Government Offices of Sweden

Ministry for Foreign Affairs
Department for International Law,
Human Rights and Treaty Law

Stockholm, 3 May 2019
UDFMR2012/144/ED

IN THE EUROPEAN COURT OF HUMAN RIGHTS

GRAND CHAMBER

Application no. 35252/08

Centrum för rättvisa

v.

Sweden

OBSERVATIONS OF THE GOVERNMENT OF SWEDEN

Table of content

I. Introduction and summary 1

1. The scope of the case before the Grand Chamber 1

1.1 The complaint before the Grand Chamber 1
1.2 The Court's questions 2
1.3 The Government's position concerning the scope of the case before the Grand Chamber 3

2. The Government's position on admissibility and merits 4

II. Generally on signals intelligence within foreign intelligence 5

The Court's question no. 1, §§ 3–4 8

III. On the Admissibility 9

1. The new complaint before the Grand Chamber is inadmissible 9

2. The applicant cannot claim to be a victim 10

3. There is no interference with the applicant's rights under Article 8 § 1 of the Convention 16

The Court's questions no. 1, §§ 1–2, and no. 3, first sentence 16

IV. On the Merits 17

1. Article 8 17

1.1 There is no interference with the applicant's rights under Article 8 § 1 of the Convention 18
1.2 Any interference is justified 18
1.2.1 The signals intelligence regime has a basis in domestic law and pursues a legitimate aim 18
1.2.2 The signals intelligence regime is lawful and necessary in a democratic society 19
The Court's question no. 2 a) 19
The Court's question no. 2 b) 22
The Court's question no. 2 d) 23
1.2.2.1 Accessibility of domestic law 23
1.2.2.2 Scope of application of signals intelligence 24
1.2.2.3 Authorisation of signals intelligence 25

1.2.2.4 The duration of signals intelligence 27
1.2.2.5 Procedures to be followed for storing, accessing, examining, using and destroying the intercepted data 28
1.2.2.6 Conditions for communicating the intercepted data to other parties 30
The Court's question no. 3, second and third sentences 32
1.2.2.7 Supervision of the implementation of signals intelligence 33
The Court's question no. 2 c) 34
1.2.2.8 Notification of signals intelligence and available remedies 35
The Court's question no. 2 e) 36
1.3 Conclusion 37
2. Article 13 37
2.1 Article 13 is not applicable 38
2.2 There are effective remedies available to the applicant 39
2.3 Conclusion 41
V. Conclusions 42

I. Introduction and summary

1. These observations on the admissibility and merits of the case are submitted on behalf of the Swedish Government in response to the Court's invitations dated 18 February and 7 March 2019. The observations are made in light of the referral request, and having regard to the Chamber's judgment of 19 June 2018 in this case. A description of relevant domestic law and practice is enclosed as Appendix 1.

2. The use of signal intelligence within foreign intelligence is essential in protecting Sweden's national security and meets intelligence requirements which cannot be satisfied by any other reasonable means. The Government is mindful of the fact that the operation of a signals intelligence regime must provide sufficient safeguards against arbitrariness and possible abuse. However, such safeguards cannot undermine the effectiveness of regimes established in order to acquire intelligence critical for the protection of national security. In the present case, the Chamber found that the Swedish signals intelligence regime provides sufficient guarantees against arbitrariness and the risk of abuse, and concluded that there was no violation of the Convention. The Government agrees with the Chamber's conclusion and will elaborate below on the reasons why the Grand Chamber is invited to reach the same conclusion.

1. The scope of the case before the Grand Chamber

1.1 The complaint before the Grand Chamber

3. The applicant has complained that Swedish legislation concerning signals intelligence within foreign intelligence violates its rights under Article 8 of the Convention. The applicant has also complained that it has had no effective domestic remedy through which to challenge this violation, and that this constitutes a violation of Article 13 of the Convention. For the purposes of these observations, the Government assumes that the applicant maintains these complaints before the Grand Chamber.

