a form of agency governance, comparable to that exercised through the appropriation directions issued annually to every government agency, with a view to steering the direction of its activities. The scope for the Government to present its needs is limited by law. For example, foreign intelligence can only be conducted for certain purposes and can only target foreign circumstances (see paras. 20–23 above and paras. 70–71, 84–87 and 107–108 below).

33. The Government's tasking directives are determined by a Government decision (*regeringsbeslut*). The Government works as a collective and thus the members of the Government must have reached consensus before a decision is taken. The quality of the Government's work is ensured by the requirements concerning the preparation of Government business, which is regulated by, *inter alia*, the Instrument of Government. As is the case for the Government's other work, the Government is answerable to the Riksdag in this area and the decisions are subject to subsequent parliamentary scrutiny functions, e.g. the Swedish

National Audit Office (*Riksrevisionen*) and the parliamentary checks exercised by the Riksdag Committee on the Constitution (*Konstitutionsutskottet*).

34. It may also be clarified that 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 work conducted by 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 (see paras. 18–19 of the Government's observations on admissibility). Before measures are initiated, the National Defence Radio Establishment naturally has a responsibility to examine whether the tasking directives are in accordance with the law; the Establishment cannot enforce tasking directives that contravene the law.

Practical aspects of signals intelligence work

35. Turning to the practical aspects of the signals intelligence work conducted by the National Defence Radio Establishment, the Government's observations on admissibility contain a general description thereof (see paras. 13–22, 32–38 and 146–151). The Government finds that it may still be worth reiterating the following.

36. In many respects 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 the relevant agencies. During all three time periods, the work has exclusively targeted foreign circumstances. However, it is important to reiterate that collection from cables was not possible until after 1 December 2009, i.e. as from the third time period, when the regulation concerning the obligation on the part of the cable owners to make traffic available entered into force. Hence, during the first and second time periods, the mandate of the National Defence Radio Establishment was limited to signals intelligence targeting wireless traffic (see further paras. 27–30 of the Government's further observations on admissibility). Apart from that, the differences between the three time periods mainly concerned the agencies that may determine the detailed tasking directives of signals intelligence, the arrangements by which the detailed tasking directives are decided, 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 (see paras. 18 and 32 of the Government's observations on admissibility).

37. The Government would like to reiterate the description of the signals intelligence process made in the Government's observations on admissibility (see paras. 21–22). The description below is technology-neutral, i.e. it can be used for signals intelligence targeting terrestrial or satellite radio communications as well as cable traffic. That said, it must be kept in mind that the collection process in stage two below must be done automatically insofar as it concerns cable collection.

38. The signals intelligence process at the National Defence Radio Establishment can be broadly divided into six stages:

1) Firstly, a choice is made as to which parts of the signal environment that 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 prescribed by law 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.

39. In this context, it may also be added that staff who process data at the National Defence Radio Establishment are security cleared in accordance with the Protective Security Act (1996:627). Security clearance assessments are made continuously throughout the term of employment. Various restrictions on access to data mean that in practice the data processed at the National Defence Radio Establishment is only accessible to a limited number of people.

40. In addition to this, and in order to further elucidate signals intelligence work and the signals intelligence process, the Government would like to refer to a few examples and illustrations; see Appendix 3. The Government also finds it relevant to refer to the 2014 Annual Report of the National Defence Radio Establishment; see Appendix 4.

Communicating the data to other parties

41. The Government finds it appropriate to give the following brief account concerning the reporting by the National Defence Radio Establishment to the government agencies concerned and the Establishment's cooperation with other countries.

42. The National Defence Radio Establishment reports to Swedish principals and relevant government agencies in accordance with applicable legislation. The Public Access to Information and Secrecy Act and legislation concerning personal data regulate the extent to which reports may be provided to other government agencies. All reports from the National Defence Radio Establishment concern national defence or national security and are thus classified in accordance with the Public Access to Information and Secrecy Act (see paras. 28–29 above). A report's classification is also applicable with regard to other government agencies.

43. International cooperation may be conducted in accordance with the Foreign Intelligence Act and, as from the second time period, with Section 9 of the Signals Intelligence Act (2008:717); see para. 47 of the Government's further observations on admissibility. The agencies that are to conduct foreign intelligence may, in accordance with specific instructions from the Government, establish and maintain cooperation in intelligence matters with other countries and international organisations (Section 3 of the Foreign Intelligence Act). Furthermore, the agencies that conduct foreign intelligence work can only cooperate on intelligence matters with other countries and international organisations on the condition that the purpose of the cooperation is to serve the Swedish government, Swedish interests and Sweden's comprehensive defence strategy. The information passed on by agencies to other countries must not be

detrimental to Swedish interests (Section 3 of the Foreign Intelligence Ordinance, 2000:131); see paras. 42–43 of the Government's observations on admissibility. It should be underlined that cooperation with other countries, which is a part of foreign intelligence work, was previously subject to supervision by the Swedish Intelligence Commission (*Försvarets underrättelsenämnd*) and is currently subject to supervision by the Swedish Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten*). Also in respect of international cooperation, the Public Access to Information and Secrecy Act and legislation concerning personal data regulate the extent to which reports may be provided.

Supervision of signals intelligence

44. The Government would like to offer the following updates and additions concerning the supervision of the signals intelligence work.

45. As stated in the Government's further observations on admissibility, the Government is required to report annually on the review of signals intelligence conducted under the Signals Intelligence Act (see para. 18). The report is made in a special written communication from the Government to the Riksdag (*regeringens skrivelse*). The most recent written communication is *Regeringens skrivelse 2014/15:27 Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet*, which covers the year 2013.

46. In this communication, the Government concludes that the system for safeguarding privacy in the signals intelligence conducted by the National Defence Radio Establishment works as intended. At the same time, the Government is open to the fact that a need may arise in the future for in-depth follow-up of the impact on privacy of the Signals Intelligence Act. Furthermore, the Government stresses the importance of safeguarding legal certainty and privacy in signals intelligence and acknowledges that this is an ongoing process.

47. In its response to the Government communication, the Riksdag noted that the system for safeguarding privacy in signals intelligence works as intended (*Försvarsutskottets betänkande, bet. 2014/15:FöU5, rskr. 2014/15:27*).

48. Under Section 2 of the Ordinance containing instructions for the Swedish Foreign Intelligence Inspectorate (2009:969), the Inspectorate is the supervisory authority under the Signals Intelligence Act. Under Section 10 of the Signals Intelligence Act, the Inspectorate is to control compliance with the Act. These controls are to encompass, in particular, scrutiny of selectors, destruction of data and reporting. The Swedish Foreign Intelligence Inspectorate issues a report on

its activities annually. The Government would like to draw the Court's attention to the following relevant passages in the latest reports.

49. During the period 2009–2014, the Inspectorate conducted audits of the National Defence Radio Establishment on 65 occasions in total.[2] The audits in the period 2009–2014 resulted in a total of 10 opinions.[3] During the same time period, the Swedish Foreign Intelligence Inspectorate carried out a total of 86 checks at the request of an individual of whether his or her communications had been the subject of signals intelligence (see paras. 111, 122 and 126 below).[4] None of the checks showed that improper signals collection had taken place.[5]

50. It may also be mentioned that the Swedish Foreign Intelligence Inspectorate's audits in the period 2009–2014 did not lead to the Inspectorate presenting any opinions to the Government, or to it referring any cases to any other agency (see para. 122 below).[6]

51. The Inspectorate has a mandate to terminate collection and/or order destruction of recordings or notes if it is shown that they were collected in a way that is incompatible with the permit issued by the Foreign Intelligence Court (see para. 120 below). Such measures have not been necessary in any year of the Inspectorate's existence so far.[7]

52. The aim of the Inspectorate's audits with regard to selectors is to check that the National Defence Radio Establishment is using selectors in a way that is compatible with the permit issued by the Foreign Intelligence Court. In the period 2010–2014, the Inspectorate audited the Establishment's use of selectors on 17 occasions.[8] During this period, only one of the audits carried out in 2010 led to the Inspectorate issuing an opinion on the Establishment's use of

