REGERINGSKANSLIET

Stockholm, 19 November 2015
UDFMR2012/144/ED

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

IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application no. 35252/08

Centrum för rättvisa

v.

Sweden

FURTHER OBSERVATIONS OF THE GOVERNMENT OF SWEDEN – INCLUDING COMMENTS ON THE APPLICANT'S CLAIMS FOR JUST SATISFACTION

Introduction

1. These further observations on the admissibility and merits of the application introduced by Centrum för rättvisa (hereinafter 'the applicant firm'), including comments on the applicant firm's claims for just satisfaction, are submitted on behalf of the Swedish Government in response to the Court's letter of 11 September 2015, in which the Government is invited to submit comments concerning the applicant firm's claims for just satisfaction and any further observations it wishes to make.

Initial remarks

2. Unless otherwise stated, in these observations the Government refers to Swedish legislation on signals intelligence within foreign intelligence applicable during the third time period.

3. At the outset, the Government finds it appropriate to once again reiterate that privacy protection, including protection for correspondence, enjoys explicit constitutional support in Chapter 2, Article 6 of the Instrument of Government. However, it has to be balanced against other societal interests and may have to yield to opposing interests of greater weight, albeit only if this is in accordance with Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. In other words, any interference must be in accordance with the law and necessary in a democratic society in the interests of, *inter alia,* national security. This level of careful consideration has been taken in the design of the Swedish legislation on signals intelligence (see Government communication 2011/12:48 p. 26, cf. paras. 2 and 18 of the Government's observations of 25 January 2013).

4. In this context, the Government would also like to recall the significance of the principle of subsidiarity. An important aspect of this principle is that the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights (cf. para. 3 of the Government's observations of 25 January 2013).

5. Furthermore, and in response to what the applicant firm has stated under the heading 'The case in a larger context' in its observations of 31 August 2015 (paras. 1–7), the Government finds it pertinent to emphasise that the present case exclusively concerns Swedish legislation on signals intelligence within foreign intelligence. Hence, intelligence operations in, *inter alia*, the United States and Germany give no guidance as to how and to what extent

signals intelligence within foreign intelligence is conducted in Sweden (cf. paras. 5–6, 16–17 and 41 of the applicant firm's observations of 31 August 2015).

6. Accordingly, the Government holds that the judgment of the Court of Justice of the European Union in the case of *Digital Rights v. Ireland* and the judgment of the United States Court of Appeals for the second circuit in the case of *ACLU v. Clapper*, to which the applicant firm refers, are irrelevant when considering the present application.

7. At this point, the Government furthermore finds it important to stress that foreign intelligence work is conducted for the purpose of supporting Swedish foreign, security and defence policy and for the purpose of protecting the security of the realm. The signals intelligence work conducted by the National Defence Radio Establishment constitutes a vital part of Sweden's foreign intelligence work. The aim of the signals intelligence work conducted by the Establishment is to obtain strategic information and identify phenomena of relevance to foreign intelligence. Consequently, the periods of signals intelligence 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 of the Government's observations of 8 May 2015).

8. In line with what is stated above, the National Defence Radio Establishment is to provide warning of events and developments of significance to Sweden and Swedish foreign, security and defence policy and otherwise identify external threats to the country. Hence, the Establishment provides information on conditions abroad to, essentially, the Government and the government agencies from which it receives tasking directives. Such information might include the espionage operations of a foreign power targeting Swedish interests, military capabilities in other countries, developments in certain regions in war and conflict, support to Swedish military operations abroad or information on international terrorism. The National Defence Radio Establishment's intelligence reports may also concern such subjects as, for example, the production, dissemination and use of weapons of mass destruction abroad, and serious external threats to the Swedish society's infrastructure.

9. As previously stated, 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 insight into the activities, even in the very long term. The need to keep secret the methods, capabilities and results, for

example, applies for a very long time (see para. 11 of the Government's observations of 27 April 2012 and paras. 25 and 28–29 of the Government's observations of 8 May 2015). However, this fact is balanced by clear and accessible legislation as well as a judicial permit procedure and effective and efficient control mechanisms, in particular through the Swedish Foreign Intelligence Inspectorate.

10. In this context it is also relevant to reiterate that the Signals Intelligence Committee (a parliamentary committee) has reviewed the signals intelligence work conducted by the National Defence Radio Establishment from 2009 until the end of 2011 (see its report *Uppföljning av signalspaningslagen, SOU 2011:13*; hereinafter 'the Signals Intelligence Committee Report'). Furthermore, the Data Inspection Board was tasked by the Government with following the processing of personal data at the National Defence Radio Establishment during 2009 and 2010 (see its report *Datainspektionens redovisning av regeringsuppdraget Fö2009/00355/SUND*). Moreover, the Swedish Foreign Intelligence Inspectorate reports annually to the Government on its supervision of, *inter alia*, the National Defence Radio Establishment[1]. In addition, the Government is required to report annually to the Riksdag on the review of the activities conducted under the Signals Intelligence Act. The report is submitted in a special written communication from the Government to the Riksdag (*regeringens skrivelse*). These temporary and recurrent reviews promote transparency and serve to elucidate the signals intelligence work conducted by the National Defence Radio Establishment as far as possible considering the need for strict secrecy (cf. paras. 16–20 and 33 of the applicant firm's observations of 31 August 2015).

11. It is also worth reiterating that the amendments to the legislation on signals intelligence within foreign intelligence as from the third time period were made in order to further strengthen the protection of privacy (see paras. 73 and 96 of the Government's observations of 27 April 2012, para. 14 of the Government's observations of 25 January 2013 and para. 111 of the Government's observations of 8 may 2015; and cf. para. 8 of the applicant firm's observations of 31 August 2015).