4. In its request for referral, the applicant has also asked the Grand Chamber to examine whether sufficient safeguards are in place in terms of *receiving* intelligence from third parties, including other states (see, e.g., para. 45 of the applicant's request for referral; italics added).

1.2 The Court's questions

5. The Court has asked the Government to address the following questions in its written observations.

1. Has there been an interference with the applicant's rights under Article 8 § 1 of the Convention on account of the "bulk interception" of communications in Sweden?

In particular, the parties are invited to clarify at which stage(s) the interception and processing of information is capable of affecting the rights of concrete individuals or organisations; and to describe the manner in which the individuals or organisations are affected at the stage(s) identified.

The Government are further invited to provide examples of queries and/or selectors used and to inform the Court about the number (and duration) of interception permissions issued annually.

In addition, the Government are invited to clarify the use which is made of retained material in general and retained communications data in particular. Does material have to be "selected for examination" by a physical person in order to provide intelligence, or could it simply be subject to complex and comprehensive analysis (by computer)? Could material that is not on an index permitting it to be "selected for examination" by a physical person nevertheless be interrogated, aggregated and subjected to complex analysis by computer in order to provide intelligence? Is a difference made between content and communications data in this regard? On what basis is this retained content and communications data eventually discarded?

2. In the event that there has been an interference, was it in accordance with the law and necessary in terms of Article 8 § 2 of the Convention? In particular,

a) To what extent should the standards developed in the Court's case-law on secret measures of surveillance – and, in particular, the interception of communications – apply to the regime permitting the bulk interception and processing of communications and related communications data?

b) In the event that Article 8 § 2 requires the existence of certain safeguards to avoid abuses of power, to what extent do these safeguards have to be made public? Can they exist without being made public if they are subject to independent oversight?

c) Does Article 8 § 2 also require supervision and review of the impugned activities by an independent body and, if so, what level of independence from the Government is needed?

In view of the specific type of analysis in bulk interception, at what stage(s) would it be appropriate for supervision to take place? What type of supervision and review, if any, is required when the surveillance is first ordered, while it is being carried out, and after it has been terminated? Should there be a body entrusted with oversight powers which is capable of rendering legally binding decisions? If so, at what stage(s)?

d) Should the same principles apply to both content and related communications data?
e) As regards individual requests for review after the impugned intelligence has been carried out, does the system applicable in Sweden meet the relevant Convention requirements?

3. In that connection, to what extent and in what manner is the legal regime applicable in Sweden to communicating intercepted data to other parties capable of interfering with the rights of concrete individuals or organisations under Article 8 § 1 of the Convention? Insofar as it is capable of doing so, is that regime in accordance with the law and necessary within the meaning of Article 8 § 2? To what extent do the standards developed in the Court's case-law on secret measures of surveillance – and, in particular, the interception of communications – apply to this regime?

6. The Government finds that the Court's questions no. 1, §§ 3–4 are most appropriately addressed in a general section of the present observations (see Section II), while questions no. 1, §§ 1–2, and question no. 3, first sentence, concerning the existence of an interference are more suitably addressed in connection with the Government's observations on the admissibility. The Government will address question no. 2 and question no. 3, second and third sentences, in connection with the Government's observations on the merits.

1.3 The Government's position concerning the scope of the case before the Grand Chamber

7. The scope of the Grand Chamber's examination upon referral of a case that has been examined by a Chamber has been the subject of several judgments by the Grand Chamber. According to its consistent case-law, the case referred to the Grand Chamber is the application as it has been declared admissible by the Chamber (e.g. *Pentikäinen v. Finland* [GC], no. 11882/10, § 81, ECHR 2015 and *Medžlis Islamske Zajednice Brčko and Others v. Bosnia and Herzegovina* [GC], no. 17224/11, § 50, 27 June 2017). Furthermore, it is clear that the Grand Chamber may dismiss applications it considers inadmissible "at any stage of the proceedings" under Article 35 § 4 of the Convention. Therefore, the Court may reconsider a decision to declare an application admissible even at the merits stage, if it concludes that it should have been declared inadmissible for one of the reasons given in the first three paragraphs of Article 35 of the Convention (see, *inter alia*, *Gillberg v. Sweden* [GC], no. 41723/06, § 54, 3 April 2012).