---

[2] 2 audits in 2009, 7 audits in 2010, 13 audits in 2011, 15 audits in 2012, 14 audits in 2013 and 14 audits in 2014.
[3] 1 opinion in 2009, 1 opinion in 2010, 4 opinions in 2011, 1 opinion in 2012, 2 opinions in 2013 and 1 opinion in 2014.
[4] 7 checks in 2010, 3 checks in 2011, 4 checks in 2012, 62 checks in 2013 och 10 checks in 2014.
[5] See p. 2 of the 2009 Annual Report, p. 1–4 of the 2010 Annual Report, p. 2 and 7 of the 2011 Annual Report, p. 5 and 10 of the 2012 Annual Report, p. 3 and 8 of the 2013 Annual Report and p. 4 and 9 of the 2014 Annual Report. The annual reports of the Swedish Foreign Intelligence Inspectorate are available at http://www.siun.se/dokument.html
[6] See the 2009 Annual Report, p. 3 of the 2010 Annual Report, p. 3 of the 2011 Annual Report, p. 7 of the 2012 Annual Report, p. 5 of the 2013 Annual Report, and p. 6 of the 2014 Annual Report.
[7] See p. 8 of the 2012 Annual Report (which also encompasses previous years' controls), p. 6 of the 2013 Annual Report, and p. 6 of the 2014 Annual Report.
[8] 3 audits in 2010, 4 audits in 2011, 4 audits in 2012, 3 audits in 2013 and 3 audits in 2014.

selectors, along with a proposal for changes to the Establishment's processing routines. The other audits did not lead to any opinions.[9]

53. The Inspectorate's audits with regard to destruction check compliance with the provision in the Signals Intelligence Act on the obligation to destroy data. In the period 2010–2014, the Inspectorate carried out audits of data destruction related to the Establishment's signals intelligence operations on a total of nine occasions.[10] During this period, only the audit carried out in 2011 led the Inspectorate to issue any opinions or proposals to the Establishment.[11] The 2011 audit led to the Inspectorate proposing that the Establishment amend its internal regulations to better correspond to the legal regulations, and later the same year the Establishment adopted the changes proposed by the Inspectorate.[12]

54. Furthermore, in the period 2011–2014, the Inspectorate carried out audits of the National Defence Radio Establishment's reporting on a total of 12 occasions.[13] Two of the audits carried out in 2011 led to opinions from the Inspectorate with respect to reporting, while the other audits did not give rise to any opinions. The National Defence Radio Establishment has followed up these opinions and tightened its routines.[14]

55. Under Section 3 of the Inspectorate's instructions, the Inspectorate is to scrutinise the National Defence Radio Establishment's processing of personal data based on the Act on Processing of Personal Data in the National Defence Radio Establishment's Defence Intelligence and Development Operations. In the period 2010–2014, the Inspectorate carried out audits of the National Defence Radio Establishment's processing of personal data on a total of 13 occasions.[15] During this period, three audits (2 in 2013 and 1 in 2014) led to comments from the Inspectorate with respect to the processing of personal data.[16]

---

[9] See p. 3–4 of the 2010 Annual Report, p. 6 of the 2011 Annual Report, p. 8 of the 2012 Annual Report, p. 7 of the 2013 Annual Report and p. 7 of the 2014 Annual Report.
[10] 1 audit in 2010, 1 audit in 2011, 3 audits in 2012, 2 audits in 2013 and 2 audits in 2014.
[11] See p. 3–4 of the 2010 Annual Report, p. 6–7 of the 2011 Annual Report, p. 8 of the 2012 Annual Report, p. 6–7 of the 2013 Annual Report and p. 7 of the 2014 Annual Report.
[12] See p. 6–7 of the 2011 Annual Report.
[13] 3 audits in 2011, 3 audits in 2012, 3 audits in 2013, and 3 audits in 2014.
[14] See p. 7 of the 2011 Annual Report, p. 9 of the 2012 Annual Report, p. 7 of the 2013 Annual Report, and p. 8 of the 2014 Annual Report as well as para. 48 of the Government's further observations on admissibility.
[15] 1 audit in 2010, 3 audits in 2011, 3 audits in 2012, 3 audits in 2013, and 3 audits in 2014.
[16] See p. 4 of the 2010 Annual Report, p. 8 of the 2011 Annual Report, p. 11–12 of the 2012 Annual Report, p. 9–10 of the 2013 Annual Report, and p. 10 of the 2014 Annual Report.

56. It may, moreover, be relevant to draw the Court's attention to the fact that during 2011, the Inspectorate controlled whether the National Defence Radio Establishment was conducting data collection for other countries pursuant to the Foreign Intelligence Act. The Establishment explained that no such collection was carried out.[17]

57. Finally, the Government would like to add that in 2014 the Swedish National Audit Office audited the Swedish Foreign Intelligence Inspectorate.[18] The National Audit Office is part of the central control power of the Swedish Riksdag and audits the entire chain of executive power (see para. 33 above). The National Audit Office is independent in relation to those it audits. It carries out both performance and financial audits. In its audit of the Swedish Foreign Intelligence Inspectorate, the National Audit Office examined whether the supervision of the foreign intelligence work functions effectively and efficiently. The conclusion reached by the National Audit Office is that the Swedish Foreign Intelligence Inspectorate has been given the necessary prerequisites in order to carry out its supervisory functions in an efficient manner, and that the Inspectorate performs its duties according to the relevant acts and ordinances. The National Audit Office also found that foreign intelligence work in general, and the signals intelligence conducted by the National Defence Radio Establishment in particular, is a field that is well regulated. The audit conducted by the National Audit Office also shows that the foreign intelligence agencies attach great importance to the Swedish Foreign Intelligence Inspectorate's views, and take measures in accordance with the Inspectorate's decisions.

Applicability of Article 8 and possible interference

58. Firstly, the Government would like to reiterate its conclusion that the applicant firm cannot claim to be a victim of a violation occasioned by the mere existence of Swedish legislation concerning signals intelligence within foreign intelligence (see para. 11 above). It hence follows that the applicant firm cannot complain of an interference with its rights under Article 8 of the Convention (compare and contrast *Kennedy v. the United Kingdom*, cited above, §§ 118–129). The Government therefore holds that Article 8 is not applicable in the present case with respect to any of the three time periods. Consequently, the applicant firm's complaint in this part should be declared inadmissible *ratione materiae* with respect to all three time periods.

---

[17] See p. 9 of the 2011 Annual Report.

[18] Kontrollen av försvarsunderrättelseverksamheten (RiR 2015:2); available at http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2015/Kontrollen-av-forsvars173under173rattelse173verk173sam173heten/

59. However, if the Court were to find that the applicant firm can claim to be a victim of a violation of the Convention, the Government does not contest that there has been an interference under Article 8. Nevertheless, the Government maintains that the only Article 8 right at issue in the present case is the applicant firm's right to respect for its correspondence (see para. 121 of the Government's observations on admissibility and paras. 5–10 in its further observations on admissibility). Furthermore, the Government holds that any possible interference is in accordance with the law and necessary in terms of Article 8 § 2 with respect to all three time periods. The Government will elaborate below on the reasons for this contention.

Justification for a possible interference

60. Initially, the Government considers that it is clear that the signals intelligence permitted by the legislation at issue in the present case during each of the three time periods pursues the legitimate aim of protecting national security (see paras. 41, 56 and 74 of the Government's observations on admissibility, cf. *Kennedy v. the United Kingdom*, cited above, § 155).

61. When assessing whether an interference is "necessary in a democratic society" in pursuit of a legitimate aim in the context of secret surveillance, the Court has stated that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others v. Germany*, §§ 49–50; *Weber and Saravia v. Germany*, § 106 and *Kennedy v. the United Kingdom*, § 153, all cited above).