12. Finally, and in response to the applicant firm's contention that the standards for the Swedish signals intelligence regime may vary depending on the ideology of the Government in power (see para. 7 of the applicant firm's

[1] See Section 5 of the Ordinance containing instructions for the Swedish Foreign Intelligence Inspectorate.

observations of 31 August 2015), the Government finds it sufficient to reply that Sweden is a parliamentary democracy.

Article 8

13. In its observations of 31 August 2015, the applicant firm has maintained that its rights under Article 8 of the Convention have been violated. However, the applicant firm has previously clarified that it does not contend that it has been the subject of secret surveillance measures, but rather that there might be a risk that such measures have been applied to it (see, *inter alia*, para. 95 of the applicant firm's application to the Court dated 14 July 2008, and para. 12 of the applicant firm's observations of 31 August 2012). Accordingly, the applicant firm has complained about the legislation *per se* and not on how it has been applied vis-à-vis the applicant firm. Thus, the applicant firm has asked the Court to undertake an *in abstracto* review of the Swedish legislation on signals intelligence within foreign intelligence (cf. para. 24 of the applicant firm's observations of 31 August 2015).

14. For its part, the Government firstly 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 paras. 5–10 of the Government's observations of 25 January 2013). Furthermore, with reference to what has been submitted in the Government's observations of 8 May 2015 (see paras. 16–128), the Government maintains – in relation to all three time periods – that the possible interference with the applicant firm's right under Article 8 was, and still is, subject to significant limitations and 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. Consequently, the possible interference should therefore be regarded as "in accordance with the law" and "necessary in a democratic society" within the meaning of Article 8 § 2 of the Convention.

15. The Government also maintains that the Contracting States enjoy a fairly wide margin of appreciation when assessing whether a possible interference is "necessary in a democratic society" in pursuit of a legitimate aim in the context of secret surveillance, and in choosing the means for achieving the legitimate aim of protecting national security (see *Klass and Others v. Germany*, no. 5029/71, §§ 49–50, 6 September 1978; *Weber and Saravia v. Germany*, (dec.), no. 54934/00, §§ 106 and 137, ECHR 2006-XI and *Kennedy v. the United Kingdom*, no. 26839/05, § 153, 18 May 2010); cf. para. 32 of the applicant firm's observations of 31 August 2015.

16. Turning to the signals intelligence process, the applicant firm holds that an interference with the rights stipulated in Article 8 begins as soon as any authority is given access to the communication. The applicant firm contends that this point is reached when the Swedish Foreign Intelligence Inspectorate provides access to a signal carrier according to a permit issued by the Foreign Intelligence Court. Moreover, the applicant firm holds – with reference to the illustration of the signals intelligence production selection process found in Appendix 3 of the Government's observations of 8 May 2015[2] – that the first two stages in that process consist of interception and storage of large amounts of data (paras. 12–15 and 26 of the applicant firm's observations of 31 August 2015).

17. At the outset, the Government finds it pertinent to clarify that it is not until the third stage in the illustrated process concerning selection referred to above that any information is available for human scrutiny. Contrary to the applicant firm's contention, there is no 'storage' taking place until after the first two stages in the illustrated process. The Government wishes to emphasise that this applies to traffic data[3] as well as content data. It should also be borne in mind that in order for either traffic data or content data to 'reveal' any information about a certain person, the data has to be analysed, i.e. subjected to human scrutiny (cf. para. 13 of the applicant firm's observations of 31 August 2015). In this context it is also relevant to reiterate that the Signals Intelligence Act, the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment and the related Ordinance[4], regulate the collection and handling of traffic data as well as content data.

18. Since the applicant firm seems to have misunderstood some vital aspects of the signals intelligence process, the Government finds it pertinent to recall

---

[2] The same illustration is reproduced in para. 11 of the applicant firm's observations of 31 August 2015.

[3] Traffic data consists of information that describes how, when and between which telecommunications addresses communication takes place, without describing the content of the transmitted communication. This concerns, for example, IP addresses, email addresses and telephone numbers. Through the collection and processing of traffic data, it is possible for the National Defence Radio Establishment to rapidly gain an idea of the traffic between countries on a given signal, without needing to examine the content of the traffic or understand the language. Traffic data is also used to enable the National Defence Radio Establishment to create a picture of normal traffic patterns and thus locate anomalies (see para. 40 of the Government's observations of 25 January 2013). The Government notes that the applicant firm uses the term 'metadata' instead of 'traffic data'. However, the Government will consistently use the term 'traffic data'.

[4] The Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment.

and, to some extent, further elucidate the second stage of the complete signals intelligence process[5] previously described in para. 22 of the Government's observations of 27 April 2012 in relation to cable collection.[6]

19. In the first stage of cable collection, the Swedish Foreign Intelligence Inspectorate gives access to a signal carrier[7] under a valid permit issued by the Foreign Intelligence Court. In the second stage, an automatic selection is made through the selectors or categories of selectors permitted by the Foreign Intelligence Court.

20. The process of selecting data through the use of selectors in the second stage of the signals intelligence process is in turn conducted in two steps. In the first step, data reduction at signals level is carried out, which means that only certain signals are chosen for further processing. In the second step, data reduction is carried out at communications level, which means that selectors are applied to the remaining information to sift out communications that are relevant to foreign intelligence (see the Signals Intelligence Committee Report, pp. 52–53).