8. Concerning the temporal scope of the Court's review, the Chamber found in the present case that it cannot be the task of the Court, when reviewing the law

in abstracto, to examine compatibility with the Convention before and after every single legislative amendment. The Chamber therefore focused its review on the Swedish legislation as it stood at the time of the Chamber's examination (see the Chamber judgment, § 98). Consequently, having regard to the case law set out above (para. 7), the Grand Chamber's review should be limited to the Swedish legislation as it stood at the time of the Chamber's examination.

9. As regards the applicant's complaint under Article 8 of the Convention, the Chamber found that it was open to doubt whether a legal person can have a private life within the meaning of Article 8. The Chamber therefore found it appropriate to examine the complaint under the right to respect for correspondence (see the Chamber judgment, § 85). The Grand Chamber's examination under Article 8 should therefore be limited to the right to respect for the applicant's correspondence.

10. As stated above, the applicant has asked the Grand Chamber to examine whether sufficient safeguards are in place in terms of sharing *and receivin*g intelligence from third parties, including other states. The Government notes that while the Chamber – as part of its examination of necessity and proportionality – considered whether there were adequate safeguards in place for the sharing of intelligence, the issue of possible receipt of intelligence was not included in the Chamber's examination. The applicant's complaint regarding "receiving information from other parties" is therefore a new complaint which did not form part of the application that was declared admissible by the Chamber. The Government argues that this complaint consequently falls outside the scope of the examination by the Grand Chamber and should be declared inadmissible. In any event, the applicant cannot have victim status for the purposes of Article 34 of the Convention as regards this new complaint.

2. The Government's position on admissibility and merits

11. Concerning the admissibility, the Government firstly holds that the applicant's complaint regarding "receiving information from other parties" should be declared inadmissible *ratione materiae* or *ratione personae.* As regards the rest of the application, the Government's position is that it should be declared inadmissible *ratione personae,* since the applicant 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, for being manifestly ill-founded. For the purposes of

admissibility, the Government has no objection regarding the exhaustion of domestic remedies.

12. Concerning the merits, the Government's position is that the present case reveals no violation of the Convention (cf. the Chamber judgment, § 181).

II. Generally on signals intelligence within foreign intelligence

13. At the outset, the Government wishes to submit some general information on signals intelligence within foreign intelligence.

14. Firstly, it may be pertinent to reiterate the regulation of signals intelligence within foreign intelligence, which can be summarised as follows.

- Foreign intelligence
  - is conducted in support of Swedish foreign, security and defence policy, and to identify external threats to Sweden, and
  - may only concern foreign circumstances.
- Signals intelligence within foreign intelligence
  - is a method for the collection of signals in electronic form for use in foreign intelligence,
  - may only be conducted under the specific terms and for the specific purposes outlined in law, i.e. to survey eight specific types of foreign phenomena and to maintain and develop signals intelligence technology and methods,
  - is conducted by using specifically formulated selectors in order to only intercept the relevant signals,
  - may <u>not</u> be used to investigate criminal offences,
  - may only be conducted in accordance with the Government's annual tasking directives and the detailed tasking directives issued by the Government, the Government Offices, the Swedish Armed Forces, the Swedish Security Police or the National Operations Department of the Swedish Police Authority,
  - may only be conducted by one authority – the FRA (*Försvarets radioanstalt*, the National Defence Radio Establishment),
  - requires a permit from a court– the Foreign Intelligence Court – for any collection,
  - is supervised by a special control authority – the Swedish Foreign Intelligence Inspectorate.

15. Signals intelligence within foreign intelligence has a threefold perspective.

- To detect and identify new developments and anomalies that may constitute threats, potential threats and risks, by long term monitoring of known phenomena.
- To react to unforeseen and suddenly emerging foreign events and threats in support of e.g. crises management, policymaking, political or military response.
- To proactively identify foreign threats in the making or foreign intents of relevance to Swedish national security and Swedish security, foreign and defence policies.