62. The Court has further acknowledged that the Contracting States enjoy a fairly wide margin of appreciation in assessing the existence and extent of such necessity and in choosing the means for achieving the legitimate aim of protecting national security, but that this margin is subject to European supervision. The Court's task in cases concerning secret surveillance measures is therefore to determine whether the procedures for supervising the ordering and implementation of the measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009, *Weber and Saravia v. Germany*, § 106, *Klass and Others v. Germany*, § 49 and *Kennedy v. the United Kingdom*, § 154, all cited above).

63. At this juncture, the Government reiterates that the present complaint concerns Swedish legislation regarding signals intelligence, and not any alleged actual interception of the applicant firm's communications. Accordingly, in its examination of the justification for a possible interference under Article 8 § 2, the Court is required to examine the proportionality of the legislation itself and the safeguards built into the system allowing signals intelligence, rather than the proportionality of any specific measures taken in respect of the applicant firm. In these circumstances, the lawfulness of a possible interference is closely related to the question whether the "necessity" test has been complied with in respect of Swedish legislation concerning signals intelligence. The Government therefore finds that it would be appropriate for the Court to address the requirements of "in accordance with the law" and "necessity" jointly (see *Kvasnica v. Slovakia* § 84 and *Kennedy v. the United*, § 155, both cited above).

64. For the assessment of these requirements, the Court has, in its case-law on secret surveillance measures, developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: 1) the nature of the offences which may give rise to an interception order; 2) a definition of the categories of people liable to have their telephones tapped; 3) a limit on the duration of telephone tapping; 4) the procedure to be followed for examining, using and storing the data obtained; 5) the precautions to be taken when communicating the data to other parties; and 6) the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig v. France*, no. 11105/84, § 34, 24 April 1990; *Amann v. Switzerland*, no. 27798/95, § 76, 16 February 2000; *Valenzuela Contreras v. Spain*, no. 27671/95, § 46, 30 July 1998; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003 and *Weber and Saravia v. Germany*, cited above, § 95; cf. *Kennedy v. the United Kingdom*, cited above, §§ 151–154).

65. For its part, the Government notes that the minimum safeguards enumerated in the cited case-law presuppose that the secret surveillance measures at issue are linked to a certain individual or to a certain place and concern a criminal offence. In the Government's view, it is thus clear that the minimum safeguards have been developed by the Court in case-law relating to the use of secret surveillance measures for the purpose of investigating crimes (e.g. *Kennedy v. the United Kingdom*, cited above), or at least in relation to legislation that permits the intelligence gathered to be used in the investigation of crimes (e.g. *Weber and Saravia v. Germany*, cited above). However, signals intelligence within Swedish foreign intelligence may not be used to collect information for use in investigating crime (see para. 23 above and para. 106 below). On the

contrary, the purpose of the signals intelligence conducted by the National Defence Radio Establishment is to obtain strategic information and identify phenomena of relevance for foreign intelligence. In certain cases, signals intelligence does indeed have to concern individuals' communications so as to make it possible to monitor a certain phenomenon that is relevant to the objectives of signals intelligence work. However, in the context of signals intelligence, individuals are not of interest *per se,* but only as carriers of information (see further para. 24 above). The Government is aware of the Court's statement in *Liberty and Others v. the United Kingdom*, cited above, that it does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications on the one hand, and more general programmes of surveillance on the other. Nevertheless, the Government holds that the requirements set out in the Court's case-law cannot be directly applicable in the present case, in which the legislation to be examined by the Court does not permit the use of signals intelligence to investigate offences. For these reasons, the Government holds that some adaptations of the minimum safeguards set out in the Court's case-law are necessary in the present case.

66. Indeed, the Court has already made some adaptations to the requirements concerning "the nature of the offences" and "categories of persons". Firstly, it is clear from the case of *Kennedy v. the United Kingdom*, cited above, that the condition of foreseeability does not require States to set out exhaustively by name the specific offences that may give rise to interception (§ 159). In the *Kennedy* judgment, the Court further held that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. Moreover, with reference to the case of *Al-Nashif v. Bulgaria,* no. 50963/99, 20 June 2002, the Court clarified that by the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. The Court's conclusion in the *Kennedy* judgment was thus that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to use secret surveillance (§ 159). The Court has also observed that there is an overlap between the requirement that the categories of persons be set out and the requirement that the nature of the offences be clearly defined, and that the relevant circumstances which can give rise to interception give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted (see *Kennedy*, § 160). However, in the Government's view, even with those adaptations, these two requirements are not directly applicable when, as in the present case, the

legislation to be examined by the Court does not permit the use of signals intelligence to investigate offences.[19] In view of the above, the Government finds that, rather than explicitly addressing requirements 1 and 2 of the minimum legislative safeguards as set out in the Court's case-law (see para. 64 above), it is more appropriate in the present case to describe the circumstances in which the National Defence Radio Establishment was and is empowered to conduct signals intelligence. The Government will therefore address this issue under that heading.

67. Moreover, the Government considers that requirements 3–6 of the minimum legislative safeguards as set out in the Court's case-law (see para. 64 above) all concern the conditions for how signals intelligence could and may be executed by the National Defence Radio Establishment. The Government will therefore jointly address those requirements under that heading.

First time period

68. Initially, the Government wishes to stress that the applicant firm's contention that the National Defence Radio Establishment conducted unregulated signals intelligence during this time period is incorrect. The signals intelligence conducted by the National Defence Radio Establishment during this time period was mainly regulated in the Foreign Intelligence Act and the Foreign Intelligence Ordinance, the Electronic Communications Act (2003:389) and the Ordinance containing instructions for the National Defence Radio Establishment (2007:937); see para. 40 of the Government's observations on admissibility. It should further be kept in mind that the signals intelligence conducted by the National Defence Radio Establishment during this time period was limited to wireless traffic.

69. Consequently, there was a legal basis for the signals intelligence conducted by the National Defence Radio Establishment during the first time period.

(1) The circumstances in which the National Defence Radio Establishment was empowered to conduct signals intelligence

70. Under the Foreign Intelligence Act, foreign intelligence during the first time period was to be undertaken to identify "external military threats to the country" and to "support foreign, defence and security policy". Foreign intelligence included Swedish participation in international security cooperation and, in

[19] Cf. the Venice Commission's report "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies", paras. 15 and 102.

accordance with what the Government decided, involvement in supporting society in the event of serious peacetime emergencies (see para. 41 of the Government's observations on admissibility). Consequently, signals intelligence could only be conducted on the grounds of national security.

71. Additional clarification on the terms "external military threats to the country" and "support foreign, defence and security policy" was provided in the *travaux préparatoires* to the Foreign Intelligence Act (Government Bill 1999/2000:25). The *travaux préparatoires* clearly state that foreign intelligence work may only concern intelligence that is important for the external security of the realm and for international security cooperation in the form of Swedish support to and participation in security-building cooperation and in peace support and humanitarian operations. With regard to external military threats to the country, foreign intelligence work is to be considered part of the tasks of the Swedish Armed Forces in peacetime, in preparedness, and at war. Foreign intelligence is to provide background data for the Swedish Armed Forces' preparedness, operational activities and military capabilities, and for the development of the wartime order of battle and the upgrading of defence equipment (see p. 9 and 14). The *travaux préparatoires* also clarify that support for Swedish foreign, defence and security policy includes involvement in Swedish participation in international security cooperation and reinforcing society during serious peacetime emergencies (see p. 19).

72. The Government therefore holds that the references in the Foreign Intelligence Act to "external military threats to the country" and "support[ing] foreign, defence and security policy", together with the interpretative clarifications in the *travaux préparatoires* to the Act, gave the general public an adequate indication of the circumstances in which the National Defence Radio Establishment was empowered to conduct signals intelligence during this period (compare and contrast *Iordachi and Others v. Moldova,* no. 25198/02, § 46, 10 February 2009). The Government holds that no further clarification can reasonably be required in the context of signals intelligence (cf. *Kennedy v. United Kingdom,* cited above, §§ 159–160 and paras. 24 and 65–66 above).