21. All the parameters of a selector must match in order for the traffic to be collected from the signal carrier. The selectors are intended to make searches accurate and to serve as a filter to limit signals intelligence collection to what is relevant with regard to the tasking directives given to the National Defence Radio Establishment by, *inter alia*, the Government, as well as to prevent signals intelligence collection that falls outside of the relevant permit (see the Signals Intelligence Committee Report, p. 52, and para. 147 of the Government's observations of 27 April 2012).

22. The automatic selection in the second stage described above is done in real time, which means that any data that is not selected disappears without any possibility of being reproduced. This data will thus not be available to the National Defence Radio Establishment. Consequently, the National Defence Radio Establishment has no possibility to gain access at a later stage to the

---

[5] I.e. not the signals intelligence production selection process referred to in paras. 16–17 above.

[6] In this context, the Government wishes to clarify that the illustration of the stages of the signals intelligence process used by the applicant firm in its observations of 31 August 2012 (para. 39) is misleading and does not match the description that it provides in paras. 31–39 of the same observations; nor does it match the description provided by the Signals Intelligence Committee on pp. 73–75 of its report, to which the applicant firm refers (see para. 31 of the same observations).

[7] I.e., an individual optical fibre; see paras. 36 and 87 of the Government's observations of 27 April 2012 and para. 114 of the Government's observations of 8 May 2015.

traffic identified as irrelevant in the automatic selection process. It is also important to understand that since the selection process is automatic, the communications are not accessible to human eyes or ears during the selection phase (see the Signals Intelligence Committee Report, pp. 33, 52 and 74).

23. In this context, the Government furthermore wishes to reiterate its position that a secret surveillance measure cannot be considered to have been applied in relation to a natural or legal person before the third stage of the signals intelligence process (see paras. 145–155 of the Government's observations of 27 April 2012). Furthermore, since there is no distinction between when the National Defence Radio Establishment is given access to 'traffic data' and 'content data', there is no distinction as to when a secret surveillance measure 'is applied' with regard to these types of data.

24. In line with this, the Government wishes to clarify that its position is that there is no interference with an individual's rights under Article 8 until the point in time when a secret surveillance measure 'is applied', i.e. at the earliest at the third stage of the signals intelligence process (cf. paras. 58–59 in the Government's observations of 8 May 2015).

25. At this juncture, the Government finds it relevant to further elaborate on the prohibition to collect domestic traffic, in order to show that the concerns expressed by the applicant firm in this regard are not legitimate (see paras. 44–46 of the applicant firm's observations of 31 August 2015).

26. Once again, the Government recalls that collection from cables was not possible until after 1 December 2009, i.e. as from the third time period (see, *inter alia*, paras. 36, 83 and 92 of the Government's observations of 8 May 2015).[8] Furthermore, the signals intelligence collection from cables conducted by the National Defence Radio Establishment is subject to two important limitations in order to ensure compliance with the prohibition to collect domestic traffic: signals may *only* be collected from electronic communications cables that cross the Swedish border, and the signals may *not* contain domestic traffic (signals between a sender and a receiver who are both located in Sweden); see Sections 2 and 2a of the Signals Intelligence Act (cf. *Weber and Saravia v. Germany,* cited above, §§ 27, 32 and 97).

[8] It may be clarified that the difference between the second and third time period concerning collection from cables, described by the applicant firm in para. 44 of its observations of 31 August 2015, is hence irrelevant.

27. The National Defence Radio Establishment may only have technical access to cable signals that are covered by permits. One decisive criterion for the signals that are to be covered by such permits is, naturally, that they do not contain domestic traffic. Given its mandate, the National Defence Radio Establishment does not need to have access to such signals. If such signals cannot be separated on collection, recordings or notes are to be deleted[9] as soon as it becomes clear that such signals have been collected (Section 2a of the Signals Intelligence Act). The prohibition to collect domestic traffic does not apply to the collection of signals between senders and receivers aboard foreign state vessels or aircrafts, or in military vehicles. The National Defence Radio Establishment has to adhere to these legal requirements and is thus responsible for ensuring that the collection of such communications is limited. The Establishment works continuously on technological developments to tackle the technological challenges associated with distinguishing such signals.

28. As stated above, in cases where such signals were not successfully separated, the National Defence Radio Establishment has an *absolute duty* to delete such data without any further consideration. Accordingly, the obligation to delete any data collected in signals between a sender and a receiver who are located in Sweden is *not* an 'exception' serving to 'circumvent' the prohibition on collecting domestic traffic (cf. paras. 44–46 of the applicant firm's observations of 31 August 2015). Furthermore, the Swedish Foreign Intelligence Inspectorate is to control compliance with the Signals Intelligence Act. Consequently, and in response specifically to the applicant firm's contention in para. 45 of its observations of 31 August 2015, the limitations mentioned in para. 26 above are not insignificant.