16. Signals intelligence within foreign intelligence concerns national security and defence, and activities within the process of collection of signals intelligence are therefore safeguarded by strict secrecy. This is balanced by clear legislation, a judicial permit requirement and special supervision.

17. Reliable intelligence collection capabilities in order to obtain information of relevance to national security interests is of critical importance to Sweden's ability to pursue its independent foreign and security policy. The aim of Sweden's foreign intelligence is to provide a basis for assessments and decisions in support of Swedish foreign, security and defence policy, and to assist Swedish participation in international security cooperation.

18. The FRA provides the Government and other Swedish specified authorities with unique knowledge of foreign developments of relevance to national security and other specified interests. This could for example include information on the military capabilities of other countries, developments in war or conflict regions, international terrorism, or state-sponsored cyber attacks.

19. Current threats to national and international security are often cross-border, asymmetric, and both military and non-military in nature, and come from state and non-state actors. Preventing and counteracting such threats requires close cooperation between Swedish authorities as well as effective international cooperation. Military action, international terrorism and cyber attacks are some examples of threats to states and their inhabitants. A well-developed capacity for intelligence collection and crisis management are important tools in this context.

20. Information technology developments, in combination with the expanding multifaceted and diverse global communication structure, have enabled and contributed to improvements in the productivity of industry and have increased welfare. At the same time, modern society's dependence on IT in critical infrastructure, such as communications, the electricity grid or transportation, has made society more vulnerable. This concerns not only individuals but organisations, companies and states too. Advanced technical competence in signals intelligence is a prerequisite for Sweden to be able to protect its own communications systems.

21. The high level of military activity in Sweden's geographic proximity means that, through airborne and naval signals intelligence and other means, the FRA can contribute necessary information on the performance and parameters of other states' radar systems. This information provides the Swedish Armed Forces with support in identifying other states' military vessels, aircraft and vehicles, for example. Through signals intelligence, the FRA can also follow movements of military units and combat activity in conflict areas and monitor developments over the long term. This gives Sweden its own intelligence on matters about which it would otherwise have been difficult to obtain reliable information. Examples of issues monitored by the FRA include arms deliveries, troop movements and power relations between various military or terrorist groups in war and conflict areas, as well as which actors are attempting to manufacture chemical or nuclear weapons.

22. Typical intelligence connected to Swedish military operational activities abroad concerns information on force protection and assessments of developments in the country in question.

23. International terrorism is a serious threat worldwide. Sweden shares security challenges with other countries. The foreign phenomena monitored by the FRA are often global but have links to Sweden. This means that the importance of international cooperation has increased in recent years. The FRA provides support to the Swedish Security Police by reporting on developments in international terrorism in general and possible links to Sweden in particular.

24. In recent years, Sweden has seen examples of attempts by foreign powers to influence decision-making processes, both internationally and in Sweden. Several countries are also carrying out intelligence operations targeting Sweden and Swedish interests.

25. In response to the Court's invitation to *provide examples of queries and/or selectors used*, the Government wishes to put forward the following.

26. Selectors refer to a combination of technical data and various addressing details. The more detailed formulation of selectors is achieved through a carefully balanced combination of technical data, such as the source country of the signals gathered and the transmission media with which they are communicated, as well as other parameters such as keywords (e.g. the specific name of a weapons system or other technical terminology), unique names and languages. The various components also include frequencies, telephone numbers or IP addresses. Names, telephone numbers and email addresses, and IP addresses that can be linked to a specific individual, may only be used if it is of particular importance for the activities. The selectors are built up with great precision, which means that they consist of several components. By specifying selectors, the FRA can search through a signal and find the items in which the selector appears. All parts must match to get a hit in the traffic collected. The selectors are intended to make searches accurate and to serve as a kind of filter to limit intelligence collection to what is relevant, as well as to prevent unlawful intelligence collection. The selectors used for interception of communications data are generally less specific than those used for interception of the content of a communication (see paras. 81–82 below). In this context, it is relevant to reiterate that the Signals Intelligence Act stipulates that the selectors must be formulated in such a way that the interference with personal integrity is limited as far as possible (see Appendix 1, Sections 4.1.5 and 4.2).