(2) The conditions for how signals intelligence could be executed by the National Defence Radio Establishment

73. In respect of the duration of any secret surveillance measure, the Court has held that in the context of national security, the scale of the activities involved is such that their planning often takes some time, and the Court is therefore of the view that the overall duration of any interception measures will depend on the

complexity and duration of the investigation in question and, provided that adequate safeguards exist, it is not unreasonable to leave this matter for the discretion of the relevant domestic authorities (*Kennedy v. the United Kingdom*, cited above, § 161). In the Government's view, such considerations are even more relevant as concerns signals intelligence within foreign intelligence. In foreign intelligence, the periods of surveillance are by necessity often long in order to make it possible to monitor a certain phenomenon that is relevant to the objectives of signals intelligence work (see paras. 20–24 above).[20] It is often necessary to observe phenomena over time in order to detect changes in patterns that could constitute a threat to national security.

74. Turning to the present case, it is pertinent to reiterate that under the Foreign Intelligence Act, the Government determines the tasking directives for all foreign intelligence work on an annual basis (see para. 32 above). In this context it may also be recalled that the Government's tasking directives are subject to subsequent parliamentary scrutiny functions, e.g. the Swedish National Audit Office and the parliamentary checks exercised by the Riksdag Committee on the Constitution (see para. 33 above). Moreover, the Government's tasking directives, as well as the more detailed tasking directives given by those commissioning the intelligence, are official documents and thus subject to the principle of public access to official documents (see paras. 26–30 above). Furthermore, the Government would like to reiterate that the National Defence Radio Establishment had a responsibility to examine whether the tasking directives were in accordance with the law before measures were initiated; the Establishment could not enforce tasking directives that contravened the law (see para. 34 above).

75. Concerning the procedure to be followed when examining, using and storing the data obtained, the Government once again reiterates that during this period too, foreign intelligence exclusively targeted foreign circumstances. In addition, the National Defence Radio Establishment was at that time, as now, only allowed to process personal data in its foreign intelligence activities if this was necessary for conducting foreign intelligence as laid out in the Foreign Intelligence Act. Furthermore, information about a person could only be processed if the person was related to the detailed tasking directives of foreign intelligence and the processing was necessary to fulfil those objectives

[20] Cf. the Venice Commission's report "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies", paras. 19 and 109.

(Chapter 1, Section 8 of the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment); see further paras. 46–47 and paras. 53–54 of the Government's observations on admissibility. In this context, it may also be reiterated that a procedure was in place for security clearance of staff of the National Defence Radio Establishment and various restrictions on access to data meant that, in practice, the data processed at the National Defence Radio Establishment was only accessible to a limited number of people (see para. 39 above). The need for protection of privacy thus coincided with the need to protect the intelligence work.

76. Furthermore, during this time period, the Swedish Intelligence Commission, which was established in 1976, had the responsibility of monitoring the intelligence work conducted by, *inter alia*, the National Defence Radio Establishment (Section 1 of the Ordinance containing instructions for the Swedish Intelligence Commission, 2007:852).

77. 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); see further paras. 49–52 of the Government's observations on admissibility.

78. With regard to the precautions to be taken when communicating data to other parties, the Government would like to put forward the following. As stated above, the National Defence Radio Establishment reported to Swedish principals and relevant government agencies in accordance with the legislation. Analyses of threats and assessments in intelligence matters were to be reported to the Government Offices (*Regeringskansliet*) and other relevant agencies. International cooperation could be conducted in accordance with the Foreign Intelligence Act and the Foreign Intelligence Ordinance. It may be recalled that the information passed on by agencies to other countries must not be detrimental to Swedish interests (see paras. 42–43 of the Government's observations on admissibility). Furthermore, the legislation on secrecy and on processing of personal data

regulated the extent to which reports could be provided to other Swedish or foreign government agencies and thus served as limitations on the possibility to communicate data to other parties (see paras. 42–43 above).

79. With respect to the circumstances in which information and data may or must be erased, the Government would like to recall that personal data that has not been processed in accordance with the legislation or regulations issued shall, at the request of the person whose data has been recorded, be corrected, blocked or deleted at the earliest opportunity by the National Defence Radio Establishment (Chapter 2, Section 4 of the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment). A decision by the National Defence Radio Establishment on rectification can be appealed to an ordinary administrative court (Chapter 6, Section 3). Consequently, there is the possibility of scrutiny by a court, the decision of which is subject to appeal.

80. With reference to what has been submitted in paras. 73–79 above, the Government holds that the legislation, which was set out in a form accessible to the public, indicated with sufficient clarity – so as to provide adequate protection against abuse of power – the conditions for how signals intelligence could be executed by the National Defence Radio Establishment during this time period.

(3) Conclusion

81. The Government recalls that the Contracting States enjoy a fairly wide margin of appreciation in assessing the existence and extent of the necessity of an interference, as well as in choosing the means for achieving the legitimate aim of protecting national security. The Government holds that, in view of all the circumstances of the case – such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law – the legislation governing signals intelligence conducted by the National Defence Radio Establishment during the first time period was such as to keep the "interference" to what was "necessary in a democratic society".

82. To sum up, the Government therefore holds that Swedish legislation concerning signals intelligence complied with the requirements of minimum legislative safeguards and of supervision of the regime during this time period. Consequently, the possible interference with the applicant firm's right under Article 8 § 1 was in accordance with the law and necessary in terms of Article 8 § 2 of the Convention.

Second time period

83. The 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 previously (see paras. 4 and 36 above), collection from cables was not possible until after 1 December 2009, i.e. as from the third time period, when the regulation concerning the obligation on the part of the cable owners to make traffic available entered into force.

(1) The circumstances in which the National Defence Radio Establishment was empowered to conduct signals intelligence

84. To cover the full complexity of the spectrum of threats – with significant elements of non-military and non-armed threats – and in order to respond to the altered threat scenario against Sweden, foreign intelligence was defined during this time period as being able to identify *external threats to the country*, irrespective of their nature or origin (Section 1 of the Foreign Intelligence Act); see paras. 56–57 of the Government's observations on admissibility.

85. Additional clarification on the term "external threats to the country" was provided in the *travaux préparatoires* to, *inter alia*, the Signals Intelligence Act and to the amendments of the Foreign Intelligence Act (Government Bill 2006/07:63). This term 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.

86. Foreign intelligence has always targeted foreign circumstances, but the legislator found it appropriate to clarify the law on this point as from the second time period. Accordingly, foreign intelligence was expressly limited to foreign circumstances. 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.

87. Moreover, the purposes for which signals intelligence could be conducted were clarified and defined in the Foreign Intelligence Act and in Section 2 of the Signals Intelligence Ordinance (2008:923); see para. 24 of the Government's

further observations on admissibility. According to Section 2 of the Ordinance, signals intelligence was allowed for the following purposes: 1. external military threats to the country; 2. circumstances of relevance to Swedish participation in international peace support and humanitarian operations and threats to Swedish personnel or other Swedish interests during ongoing operations; 3. strategic circumstances concerning international terrorism or other serious international crime that may threaten essential national interests; 4. the development and proliferation of weapons of mass destruction and military equipment; 5. external threats to society's technical infrastructure; 6. conflicts abroad with consequences for international security; and 7. other international phenomena of significance to Swedish foreign, security and defence policy.

88. Against this backdrop the Government holds that the reference in the Foreign Intelligence Act to "external threats to the country", together with the interpretative clarifications in the *travaux préparatoires* to that Act and to the Signals Intelligence Act, as well as Section 2 of the Signals Intelligence Ordinance, sufficiently clarified the purposes for which signals intelligence could be conducted and gave the general public a clear indication of the circumstances in which the National Defence Radio Establishment was empowered to conduct signals intelligence during this time period (compare and contrast *Iordachi and Others v. Moldova,* cited above, § 46).

(2) The conditions for how signals intelligence could be executed by the National Defence Radio Establishment

89. The Signals Intelligence Act introduced a special permit procedure concerning signals intelligence within foreign intelligence, and a new court-like permit authority was established – the Signals Intelligence Board (*Signalspaningsnämnden*). A permit was required for the agencies designated by the Government in order to decide on the detailed tasking directives of signals intelligence. A permit was valid for a maximum of six months and could be extended for a maximum of six months at a time after renewed examination. The scope of the renewed examination had to be adapted to what the permit covered, the results of signals collection thus far, and any new circumstances of relevance to the examination (see further paras. 55 and 61–62 of the Government's observations on admissibility).