29. In response to the applicant firm's contention that the Foreign Intelligence Court acts in secrecy and lacks impartiality (see paras. 19, 52 and 72 of the applicant firm's observations of 31 August 2015), the Government recalls that the main task of the Foreign Intelligence Court is to consider whether the conditions for issuing permits for signals intelligence are satisfied

---

[9] It is relevant to explain that in, *inter alia*, the Signals Intelligence Act, the Swedish term '*förstöring*' is used when prescribing that recordings or notes must be destroyed. However, under the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment, and the related Ordinance, the Swedish term '*gallring*' is used when prescribing the destruction of official documents or of data contained in official documents. In the following, the Government will use the term 'deletion' when referring both to '*gallring*' and '*förstöring*'. It might also be added that the Government has in previous observations used the terms 'erase' and 'destroy' when translating *förstöring*/*gallring*.

and to ensure that signals intelligence collection assignments are not in any way incompatible with the legislation. The Government also finds it pertinent to emphasise that the Foreign Intelligence Court is an independent court, and that neither the Riksdag nor a public authority may determine how the court shall adjudicate an individual case or otherwise apply a rule of law in a particular case (see Chapter 11, Article 3 of the Instrument of Government). It is also relevant to reiterate that even if the activities of the Foreign Intelligence Court are surrounded by secrecy, a privacy protection representative safeguards the privacy interests of individuals. Finally, the Court comes under the supervision of, *inter alia*, the Parliamentary Ombudsmen, the Office of the Chancellor of Justice and the Data Inspection Board; see further paras. 84–86, 99 and 101 of the Government's observations of 27 April 2012, para. 14 of the Government's observations of 25 January 2013 and para. 117 of the Government's observations of 8 May 2015.

30. Moving on to the applicant firm's statements regarding the duration of signals intelligence collection assignments (see para. 48 of the applicant firm's observations of 31 August 2015), the Government wishes to clarify the following. As previously mentioned, permits issued by the Foreign Intelligence Court are valid for a maximum period of six months and can be extended for a maximum of six months at a time after renewed examination (see paras. 61–62 of the Government's observations of 27 April 2012 and para. 110 of the Government's observations of 8 May 2015). The National Defence Radio Establishment must consistently assess the needs at hand relative to the applicable tasking directives, and apply for permits. The regulatory framework demands that the National Defence Radio Establishment – and, ultimately, the Foreign Intelligence Court – conduct continuous needs assessments.

31. Moreover, the applicant firm holds that the fact that signals intelligence can be conducted for development operations is problematic in several senses (see paras. 43 and 55 of the applicant firm's observations of 31 August 2015). In light of this, the Government would like to make some clarifications regarding the National Defence Radio Establishment's signals intelligence in development operations.

32. If necessary for foreign intelligence work, electronic signals may be collected in signals intelligence in order to conduct development operations, for example to develop technology and methods (Section 1, third paragraph of the Signals Intelligence Act). It is thus part of the National Defence Radio Establishment's mandate to develop the technology and methods needed to

conduct its foreign intelligence work. In order to collect and process signals and communications with the aim of providing intelligence, the National Defence Radio Establishment has a considerable need to develop and produce its own technical solutions in the form of new systems and new functions in existing systems. The National Defence Radio Establishment needs to collect signals to ensure the functionality and reliability of these technical systems. Consequently, the Establishment is dependent on development operations for its foreign intelligence work (see Government Bill 2006/07:46, p. 67–68).

33. Only the Government may decide the tasking directives for development operations (Section 4, second paragraph of the Signals Intelligence Act). This is done on a yearly basis. It is important to emphasise that all signals intelligence requires a permit from the Foreign Intelligence Court, i.e. including signals intelligence conducted in development operations (Section 4a and 5 of the Signals Intelligence Act). Furthermore, when processing personal data as part of its development operations, the National Defence Radio Establishment is to apply the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment and the related Ordinance (see further paras. 34–48 below). Moreover, in contrast to the foreign intelligence work conducted by the National Defence Radio Establishment, the development operations are conducted for the Establishment's own technical needs as described in para. 32 above. In conclusion, the signals intelligence conducted by the National Defence Radio Establishment in its development operations is as rigorously regulated – and subject to supervision to the same extent – as its foreign intelligence work.

34. The National Defence Radio Establishment processes personal data in both its foreign intelligence and development operations, and in its other activities, such as information security and human resources administration. When processing personal data as part of its foreign intelligence and development operations (which is what is relevant in relation to the present complaint), the National Defence Radio Establishment is to apply the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment and the related Ordinance. The Act applies where data processing is wholly or partly automated, or if the data is included in, or is intended to form part of, a structured collection of searchable personal data or a compilation according to particular criteria (Chapter 1, Section 1 of the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment). The aim of this legislation is to

protect individuals from intrusion of their personal privacy when personal data is processed in the course of the National Defence Radio Establishment's foreign intelligence and development operations.

35. Since the applicant firm has expressed concerns that the legislation on deletion of personal data is unclear (see paras. 65–66, 68–69 and 96 of the applicant firm's observations of 31 August 2015), the Government wishes to elaborate on these rules.

36. Under Chapter 6, Section 1 of the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment, personal data that is processed automatically must be deleted as soon as the data is no longer needed for the purposes for which it was processed, unless the Government or an agency designated by the Government has issued regulations or taken a decision in a specific case that deletion is to take place no later than a given date or that the data may be retained for historical, statistical or scientific purposes[10]. Thus, if not stated otherwise this main rule applies. Based on this main rule, needs assessments are continuously undertaken by the National Defence Radio Establishment. The Data Inspection Board and the Swedish Foreign Intelligence Inspectorate are responsible for monitoring the Establishment's work under the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment (see Chapter 5, Section 1 of the Act, Section 10 of the related Ordinance and Section 3 of the Ordinance containing instructions for the Swedish Foreign Intelligence Inspectorate[11]); cf. paras. 66 and 68 of the applicant firm's observations of 31 August 2015.

37. In view of the purpose of foreign intelligence work, there may be a need to retain personal data for a very long time (cf. para. 7 above). There can be instances in foreign intelligence work in which data as old as 40–70 years can be of significance for assessments in matters concerning Swedish foreign, defence and security policy. This could, for example, include biographical intelligence concerning foreign military officials where data is collected at the

[10] These provisions on deletion of data follow the EU Data Protection Directive. Provisions corresponding to those in the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment are also found in the Personal Data Act.