27. As regards the Court's invitation to *inform the Court about the number (and duration) of signals intelligence permits issued annually*, the Government wishes to state that this kind of information could be indicative of the ability and methods of the FRA in a manner incompatible with the purposes of signals intelligence. It is therefore not possible to inform the Court about the annual number of permits. Regarding their duration, permits may be granted for a maximum period of six months. Upon application by the FRA and renewed examination by the Foreign Intelligence Court, a permit may be extended for a maximum of six months at a time (see Appendix 1, Section 4.3). Foreign intelligence is a long-term activity which means that the need for using certain approved selectors in a signals intelligence mission may need to extend for several years. This can be clearly illustrated, *inter alia,* by the requirement to map foreign military activity around the borders of Sweden.

28. The Government would furthermore like to make the following clarifications regarding *the use which is made of retained material in general and retained communications data in particular* in response to the Court's invitation.

29. Collected material always needs to be examined by a physical person – an analyst – at the FRA in order to provide intelligence, irrespective of whether the material collected consists of content or communications data. The analyst controls the quality of the data by assessing its reliability and accuracy. The relevance of the data must also be assessed based on the requirement that data that is included in the final report to the requesting authority must always add value in accordance with the applicable tasking directive. The analyst must assess whether the data is already known to the requesting authority and determine when the data is to be reported. The analyst must also examine any personal data from a perspective of proportionality. This assessment involves justifying and examining whether it is necessary to use personal data in relation to their importance for foreign intelligence purposes, i.e. supporting Swedish foreign, security and defence policy and identifying external threats to Sweden. The Government would like to stress that material which may not be "selected for examination" by a physical person cannot be interrogated, aggregated and subjected to complex analysis by computer in order to provide intelligence. No distinction is made between content and communications data in this regard.

30. Finally, the FRA Personal Data Processing Act and its associated ordinance contain rules about discarding personal data. According to the main rule, personal data that is processed automatically must be discarded as soon as the data is no longer needed for the purposes for which it was processed. This is equivalent to the EU regulation on the processing of personal data. In any circumstances, unprocessed and automatically processed data collected in foreign intelligence and development activities must be discarded no later than one year after the processing of the data began, i.e. when it was collected (see the FRA Personal Data Processing Ordinance as described in Appendix 1, Section 4.4).

III. On the Admissibility

1. The new complaint before the Grand Chamber is inadmissible

31. The Government holds that the applicant's complaint regarding "receiving information from other parties" should be declared inadmissible, see para. 10 above.

2. The applicant cannot claim to be a victim

32. In the *Roman Zakharov v. Russia* judgment ([GC], no. 47143/06, ECHR 2015), the Court clarified the conditions under which an applicant can claim to be a victim of a violation of Article 8 of the Convention occasioned by the mere existence of secret surveillance measures, or of legislation permitting such measures. The Court found that the *Kennedy* approach (*Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010) is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the Court (*Roman Zakharov*, § 171). The Court outlined the conditions as follows.

33. Firstly, regard should be had to the scope of the legislation permitting secret surveillance measures through an examination of whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted (*Roman Zakharov*, § 171).

34. Secondly, the availability of remedies at the national level should be taken into account; the degree of scrutiny should be adjusted depending on the effectiveness of such remedies. Where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances, the threat of surveillance can be claimed in itself to restrict free communication through postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court, and an exception to the rule denying individuals the right to challenge a law *in abstracto* is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were actually applied to him or her (*Roman Zakharov*, § 171).

35. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he or she is

able to show that, due to his or her personal situation, he or she is potentially at risk of being subjected to such measures (*Roman Zakharov*, § 171).