90. It appears that the applicant firm has reached the conclusion that the limit on the duration satisfies the minimum safeguards in this respect (see para. 69 in the applicant firm's complaint to the Court, dated 14 July 2008).

91. For its part, and in view of the provisions on the duration of a permit described above, the Government holds that it is evident that the Signals Intelligence Act clearly stipulated, firstly, the period after which a permit would expire and, secondly, the conditions under which a permit could be renewed (cf. *Kennedy v. the United Kingdom*, cited above, § 161). When a permit was to be renewed, the Signals Intelligence Board had to examine the request for renewal and, upon such examination, the Board again had to satisfy itself that the permit remained necessary on the grounds stipulated in the legislation. The Government thus concludes that the provisions on duration and renewal are sufficiently clear.

92. As regards the procedure to be followed for examining, using and storing the data obtained, it may again be reiterated that collection from cables was not possible until after 1 December 2009, i.e. as from the third time period (see para. 58 of the Government's observations on admissibility). During this time period too, the National Defence Radio Establishment could only process personal data under certain conditions (see para. 75 above). Furthermore, it is important to keep in mind that tasking directives may not refer to a specific natural person. In certain cases, signals intelligence does indeed have to concern individuals' communications so as to make it possible to monitor a certain phenomenon that is relevant to the objectives of signals intelligence work. However, a signals intelligence collection assignment must not exclusively target a specific natural person (see further para. 60 of the Government's observations on admissibility).

93. Moreover, the Swedish Intelligence Commission was entrusted with the task of supervising the signals intelligence mandate. Selectors, destruction and reporting were to be examined in particular. 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 a tasking directive. The control function also covered, in particular, signals intelligence that could more obviously affect the privacy interests of individuals. The supervision furthermore included the selectors used by the National Defence Radio Establishment in its collection systems, in accordance with detailed tasking directives. 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 any other ways it deemed 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 with individuals' privacy. The Swedish Intelligence Commission was also to supervise that data was destroyed to the extent required by law and that 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 (see paras. 66–68 of the Government's observations on admissibility).

94. It is also relevant to reiterate that the Signals Intelligence Commission, through the Signals Intelligence Control Delegation (*Signalspaningskontroll-delegationen*), was authorised to order the discontinuation of a specific ongoing collection process and the destruction of the recordings or notes of data already collected (see further paras. 69–70 of the Government's observations on admissibility).

95. 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. The Council had, and still has, a special responsibility within the context of the Establishment's work to prevent signals intelligence – irrespective of the tasking 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 (see further para. 71 of the Government's observations on admissibility).

96. Although the permit requirement did not apply during this period to the Government's tasking directives (see para. 89 above), the National Defence Radio Establishment naturally had a responsibility to examine whether the tasking directives were in accordance with the law before measures were initiated; the Establishment could not enforce tasking directives that contravened the law (see para. 34 above). The responsibility of the National Defence Radio Establishment to determine the lawfulness of signals collection before it began naturally included checking that signals collection for the Government's own intelligence needs did not exclusively target a specific natural person. The Privacy Protection Council established during the second time period played – and still plays – an important role in ensuring that the activities were/are lawful.

97. In this context, it may also be recalled that a security clearance procedure for the staff of the National Defence Radio Establishment was in place and various restrictions on access to data meant that, in practice, the data processed at the National Defence Radio Establishment was only accessible to a limited number of people (see para. 39 above). The need for protection of privacy thus coincided with the need to protect the intelligence work.

98. With regard to the precautions to be taken when communicating data to other parties, the Government refers to the information submitted in para. 78 above.

99. Turning to the circumstances in which information and data may or must be erased, the Government recalls the following. 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 specific natural person and it is considered that it lacks importance for foreign intelligence requirements. This applies regardless of whether signals have been collected with the help of automated processing or by manual methods. 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. 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. Moreover, superfluous information concerning individuals that lacks relevance from a foreign intelligence perspective must not be reported (see para. 65 of the Government's observations on admissibility).

100. At this point, it is also relevant to reiterate that the Swedish Intelligence Commission was to supervise that data was destroyed to the extent required by law (para. 68 of the Government's observations on admissibility and para. 93 above), and that the Signals Intelligence Control Delegation was authorised to order that data collected be destroyed (see para. 69 of the Government's observations on admissibility and para. 94 above).

101. With reference to what has been submitted in paras. 89–100 above, the Government asserts that the legislation, which was set out in a form accessible to

the public, indicated with sufficient clarity – so as to provide adequate protection against abuse of power – the conditions for how signals intelligence could be executed by the National Defence Radio Establishment during this time period too.

(3) Conclusion

102. To sum up, and with reference to para. 81 above, the Government holds that Swedish legislation on signals intelligence complied with the requirements of minimum legislative safeguards and of supervision of the regime during this time period. Consequently, the possible interference with the applicant firm's right under Article 8 § 1 was in accordance with the law and necessary in terms of Article 8 § 2 of the Convention.

Third time period

103. Initially, the Government finds it relevant to inform the Court that, as from 1 January 2013, two additional authorities were empowered to determine the more detailed tasking directives of signals intelligence conducted by the National Defence Radio Establishment, namely the Swedish Security Service (*Säkerhetspolisen*) and the National Criminal Police (*Rikskriminalpolisen*); see Section 4 of the Signals Intelligence Act.[21] The new system aims to improve the possibilities for the Swedish Security Service and the National Criminal Police to obtain data about foreign circumstances at a strategic level concerning international terrorism and other serious international crime that may threaten essential national interests. The legislative amendment means that the entire regulatory framework that applies to signals intelligence within foreign intelligence work is also to be applied to tasking directives from the Swedish Security Service or the National Criminal Police.

104. It is also relevant to inform the Court that as from 1 January 2015, the National Police Board (*Rikspolisstyrelsen*) and the 21 police authorities, together with the National Laboratory of Forensic Science, was reorganised as a single agency, the Swedish Police Authority (*Polismyndigheten*). As part of the reorganisation of the police, the National Criminal Police changed its name to the Department of National Operations (*Nationella operativa avdelningen*). Further, the Swedish Security Service was reorganised into a separate authority, independent of the rest of the new Police Authority.

[21] It should be recalled that the Swedish Security Service and the National Criminal Police could determine the more detailed tasking directives of signals intelligence conducted by the National Defence Radio Establishment during the first two time periods.

105. To sum up, within the framework of the Government's annual tasking directive for all foreign intelligence work, the detailed tasking directives of signals intelligence conducted by the National Defence Radio Establishment may currently be determined by the Government, the Government Offices, the Swedish Armed Forces, the Department of National Operations within the Police Authority and the Swedish Security Service (Section 1 of the Foreign Intelligence Act and Section 4 of the Signals Intelligence Act).

106. Furthermore, the Government finds it pertinent to stress that the fact that two additional authorities can determine the detailed tasking directives of signals intelligence does not in any way entail an amendment of the purposes for, or the conditions on, which signals intelligence may be conducted by the National Defence Radio Establishment.[22] There are certain basic principles concerning the demarcation between foreign intelligence and investigation of crime (see further Government Bill 2006/07: 63, Section 6.3.2. and p. 108). Thus, as the Government has previously emphasised, signals intelligence may not be used to collect information for use in investigating crime. Measures for the investigation of crime, for example covert interception and surveillance of electronic communications, are regulated in other legislation, for example Chapter 27 of the Swedish Code of Judicial Procedure.

(1) The circumstances in which the National Defence Radio Establishment is empowered to conduct signals intelligence

107. 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 work 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 (see para. 74 of the Government's observations on admissibility; cf. para. 87 above).

[22] See also para. 49 in the Government's further observations on admissibility.