[11] The processing of personal data was regulated until June 2007 in the Personal Data Act, the Personal Data Ordinance and the Ordinance on certain processing of personal data within the Swedish Armed Forces and the National Defence Radio Establishment; see para. 46 of the Government's observations of 27 April 2012.

beginning of an official's career without any possibility to predict its significance for operations in the future. Correspondingly, data concerning a foreign official may be valuable throughout that person's lifetime – and sometimes longer – when conducting retrospective studies of developments in a given state, for example. These examples show how operations can, in some cases, require much longer retention times. Naturally, there is also personal data that can be deleted at a significantly earlier stage. The Government has also, in some cases, prescribed set – relatively short – time frames.

38. In the National Defence Radio Establishment's foreign intelligence and development operations, personal data shall be processed in data compilations[12] in accordance with the provisions of the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment and the related Ordinance. A data compilation is a compilation of data used collectively with the aid of automated processing (Chapter 1, Section 4 of the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment). It is accessible to various officials within the organisation, limited by the official's need for the data in order to fulfil his or her work assignments as well as his or her level of authorisation; see further paras. 49–50 below (cf. *Kennedy v. the United Kingdom*, cited above, §§ 43–47 and 163).

39. The data compilations that can be held at the National Defence Radio Establishment are exhaustively listed in Sections 2–6b of the Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment (cf. para. 58 of the applicant firm's observations of 31 August 2015). According to these provisions, the following data compilations may be held:

- data compilations for raw material (Section 2);
- data compilations for analyses (Section 3);
- data compilations for intelligence reports (Section 4);
- data compilations for information on the signals environment (Section 5);
- data compilations for information on phenomena targeted by signals intelligence (Section 6);

[12] The Government has previously used the term 'data collection' when translating *uppgiftssamling* (see para. 125 of the Government's observations of 8 May 2015). However, the Government finds that the term 'data compilation' is a more accurate translation and serves to avoid confusion with the expression 'collection of data'.

- data compilations for information on technological and methodological development (Section 6a); and
- data compilations for information on communications security (Section 6b).

40. A data compilation for raw material may only contain unprocessed and automatically processed material collected in foreign intelligence and development operations. Personal data in this kind of data compilation must be deleted no later than one year after the processing of the data began. This is an absolute rule without any exceptions.

41. A data compilation for analyses may only contain analysis results, processing data and report data (*analysresultat samt bearbetnings- och rapportunderlag*). Personal data that is processed automatically must be deleted as soon as the data is no longer needed for the purpose for which it was processed.

42. A data compilation for intelligence reports may only contain complete intelligence reports. Personal data that is processed automatically must be deleted as soon as the data is no longer needed for the purpose for which it was processed. On 19 March 2009, the National Archives decided, pursuant to Section 12 of the Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment, that intelligence reports are to be retained for historical, statistical and scientific purposes.

43. A data compilation for information on the signals environment may only contain information and technical parameters concerning the signals environment. Personal data in this kind of data compilation is to be deleted no later than the end of the first year after the processing of the data began, unless the National Defence Radio Establishment has decided prior to this that the data is to be retained because it is still needed for the purposes for which it was processed. If the data is retained by virtue of such a decision, it is to be deleted – or the question of retention is to be re-examined – no later than the end of the first year after the decision was taken.

44. A data compilation for information on phenomena targeted by signals intelligence may only contain information about signals intelligence targets that is necessary to enforce signals intelligence tasking directives. Personal data in this kind of data compilation is to be deleted no later than the end of the third year after the processing of the data began, unless the National Defence Radio Establishment has decided prior to this that the data is to be

retained because it is still needed for the purposes for which it was processed. If the data is retained by virtue of such a decision, it is to be deleted – or the question of retention is to be re-examined – no later than the end of the third year after the decision was taken.

45. In this context, the Government would like to draw the Court's attention to the Swedish Foreign Intelligence Inspectorate's inspection report of 19 June 2013, in which the Inspectorate found that it is necessary for the National Defence Radio Establishment to process personal data in test materials for recurring tests in its development operations, but considered that this data cannot be placed in data compilations for analyses. The Inspectorate also noted that the National Defence Radio Establishment needs to be able to save test material throughout a system's lifespan so that new tests can be conducted if the system is modified during the time it is in operation. With reference to the opinion expressed by the Swedish Foreign Intelligence Inspectorate, the National Defence Radio Establishment petitioned the Government for clarification of the provisions in the Ordinance on processing of personal data in the defence intelligence and development operations of the National Defence Radio Establishment on what data compilations may be held and what data can be processed in them. After the referral of an amendment proposal to the relevant bodies for consideration, the Government found reason to make such clarifications. Accordingly, as from July 2015 two additional data compilations were listed in the aforementioned Ordinance, i.e. Section 6a and 6b (cf. para. 59 of the applicant firm's observations of 31 August 2015).

46. A data compilation for information on technological and methodological development may only contain information and technical parameters concerning technological and methodological development. Personal data that is processed automatically must be deleted as soon as the data is no longer needed for the purpose for which it was processed.

47. A data compilation for information on communications security may only contain information and technical parameters concerning information on communications security. Personal data that is processed automatically must be deleted as soon as the data is no longer needed for the purpose for which it was processed.