36. In the present case, the Chamber, seemingly applying the *Kennedy* approach as developed in *Roman Zakharov*, considered an examination of the relevant legislation *in abstracto* to be justified. This conclusion was based on the Chamber's opinion that the Swedish legislation on signals intelligence within foreign intelligence institutes a system of secret surveillance that potentially[1] affects all users of, for example, mobile telephone services and the internet, without their being notified about the surveillance, and that there is no domestic remedy which provides detailed grounds in response to a complainant who suspects that he or she has had his or her communications intercepted (see the Chamber judgment, § 94). The Government objects to this finding for the reasons set out below.

37. As regards the scope of the legislation, the Government argues that the applicant, being a non-profit public interest law firm based in Sweden whose activities mainly concern Swedish law and individuals, does not, using the Court's terminology, belong to a "group of persons or entities targeted by the legislation" on signals intelligence within foreign intelligence. Furthermore, the Government contests that the legislation *directly* affects all users of mobile telephone services and the internet. There are inherent limitations in the legislation on signals intelligence within foreign intelligence, since it is restricted to foreign intelligence, and thereby foreign circumstances, and may only be carried out for the purposes specified in law (see above, section II and Appendix 1, Section 4.1). This essentially means that not all those communicating by internet and telephone are *directly* affected by the legislation on signals intelligence within foreign intelligence. Accordingly, the scope of the legislation on signals intelligence within foreign intelligence is not such that the applicant can possibly be affected by it.

38. As concerns the availability of remedies, the Government holds that the Swedish regime concerning signals intelligence within foreign intelligence affords effective remedies for a person who suspects that he or she was subjected to secret surveillance.

39. In this context, the Government would primarily like to point to the control that the Swedish Foreign Intelligence Inspectorate will carry out at the request of an individual of whether his or her communication has been collected in

[1] Cf. *Roman Zakharov,* § 171, where the Court uses the expression "*directly* affects all users" (italics added).

connection with signals intelligence. A request can be made by legal and natural persons, regardless of nationality and residence. Following the control, the Inspectorate must notify the individual that a control has been carried out and report whether or not any improper collection has taken place. If the Inspectorate finds evidence of improper signals collection, this must be reported to the authorities responsible for the matter at hand, e.g. the Swedish Data Protection Authority, the Office of the Chancellor of Justice or the Office of the Prosecutor-General. The Inspectorate has the power to decide that the interception of data must cease or that the intercepted data must be destroyed. For further details, see Appendix 1, Section 4.7.2.

40. At this juncture, the Government wishes to clarify that the Inspectorate carries out such controls at the premises of the FRA, with its full cooperation, and that the Inspectorate has the authority to access all necessary data compilations in order to investigate whether the individual has been subjected to any improper signals collection.

41. In its judgment in the present case, the Chamber expanded the requirement of the availability of remedies when it held that there is no remedy in Sweden that provides "detailed grounds in response to a complainant who suspects that he or she has had his communication intercepted" (see the Chamber judgment, § 94). Neither the *Kennedy*, nor the *Roman Zakharov* judgment supports the conclusion that, in order to be effective, a remedy has to provide "detailed grounds". The Government holds that the control carried out by the Swedish Foreign Intelligence Inspectorate upon a request by an individual is an effective remedy for the purpose of deciding whether the applicant can claim to be a victim.

42. In addition, there are a number of other remedies available to the public, namely the possibility to apply to the Parliamentary Ombudsmen, the Chancellor of Justice or the Swedish Data Protection Authority, the possibility to bring an action for damages, the possibility to report a matter for prosecution and the possibility to bring a claim for compensation for violations of the Convention.

43. Both the Parliamentary Ombudsmen and the Chancellor of Justice have the competence to receive individual complaints and they may investigate such complaints in order to ensure that the relevant laws have been properly applied by the relevant authorities (see Appendix 1, Sections 4.7.4–4.7.5). In their performance of these duties, both officials are entitled to have access to the minutes and other documents of the courts and the administrative authorities.

Although neither of these officials, notwithstanding their competence to institute criminal and disciplinary proceedings, have the power to issue legally binding decisions, it should be stressed that the opinions of the Parliamentary Ombudsmen and the Chancellor of Justice traditionally command great respect in Swedish society and are usually followed in practice.