108. It is also pertinent to reiterate that as from the third time period, signals intelligence conducted by the National Defence Radio Establishment may *not* target domestic traffic (signals between a sender and a recipient who are both located in Sweden). Signals may be collected from electronic communications cables that cross the Swedish border. For network configuration reasons, domestic traffic could also cross the national border, and 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 of the amended Signals Intelligence Act); see paras. 18 and 75 of the Government's observations on admissibility.

109. Against this backdrop, the Government holds that it is clear that the amended Signals Intelligence Act sufficiently clarifies the purposes for which signals intelligence can be conducted, and that it is beyond doubt that the legislation gives the general public a clear indication of the circumstances in which the National Defence Radio Establishment is empowered to conduct signals intelligence as from the third time period.

(2) The conditions for how signals intelligence may be executed by the National Defence Radio Establishment

110. As regards the limit on the duration of the surveillance, the Government would like to put forward the following. As from the third time period, any signals intelligence conducted by the National Defence Radio Establishment requires a permit from the Foreign Intelligence Court. A permit for signals intelligence is valid for a maximum of six months and can be extended for a maximum of six months at a time after renewed examination (Section 5 a of the amended Signals Intelligence Act); see also paras. 61–62 of the Government's observations on admissibility. In view of this, the Government concludes that the provisions on duration and renewal are sufficiently clear (cf. paras. 90–91 above).

111. Turning to the procedure to be followed for examining, using and storing the data obtained, it may be stressed that the rights of individuals have been strengthened as from the third time period. Firstly, an individual must be notified if, during signals intelligence, selectors have been used that directly pertain to him or her, unless secrecy applies to the information. Further, the Swedish Foreign Intelligence Inspectorate must check, at the request of an individual, whether his or her communications have been the subject of signals intelligence (see further paras. 122, 148 and 150 below).

112. Moreover it is relevant to recall that 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 selector 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 of people's 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 (see further paras. 37–38 and 76 of the Government's observations on admissibility).

113. As stated above, any signals intelligence collection 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 (see further para. 77 of the Government's observations on admissibility).

114. 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' refers 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 also 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 Foreign Intelligence Court to determine the level on which selectors must be described (see para. 78 of the Government's observations on admissibility).

115. 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 interference with privacy in connection with the signals collection (see para. 79 of the Government's observations on admissibility).

116. 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 greater detail in the Signals Intelligence Act. In addition, the examination is to ensure that the collection assignment is not in any other way incompatible with the legislation. This includes checking that tasking directives form the basis of the application. The National Defence Radio Establishment also has to provide the Foreign Intelligence Court with information in these regards. 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 interference with privacy (see para. 80 of the Government's observations on admissibility).

117. A proportionality assessment is to be carried out by the Foreign Intelligence Court, in which the value of the information expected from a collection assignment is to be placed in relation to the interference with privacy that it may entail. When assessing interference with 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. 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 of the amended Signals Intelligence Act); see para. 81 of the Government's observations on admissibility. Moreover, 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 rather individuals' interests in general in the proportionality assessment. The privacy protection representative is permitted to see the material in the case file (see para. 85 of the Government's observations on admissibility).

118. 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 Foreign Intelligence Court finds this necessary (see para. 82 of the Government's observations on admissibility).

119. As has been mentioned, a collection assignment may not exclusively target a specific natural person. In such cases, a permit may not be issued by the Court. Furthermore, the Court may issue conditions that are needed to limit the interference with the privacy of individuals. The conditions that are relevant depend on what the collection assignment refers to (see para. 83 of the Government's observations on admissibility).

120. Moreover, it may be recalled that the Swedish Foreign Intelligence Inspectorate is responsible for controlling signals intelligence and is, in particular, to scrutinise selectors, destruction of data and reporting. 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. That said, the Inspectorate is of course to ensure that the Court's decisions are followed (see para. 89 of the Government's observations on admissibility). The Inspectorate has a mandate to terminate collection and/or order destruction of recordings or notes if it is shown that they are collected in a way that is incompatible with the permit issued by the Foreign Intelligence Court (see para. 51 above).

121. 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 (see para. 90 of the Government's observations on admissibility).

122. Further, as stated above, the Swedish Foreign Intelligence Inspectorate is to check, at the request of an individual, whether his or her communications have 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 (*Datainspektionen*), the Office of the Chancellor of Justice (*Justitiekanslern*) or the Office of the Prosecutor-General (*Riksåklagaren*) at the Swedish Prosecution Authority (*Åklagarmyndigheten*); see para. 91 of the Government's observations on admissibility. The Inspectorate's supervisory and investigatory functions compensate for the fact that, due to secrecy, individuals cannot adequately benefit from the protection of privacy provided for in the provisions on notification and rectification etc. This supervision and duty to investigate therefore serve as an extra control mechanism, intended to protect the privacy of individuals against violations in the processing of personal data and against improper signals collection.

123. Moreover, it may be reiterated that a security clearance procedure for the staff of the National Defence Radio Establishment is in place and various restrictions on access to data mean that, in practice, the data processed at the National Defence Radio Establishment is only accessible to a limited number of people (see para. 39 above). The need for protection of privacy thus coincides with the need to protect the intelligence work.

124. As regards the precautions to be taken when communicating the data to other parties, the Government refers to para. 78 above.

125. As concerns the circumstances in which information must be erased, the Government refers to para. 99 above. It may further be reiterated that the requirement that signals intelligence at the National Defence Radio Establishment may *not* target domestic traffic 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 of the Signals Intelligence Act); see para. 108 above and paras. 18, 75 and 92 of the Government's observations on admissibility. Protection of privacy is thus safeguarded through the obligation to destroy data and supervision of compliance with this obligation. Furthermore, data in the form of unprocessed raw material that is part of a data collection *must* be deleted no later than one year after the processing of the data began (Section 2 of the Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment, 2007:261). The deletion of this personal data is final (Section 12 of the same ordinance); see para. 96 of the Government's observations on admissibility. Finally, as stated above, the Swedish Foreign Intelligence Inspectorate is to scrutinise, in particular, the destruction of data.

126. At this juncture, it should be emphasised that the annual reports of the Swedish Foreign Intelligence Inspectorate testify to the fact that there is no evidence of any breaches of the regulations concerning signals intelligence or any deliberate abuse of signals intelligence by the National Defence Radio Establishment. Moreover, the opinions submitted by the Inspectorate in the course of its supervising activities have been adhered to by the National Defence Radio Establishment, and are rather a sign that the supervision is effective. It is also worth emphasising that the Swedish Foreign Intelligence Inspectorate has the mandate to examine any complaint of unlawful interception, and that none of its checks have shown that improper signals collection has taken place (cf. *Kennedy v. the United Kingdom*, cited above, §§ 167–168).

127. With reference to what has been submitted in paras. 110–126 above, the Government holds that the legislation, which is set out in a form accessible to the public, indicates with sufficient clarity – so as to provide adequate protection against abuse of power – the conditions for how signals intelligence may be executed by the National Defence Radio Establishment with respect to this time period too.

(3) Conclusion

128. To sum up, and with reference to para. 81 above, the Government holds that Swedish legislation on signals intelligence complies with the requirements of minimum legislative safeguards and of supervision of the regime also with respect to this time period. Consequently, the possible interference with the applicant firm's right under Article 8 § 1 is in accordance with the law and necessary in terms of Article 8 § 2 of the Convention.

Conclusion

129. For the reasons set out in paras. 60–128 above, the Government holds that the possible interference with the applicant firm's right under Article 8 was – during all three time periods – subject to significant limitations and was accompanied by effective and adequate safeguards against abuse as well as supervision of the regime. The possible interference was thus not disproportionate to the legitimate aim pursued. Therefore, the possible interference should be regarded as "in accordance with the law" and "necessary in a democratic society" within the meaning of Article 8 § 2 of the Convention. Consequently, there has been no violation of Article 8 of the Convention during any of the three time periods and the applicant firm's complaint regarding Article 8 should be declared inadmissible as being manifestly ill-founded.

Article 13

130. The applicant firm complains that it has not had any effective domestic remedy through which it could challenge the breach of its rights under Article 8 of the Convention during any of the three time periods. Thus, the applicant firm claims that its rights under Article 13 of the Convention have been and continue to be violated.