48. The National Defence Radio Establishment has developed clear routines for reviewing the personal data processed, and for assessing when personal data is no longer needed for operational purposes and can therefore be deleted. It should also be recalled that supervision of the processing and

deletion of personal data is exercised by the Swedish Foreign Intelligence Inspectorate and the Data Inspection (cf. *Weber and Saravia v. Germany*, cited above, §§ 46, 48 and 100 and *Kennedy v. the United Kingdom*, cited above, §§ 46 and 164).

49. In this context, it may be relevant to add the following concerning the protective security at the National Defence Radio Establishment. Under Section 7 of the Protective Security Act, protective security is to prevent, *inter alia*, unauthorized disclosure, alteration or destruction of data subject to secrecy according to the Public Access to Information and Secrecy Act and that concerns the security of the realm. The National Defence Radio Establishment has an extensive internal and external protection. There is a well-constructed outer physical protection in the form of fences, surveillance, locked office doors and vaults. Much of the interior protection is linked to IT and security for the data which is processed by the National Defence Radio Establishment. For example, all measures taken by those processing the data are logged. Such measures are designed to provide protection against improper handling of sensitive data.

50. All employees at the National Defence Radio Establishment are security cleared in accordance with the Protective Security Act. In order to maintain a high security level, security clearance assessments are made continuously throughout the term of employment. Due to the strict secrecy that surrounds the signals intelligence conducted by the National Defence Radio Establishment, the work is organised in a compartmentalised way and, in practice, access to data is limited to include only the data each employee needs to perform his/her assignments. This ensures a limited and controlled dissemination of the data.[13]

51. The applicant firm has stated that it is not convinced that signals intelligence is not used to investigate offences (see para. 36 of the applicant firm's observations of 31 August 2015). Here the Government finds it pertinent to once again stress the fact that signals intelligence work is only allowed for certain purposes which are formulated in Section 1 of the Signals Intelligence Act (see paras. 59 and 74 of the Government's observations of 27 April 2012, paras. 87 and 107 of the Government's observations of 8 May 2015 and paras. 31–33 above). If a preliminary investigation has been initiated, signals intelligence within foreign intelligence may not be used by the law enforcement authority under which the preliminary investigation is being

[13] See the Signals Intelligence Committee Report, pp. 43–44.

conducted (see Government Bill 2006/07:63, p. 108). See also paras. 15 and 42 of the Government's observations of 27 April 2012, paras. 48–49 of the Government's observations of 23 January 2013 and paras. 104–106 of the Government's observations of 8 May 2015.

52. Moving on to the issue of possible direct access to data compilations at the National Defence Radio Establishment, the Government notes that the applicant firm erroneously holds that Section 9 of the Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment entails that a number of agencies have direct access to data collected by the National Defence Radio Establishment. Moreover, against this background, the applicant firm appears to draw the conclusion that data collected by the National Defence Radio Establishment may be used for purposes other than foreign intelligence work (see paras. 56 and 61–63 of the applicant firm's observations of 31 August 2015, cf. para. 37 of the same observations). In light of this, the Government finds it pertinent to clarify the rules on direct access under Section 9 of the aforementioned Ordinance.

53. Under Section 9 of the Ordinance on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment, a limited number of Government agencies[14] may be given direct access to information in a data compilation for *intelligence reports* to the extent decided by the National Defence Radio Establishment. However, the National Defence Radio Establishment has not taken any decisions regarding direct access. Hence, no government agency has direct access to any data compilation for intelligence reports.

54. Furthermore, a data compilation for intelligence reports may only contain *complete* intelligence reports (see further para. 42 above). Consequently, even if the National Defence Radio Establishment would give direct access to any of the government agencies that are listed in Section 9 of the aforementioned Ordinance, such access is limited to complete intelligence reports. Accordingly, there is no support for the applicant firm's claim that the possibility of direct access under Section 9 of the Ordinance on processing of personal data in the foreign intelligence and development

[14] The Government Offices, the Swedish Security Service, the Swedish Police Authority (National Operations Department), the Swedish Agency for Non-Proliferation and Export Controls, the Swedish Armed Forces, the Defence Materiel Administration, the Swedish Defence Research Agency, the Swedish Civil Contingencies Agency and Swedish Customs. It should be clarified that if access would be given, it is to be restricted to persons at these agencies who need access to this information for their work.

operations of the National Defence Radio Establishment means that data collected by the National Defence Radio Establishment may be used for purposes other than foreign intelligence work.

55. The applicant firm contends that the provisions in Sections 8 and 9 of the Signals Intelligence Act on reporting and international cooperation are broadly held and leave a large discretion to the National Defence Radio Establishment (see paras. 61 and 64 of the applicant firm's observations of 31 August 2015). In response thereto the Government refers to para. 47 of the Government's observations of 25 January 2013 and paras. 41–43 and 78 of the Government's observations of 8 May 2015. Hence, the Government maintains that the precautions to be taken by the National Defence Radio Establishment when communicating data to other parties are clearly regulated and subject to supervision.

56. As stated in previous observations, the Swedish Foreign Intelligence Inspectorate is to control compliance with the Signals Intelligence Act. This supervision covers all the stages of the signals intelligence process (see paras. 73, 88–92 and 142–144 of the Government's observations of 27 April 2012, paras. 15, 17 and 43 of the Government's observations of 23 January 2013 and para. 48 of the Government's observations of 8 May 2015). It should also be borne in mind that the Swedish Foreign Intelligence Inspectorate has control over the signals that the operators transmit to interaction points, and that the Inspectorate must ensure that the National Defence Radio Establishment only gains access to the signal carriers covered by a permit (Section 12 of the Signals Intelligence Act). The Swedish Foreign Intelligence Inspectorate is, among other agencies, also to control the National Defence Radio Establishment's compliance with the Act on Processing of Personal Data in the Foreign Intelligence and Development Operations of the National Defence Radio Establishment.

57. In response to the applicant firm's contention that the Swedish Foreign Intelligence Inspectorate lacks the power to grant compensation (see para. 75 of the applicant firm's observations of 31 August 2015), it is worth repeating that if, in the course of its supervision, the Swedish Foreign Intelligence Inspectorate notices any irregularities that may entail liability for the state towards a natural or legal person, the Inspectorate must 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 Foreign Intelligence and Development Operations of the National Defence Radio Establishment (see para. 148 of the Government's observations of 8 May 2015).

58. In paras. 26–27 and 75 of its observations of 31 August 2015, the applicant firm argues that the checks carried out by the Swedish Foreign Intelligence Inspectorate at the request of an individual on whether his or her communications have been the subject of signals intelligence do not entail a complete control of the National Defence Radio Establishment's activities, but only cover the stages after which the collected data has been made available for further processing. The applicant firm holds that this means that large amounts of data are left without any possibility of supervision. In response to this, the Government would like to draw the Court's attention to the fact that this assumption is based on the applicant firm's erroneous conclusion that traffic that has not been selected in the second stage of the signals intelligence process is somehow available to and stored by the National Defence Radio Establishment (see paras. 17–22 above and para. 55 of the applicant firm's observations of 31 August 2012 as well as paras. 12–15 of its observations of 31 August 2015).

59. As stated above (para. 22), the selection of signals is done in real time, which means that the traffic that is not selected in the second stage of the signals intelligence process will not be available to the National Defence Radio Establishment. While it is true that the checks carried out by the Swedish Foreign Intelligence Inspectorate at the request of an individual cover only the data that has been made available to the National Defence Radio Establishment for further processing, the Government wishes to clarify that such an order is a natural consequence of the fact that this is the only data that is available to the National Defence Radio Establishment (see Government Bill 2008/09:201, p. 92, and the Signals Intelligence Committee Report, p. 53; cf. para. 26 of the applicant firm's observations of 31 August 2015). A different order would mean that the data that has not reached the third stage of the signals intelligence process would have to be stored (cf. p. 13 of the Data Inspection report mentioned in para. 10 above and Government Bill 2008/09:201, p. 80).

60. The same argument applies to information that has been considered to lack importance for the signals intelligence conducted by the National Defence Radio Establishment, or is subject to the absolute duty of immediate deletion (see, *inter alia*, paras. 65, 75 and 92 of the Government's observations of 27 April 2012 and paras. 99, 108, 125 and 152 of the Government's observations of 8 May 2015). If such information would have to be available for later control by the Swedish Foreign Intelligence Inspectorate, it would have to be stored by the National Defence Radio Establishment (see para. 27 of the applicant firm's observations of 31 August 2015). The Government would like to stress that the whole point of having a permit procedure and

precise selectors is to protect privacy by avoiding collection or storage of more data than necessary.

61. When a recording or note is deleted, the measure is documented in a log in the computer system. The logs in the National Defence Radio Establishment's computer system contain the reason for deletion, the identity of the person who carried out the deletion, what kind of material was deleted and which case it was connected to. The Swedish Foreign Intelligence Inspectorate scrutinises the logs. Consequently, the logs ensure that supervision of compliance with the obligation to delete certain data is possible (see the Signal Intelligence Committee Report, p. 55).

62. In response to the applicant firm's contention that checks carried out by the Swedish Foreign Intelligence Inspectorate at the request of an individual are limited to the data available at the moment in time when the request is made (paras. 27, 75 and 86 of the applicant firm's observations of 31 August 2015) it is worth mentioning that an individual may turn to the Swedish Foreign Intelligence Inspectorate as many times and as frequently as he or she wishes.

63. As the Government mentioned in its observations of 8 May 2015 (para. 57), the Swedish National Audit Office audited the Swedish Foreign Intelligence Inspectorate in 2014. The audit included the Inspectorate's supervision of all four of the foreign intelligence agencies[15] and resulted in a National Audit Office audit report (RiR 2015:2). When the Swedish National Audit Office submits an audit report, the Government must submit its assessment of the report to the Riksdag within four months. This is done in a written communication (*regeringens skrivelse*).

64. The Government addressed the National Audit Office's observations in written communication 2014/15:142. In this communication, the Government welcomed the National Audit Office's audit of controls of foreign intelligence work. The Government further held that effective audits of all state-controlled activities are important, not least of activities surrounded by strict secrecy, and that the audit carried out by the National Audit Office contributes to further strengthening controls of foreign intelligence work.

[15] The Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Defence Materiel Administration and the Swedish Defence Research Agency.

65. Moreover, the Government noted the following. The overall conclusion of the National Audit Office is that the Swedish Foreign Intelligence Inspectorate has been given the necessary prerequisites to carry out its supervisory functions in an efficient and effective manner. The National Audit Office audit also attests that the foreign intelligence agencies take the Inspectorate's views seriously and implement measures in accordance with its decisions. In addition, the National Audit Office concludes that the Inspectorate carries out the tasks assigned to it under laws and ordinances. Furthermore, the National Audit Office considers that the Inspectorate prioritises controls in areas where it considers the risk of intrusion of privacy to be greatest, in line with the *travaux préparatoires* and the Inspectorate's instructions.