131. The Court has asked whether the applicant firm's concerns about secret surveillance measures being applied to it have required that it has access to an effective remedy within the meaning of Article 13 of the Convention, and, if so, whether the applicant firm has had an effective remedy at its disposal.

132. At this juncture, the Government finds it relevant to reiterate that Swedish tort law has been developed in case-law as regards compensation for actions involving violations of fundamental rights and freedoms (see paras. 111–118 of the Government's observations on admissibility).

133. In this connection, it is appropriate to stress that the Court has referred to the case-law established by the Swedish Supreme Court and the Chancellor of Justice over recent years and their continued development of case-law in this domain. The Court has on these grounds considered that there exists an effective remedy in Sweden that is capable of affording redress in respect of alleged violations of the Convention (see *Eriksson v. Sweden*, no. 60437/08, §§ 50–52, 12 April 2012; *Ruminski v. Sweden* (dec.), no. 10404/10, §§ 37 and 39, 21 May 2013; *Marinkovic v. Sweden* (dec.), no. 43570/10, §§ 39 and 41, 10 December 2013, and *Johansson Prakt and Salezhade v. Sweden* (dec.), no. 8610/11, §§ 52–60 and 70, 16 December 2014).

Applicability of Article 13 and requirements of access to an effective remedy

134. According to the Court's case-law, Article 13 applies only where an individual has an "arguable claim" to be the victim of a violation of a Convention right (see *Boyle and Rice v. the United Kingdom*, nos. 9659/82; 9658/82, § 52, 27 April 1988; *Voyager Limited v.* Turkey (dec.), no. 35045/97, 4 September 2001; *Ivison v. the United Kingdom* (dec.), no. 39030/97, 16 April 2002; *Petersen v. Germany* (dec.), nos. 38282/97 and 68891/01, 12 January 2006; and *Weber and Saravia v. Germany*, cited above, § 155).

135. In view of this, the Government initially contends that it takes more than mere *concerns* that it has been subjected to signals intelligence for the applicant firm to establish an arguable claim for the purposes of Article 13. Further, the

Government would like to reiterate that it considers that the applicant firm cannot claim to be a victim of a violation of Article 8 occasioned by the mere existence of Swedish legislation concerning signals intelligence during any of the three time periods (see para. 11 above). Consequently, the Government holds that the applicant firm has no arguable claim for the purposes of Article 13 concerning any of the three time periods.

136. If the Court were to find that the applicant firm can claim to be a victim of a violation of Article 8, the Government holds that it does not follow automatically from such a finding that it has an arguable claim for the purposes of Article 13. This conclusion is supported by the case of *Weber and Saravia v. Germany*, cited above, in which the Court found that there was an interference with the applicants' rights under Article 8, but that they did not have an arguable claim for the purposes of Article 13. For its part, the Government thus holds that even if the Court were to find that the applicant firm can claim to be a victim of a violation of Article 8, it has no arguable claim for the purposes of Article 13 concerning any of the three time periods.

137. It therefore follows that Article 13 is not applicable in the present case with respect to any of the three time periods. Consequently, the applicant firm's complaint in this part should be declared inadmissible *ratione materiae* concerning all three time periods.

138. If the Court were to find that the applicant firm has an arguable claim for the purposes of Article 13 of the Convention as regards any of the three time periods, the Government would like to emphasise once again that the present complaint concerns the review of the relevant legislation *in abstracto.* In this context, the Government refers to the Court's case-law, according to which 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 (see *Leander v. Sweden,* no. 9248/81*,* § 77(d)), 26 March 1987). Consequently, the fact that there is no constitutional court in Sweden before which the applicant firm could challenge the law *in abstracto* does not entail a violation of Article 13 of the Convention. Indeed, with regard to a complaint on legislation *in abstracto*, Article 13 does not require the law to provide an effective remedy where the alleged violation arises from primary legislation (*Kennedy v. the United Kingdom,* cited above, § 197). Accordingly, the Government holds that the Court's examination under Article 13 should, as in the case of *Kennedy*, terminate already at this stage with the conclusion that there has been no violation of Article 13 in the present case,

since the applicant firm complains about the signals intelligence regime – which is set out in primary law – *in abstracto*.

139. In view of this, and in reply to the Court's question, the Government contends that the applicant firm's *concerns* about being subjected to signals intelligence have not required that it should have access to an effective remedy within the meaning of Article 13 during any of the three time periods.

140. Nevertheless, if the Court were not to conclude its examination there, the Government holds that the applicant firm has had effective remedies at its disposal during all three time periods. The reasons for this contention will be elaborated on below.

The availability of effective remedies

141. Where an individual does have an arguable claim to be the victim of a violation of the rights set forth in the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress. An effective remedy under Article 13 may not necessarily in all instances be a judicial authority in the strict sense. Furthermore, although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so (see *Klass and Others v. Germany*, cited above, § 67, *Leander v. Sweden*, cited above, § 77 and *Nada v. Switzerland*, [GC], no. 10593/08, § 207, ECHR 2012).

142. According to the Court's case-law in the context of secret surveillance measures, an effective remedy under Article 13 means a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in such a system (see *Klass and Others v. Germany*, § 69; *mutatis mutandis*, *Leander v. Sweden*, § 78 *in fine*, both cited above; and *Mersch and Others v. Luxembourg,* nos. 10439–41/83, 10452/83, 10512/83 and 10513/83, Commission decision of 10 May 1985, Decisions and Reports (DR) 43, p. 34, at p. 118, and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, cited above, § 99).

143. In view of the above, the Court's task in the present case is therefore to examine the various remedies available to the applicant firm under Swedish law, in order to see whether they are effective in this limited sense (cf. *Klass and Others v. Germany*, cited above, § 69).

144. Moreover it is relevant to note that the Court, in the context of secret surveillance measures, has in several cases reached the conclusion that the absence of notification to the person concerned while surveillance is in progress

is compatible with Article 8 in order to ensure the efficacy of surveillance measures. When subsequently examining the existence of effective remedies under Article 13, the Court has held that it cannot interpret or apply Article 13 so as to arrive at a result tantamount to nullifying its conclusion under Article 8, since the Convention is to be read as a whole, and that any interpretation of Article 13 must therefore be in harmony with the logic of the Convention (see *Klass and Others v. Germany*, § 68 and, *mutatis mutandis*, *Leander v. Sweden*, § 78, cf. *Mersch and Others v. Luxembourg*, p. 118, all cited above). In those cases, the Court has consequently found that the lack of, *inter alia*, notification of secret surveillance measures while in progress did not entail a breach of Article 13.

145. It is furthermore relevant to recall that according to the legislation at issue in the case of *Klass and Others v. Germany*, the competent authority was bound to inform the person concerned as soon as the surveillance measures were discontinued and *notification could be made without jeopardising the purpose of the restriction* (ibid., §§ 11, 19 and 71). The Court found that from the moment of such notification, various legal remedies became available to the individual in that case.

146. Turning to the facts of the present case, the Government initially wishes to refer to the description of remedies outlined in the Government's observations on admissibility. In particular, the Government wishes to draw the Court's attention to the following.

147. 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 (see para. 53 of the Government's observations on admissibility). This right to obtain information has been applicable during all three time periods.