66. However, in its audit report, the National Audit Office considers that there is a lack of overall objectives for what is to be achieved by the Swedish Foreign Intelligence Inspectorate in its control activities. Nonetheless, the National Audit Office finds that it is clear what tasks the Inspectorate is to carry out. In its written communication in response to the audit report, the Government concurred with the National Audit Office that the Inspectorate's tasks as the supervisory body for foreign intelligence work are clearly formulated in laws and ordinances. The Government therefore considered that the Inspectorate's tasks are clear, and that there is no need for any specific objectives for the Inspectorate (cf. para. 73 in the applicant firm's observations of 31 August 2015).

67. Finally, in its written communication, the Government concluded the following. The Inspectorate's control function is deemed to be exercised appropriately and effectively, as expressed in the National Audit Office report. The few recommendations made by the National Audit Office are primarily administrative and marginal in nature, and do not imply any criticism of the activities as such. The Swedish Foreign Intelligence Inspectorate has already been working for some time on some of the National Audit Office's recommendations, and the Inspectorate will incorporate them into its future organisational development.

68. On 11 November 2015 the Riksdag decided to file the Government's written communication 2014/15:142 (*Försvarsutskottets betänkande 2015/16:FöU2, rskr. 2015/16:30*).

69. To sum up, the Government maintains that Article 8 is not applicable in the present case. Furthermore, the Government maintains that, in any event, Swedish legislation on signals intelligence within foreign intelligence complies

with the requirements of minimum legislative safeguards and of supervision of the regime with respect to all three time periods. 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. The case thus reveals no violation of Article 8 of the Convention and the applicant firm's complaint regarding Article 8 should therefore be declared inadmissible as being manifestly ill-founded.

Article 13

70. In its observations of 31 August 2015, the applicant firm has maintained that its right to an effective remedy under Article 13 of the Convention has been violated.

71. For its part, and with reference to what has been submitted in the Government's observations of 8 May 2015 (see paras. 134–158), the Government maintains 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. The Government furthermore maintains that, in any event, the applicant firm has had effective remedies at its disposal during all three time periods.

72. The Government agrees with the applicant firm's assertion that Article 13 does not require that a domestic remedy can challenge the existence of the legislation concerning the signals intelligence regime (see para. 81 of the applicant firm's observations of 31 August 2015 and cf. para. 138 of the Government's observations of 8 May 2015).

73. The applicant firm has furthermore stated that the remedies referred to by the Government *appear* far-fetched, tedious and ineffective (paras. 82–83 of the applicant firm's observations of 31 August 2015). However, the applicant firm has not presented any facts or arguments in support of this contention. The Government therefore does not find it necessary to further respond to the applicant firm's observations in this respect.

74. As regards the applicant firm's claim that the Data Inspection Board's mandate is limited to controls of the use of personal data and that the term 'personal data' is not applicable to the applicant firm (paras. 67 and 84 of the applicant firm's observations of 31 August 2015), the Government would like to state the following. Processing of data concerning natural persons enjoys special protection in European and Swedish law because such data may be of

a delicate nature. However, legal persons – such as the applicant firm – by necessity communicate through natural persons. Also when communicating on behalf of a legal person, natural persons enjoy the same protection of their personal data as any other natural person.

75. Moreover, the applicant firm asserts that checks carried out by the Swedish Foreign Intelligence Inspectorate at the request of an individual are limited to the last two stages of the signals intelligence conducted by the National Defence Radio Establishment, and do not cover all data stored by the Establishment. The applicant firm furthermore contends that checks by the Inspectorate are limited to data available at the moment in time when the request is made (see paras. 26–27, 75 and 85–86 of its observations of 31 August 2015). In response to this, the Government refers to paras. 58–62 above.

76. To sum up, the Government maintains that Article 13 is not applicable in the present case and, in any event, that the case reveals no violation of Article 13 of the Convention and that the applicant firm's complaint regarding Article 13 should therefore be declared inadmissible as being manifestly ill-founded.

On the applicant firm's claims for just satisfaction

77. The applicant firm has claimed compensation with SEK 282 534 (VAT included) for costs incurred in the proceedings before the Court.

78. If the Court finds that there has been a violation of the Convention, it may award the applicant, *inter alia*, compensation for the costs and expenses incurred in the proceedings before the Court. However, as the Court has repeatedly stated, an award under this head may be made only in so far as the costs and expenses were actually and necessarily incurred and reasonable as to quantum (see, among other authorities, *Dickson v. the United Kingdom* [GC], no. 44362/04, § 94, ECHR 2007-V, *Söderman v. Sweden* [GC], no. 5786/08, § 124, ECHR 2013).

79. In the event of the Court finding a violation of the Convention, and in addition finding that the applicant firm should be awarded compensation for the costs incurred in the proceedings before the Court, the Government has no objection as concerns the hourly fee claimed by the applicant firm, and leaves it for the Court to decide what sum is reasonable to award. Naturally, should the Court find that there has been a violation of the Convention in relation to only one of the Articles or in relation to only one or two of the

three time periods at issue in the present case, the Government holds that the compensation should be reduced accordingly.

Conclusions

80. The Government wishes to emphasise that it fully maintains its position concerning the admissibility and merits of the present application as outlined in its previous observations. A general reference is therefore made to what is stated in those observations. In addition, the fact that all the issues raised by the applicant firm are not commented upon should not be taken to mean that the Government accepts those parts of the applicant firm's observations that are not addressed.

81. In conclusion, 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 is applicable, and, in any event,
  - as being manifestly ill-founded;

concerning the merits,

- that the case reveals no violation of the Convention; and

concerning the applicant firm's claims for just satisfaction,

- that, in the event of the Court finding a violation of the Convention, the Government leaves it for the Court to decide what sum is reasonable to award for costs.