148. Furthermore, as from the third time period, the Swedish Foreign Intelligence Inspectorate is to check, at the request of an individual (including businesses and organisations), whether the requesting party's communications have been the subject of signals intelligence (cf. *Kennedy v. the United Kingdom*, cited above, § 167). Following the check, the requesting party must be informed

whether or not any improper signals collection has taken place.[23] If evidence of improper signals collection is found, this must be reported to the requesting party 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 at the Swedish Prosecution Authority (see para. 122 above). If, in the course of its supervision, the Swedish Foreign Intelligence Inspectorate notices circumstances that may constitute a criminal offence, the Inspectorate shall report this to the Swedish Prosecution Authority (Prosecutor-General). If an offence has been committed, a prosecutor may initiate a preliminary investigation (Chapter 23, Section 1 of the Swedish Code of Judicial Procedure) and must thereafter – if the conditions are met – prosecute the offence (Chapter 20, Section 6 of the Swedish Code of Judicial Procedure). If the Swedish Foreign Intelligence Inspectorate notices any irregularities that may entail liability for the state towards a natural or legal person, the Inspectorate is to report this to the Office of the Chancellor of Justice. It is the Office of the Chancellor of Justice that handles claims for damages under Chapter 2, Section 5 of the Act on Processing of Personal Data in the National Defence Radio Establishment's Foreign Intelligence and Development Operations (see Section 3 of the Ordinance on processing claims for damages against the state, 1995:1301). If the Swedish Foreign Intelligence Inspectorate discovers circumstances that should be brought to the attention of the Data Inspection Board, the Inspectorate shall report this to the Board. Under Section 1 of the Ordinance concerning the duties of the Data Inspection Board (2007:975), the Board is responsible for working to ensure that people are protected against violations of their privacy via processing of personal data.

149. In addition, it is relevant to note that as from the third time period, the National Defence Radio Establishment is required to notify an individual if selectors have been used in signals intelligence that directly pertain to him or her, unless secrecy applies (see further paras. 93–95 of the Government's observation on admissibility and para. 16 of the Government's further observations on admissibility).

150. During all three time periods, the National Defence Radio Establishment has been – and still is – obliged, at the request of the person whose data has been recorded, to correct, block or delete at the earliest opportunity personal data that

[23] Cf. the Venice Commission's report "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies", para. 138.

has not been processed in accordance with the legislation or regulations issued (Chapter 2, Section 4 of the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment). 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). Accordingly, even if the individual concerned will not receive the information or documents requested, there is the possibility of scrutiny by a court, the decision of which is subject to appeal.

151. Moreover, during the second time period, the Signals Intelligence Control Delegation had 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. The measures that the Delegation was authorised to order included the discontinuation of a specific ongoing collection process and the destruction of the recordings or notes of data already collected (see para. 69 of the Government's observation on admissibility). As from the third time period, the Swedish Foreign Intelligence Inspectorate has a mandate to terminate collection and/or order destruction of recordings or notes if it is shown that they are collected in a way that is incompatible with the permit issued by the Foreign Intelligence Court (see paras. 51 and 120 above).

152. As from the third time period, the Swedish Foreign Intelligence Inspectorate has the task of supervising that the foreign intelligence work conducted by, *inter alia*, the National Defence Radio Establishment, is in accordance with primary and secondary legislation (acts and ordinances). The Swedish Foreign Intelligence Inspectorate is to ensure that the Foreign Intelligence Court's decisions are followed and to monitor, in particular, selectors, destruction of data and reporting. 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. Data that is of a superfluous nature is covered by the obligation to destroy data (see paras. 89, 90 and 92 of the Government's observations on admissibility).

153. Furthermore, during all three time periods an individual has had the possibility to apply to the Parliamentary Ombudsmen (*Riksdagens ombudsmän*); see paras. 98–100 and 132 of the Government's observations on admissibility, the Chancellor of Justice (see ibid. paras. 101–102 and 132) or the Data Inspection Board (see ibid. paras. 103 and 133), the possibility to bring an action for damages (see ibid. paras. 104–109 and 133), the possibility to report a matter for

prosecution (see ibid. paras. 110 and 133) and the possibility to bring a claim for compensation for violations of the Convention (see paras. 132–133 above).

154. Moreover, as stated above, the principle of public access to official documents applies to foreign intelligence work and thus to the signals intelligence conducted by the National Defence Radio Establishment (see paras. 25–30 above). 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 (see para. 54 of the Government's observations on admissibility). Accordingly, even if the individual concerned does not receive the information or documents requested, there is the possibility of scrutiny by a court, the decision of which is subject to appeal.

155. To sum up, several remedies have been and are open to an individual believing himself to be subjected to signals intelligence. In the Government's view, it is hard to conceive of more effective remedies being possible in the context of signals intelligence within foreign intelligence, especially while it is in progress (cf. *Klass and Other v. Germany*, cited above, §§ 70–71 and cf. *Segerstedt-Wiberg v. Sweden*, no. 62332/00, § 120, 6 June 2006).

156. Thus, the Government holds that the present case differs from the case of *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, cited above, in which Bulgarian law did not provide any notification mechanisms at any point in time and, in fact, the individual was never and under no circumstances appraised of the fact that his or her communications had been monitored (ibid. §§ 100–101). In addition, also in contrast to the Bulgarian law at issue in that case, the Government holds that there existed, during all three time periods, a sufficiently effective apparatus for controlling the use of secret surveillance measures (see further paras. 48–54, 66–71, 88–118 and 129–144 of the Government's observations on admissibility; cf. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, § 100). At this juncture, the Government finds it relevant to stress that according to the legislation at issue in the case of *Klass and Others v. Germany*, cited above, notification was to be made only *if it could be made without jeopardizing the purpose of the surveillance measure* (see *Klass,* § 71 and *Weber and Saravia v. Germany*, cited above, §§ 51 and 135–136). Accordingly, the obligation to make a notification was not absolute.

157. Furthermore, the present case is, in the Government's view, not comparable to the case of *Segerstedt-Wiberg v. Sweden*, cited above, in which the Court found that the aggregate of remedies were not sufficient to satisfy the

requirements of Article 13. In that case, the applicants complained that the storage in the Security Service files of certain information that had been released to them constituted unjustified interference with their rights under Articles 8, 10 and 11. Under those Articles, they further complained of the refusal to advise them of the full extent to which information concerning them was kept on the Security Service register (ibid. § 3). In the case of *Segerstedt-Wiberg*, the assessment for the Court to make under Article 13 was thus whether the applicants, in those circumstances, had remedies at their disposal that would entail an examination of whether they had the right to be further advised on which information concerning them was kept on the Security Service register and whether stored information should be destroyed. Thus, in *Segerstedt-Wiberg*, there were two specific grievances that the remedies examined had to redress. In contrast, in the present case, where the Court is called upon to make an *in abstracto* assessment of certain legislation, it cannot be required that the available domestic remedies must attain the same level of specificity or be directed at redressing a certain grievance (cf. *mutatis mutandis*, *Kennedy v. the United Kingdome*, cited above, § 155). Consequently, the fact that the Court in the case of *Segerstedt-Wiberg* did not find that the aggregate of domestic remedies were sufficient in that case is irrelevant for the assessment of the complaint concerning Article 13 in the present case.

158. To sum up, having regard to the inherent limitations in the context of signals intelligence within foreign intelligence, the Government holds that the aggregate of domestic remedies provided for under Swedish law satisfies the requirements of Article 13 during all three time periods (cf. *Leander v. Sweden*, cited above, § 84 and *Klass and Others v. Germany*, cited above, § 72).

Conclusion

159. With reference to what has been submitted in paragraphs 134–158 above, the Government holds that the applicant firm's concerns about being subjected to signals intelligence have not required that it should have access to an effective remedy within the meaning of Article 13 during any of the three time periods, and, in any event, that the applicant firm has had effective remedies at its disposal during all three time periods. Consequently, the case reveals no violation of Article 13 of the Convention and the applicant firm's complaint regarding Article 13 should be declared inadmissible as being manifestly ill-founded.

V. Conclusions

160. The position of the Swedish Government in this case is,

concerning the **admissibility,**

- that the application should be declared inadmissible
  - *ratione personae* since the applicant firm cannot claim to be a victim of a violation of the Convention, or
  - *ratione materiae* since neither Article 8, nor Article 13, are applicable,

and, in any event,

- as being manifestly ill-founded; and

concerning the **merits,**

- that the case reveals no violation of the Convention.

Gunilla Isaksson

Jessica Sjöstrand

Agents of the Swedish Government

Appendices

1. Relevant agencies
2. Relevant acts and ordinances
3. Signals intelligence process – illustrations (sent only by post)
4. 2014 Annual Report of the National Defence Radio Establishment