44. While the abovementioned authorities do not have the power to annul the provisions on foreign intelligence or signals intelligence if the provisions themselves were to be considered incompatible with the Convention, their scrutiny could provide further elucidation of the applicable safeguards and of the general operation of signals intelligence conducted by the FRA, such as would assist the Court in its consideration of the compliance of these activities with the Convention (see *Kennedy,* cited above, § 110).

45. The Government would also like to recall the supervisory tasks of the Swedish Data Protection Authority in this context. The Authority may examine complaints by natural or legal persons. On request, the Authority has access to personal data that is processed, documentation on the processing of personal data along with the security measures taken on such treatment and access to the facilities connected to the processing of personal data. If the Authority finds that personal data is or could be processed in an unlawful manner, it must endeavour to obtain rectification. The Authority may also apply to an administrative court to have unlawfully processed personal data destroyed. The State is liable for damages following a violation of personal integrity caused by processing of personal data not in accordance with the FRA Personal Data Processing Act. For further details, see Appendix 1, Sections 4.6.2 and 4.7.6; see also the Chamber judgment, § 50.

46. Furthermore, any individual has the right to apply to the FRA for information on whether or not personal data concerning him or her is being processed. The FRA is obliged to provide such information free of charge once per calendar year to any individual who applies. It is also obliged to correct, block or delete at the earliest opportunity personal data that has not been processed in accordance with the legislation or regulations issued pursuant to the law. A decision by the FRA on disclosure of information or rectification can be appealed to an administrative court. 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 (see Appendix 1, Section 4.7.3). It should be clarified that the administrative courts that examine the appeal may have access

to any documents and personal data available at the FRA regarding the individual concerned, for the purpose of carrying out its examination.

47. To sum up, the Government holds that the Swedish regime concerning signals intelligence within foreign intelligence provides for effective remedies for a person who suspects that he or she was subjected to secret surveillance. Consistent with the Court's findings in *Roman Zakharov*, the applicant may therefore only claim to be a victim of a violation occasioned by the mere existence of legislation permitting secret measures if it is able to show that, due to its "personal" situation, it is potentially at risk of being subjected to such measures (*Roman Zakharov*, § 171).

48. In determining the risk of secret surveillance measures being applied to the applicant, the Government would like to make a reference to the signals intelligence process as described in Appendix 1, Section 4.1.3. In short, the six stages of the signals intelligence process can be described as follows:

1 A choice is made as to which segments of the signals intelligence environment are assessed as the most relevant to target for collection at any given time, considering current and valid tasking directives and detailed intelligence requirements, the court's permits in force and with regard to the practical limitations of the FRA's collection, processing and analysis capacity.

2 For any automatic collection selectors are applied to signals in electronic form in the segments defined as the most relevant in order to intercept and gradually reduce what is finally collected to such data which is of relevance to meet the intelligence requirements within the tasking directives.

3 The data is further processed in order to refine the information and make it as easily exploitable as possible from an analysis perspective. Examples of further processing include cryptoanalysis, structuring and language translation. The refinement of collected data is usually performed both through automatic and manual means.

4 The processed information is analysed by an analyst in order to identify intelligence within available information.

5 A report is written and disseminated to one or several recipients within the select group of foreign intelligence recipients which have both a right and a requirement to receive signals intelligence reports on the specific matter covered by the specific report at hand.

6 Feedback on use and effect of the intelligence provided is requested and shared with those involved in the signals intelligence process that enabled the report.

49. It must be assumed that the applicant has made and makes fixed and mobile telephone calls, and has used and uses the internet via fixed and mobile connections. This means that the applicant has used and uses public electronic communication networks and services for its communication needs.

50. An initial prerequisite for the applicant's traffic to have been collected through signals intelligence in the first place is that the traffic occurred in the signals environment chosen for the collection of data (first stage). In this context, it is relevant to take into consideration that signals intelligence may not be conducted on domestic traffic within Sweden. Moreover, the majority of purely domestic electronic communication signals will not pass the hand-over points in cross-border cables, for which reason such signals will not be subject to collection by the FRA. Furthermore, for the applicant's communication to have been sifted out at all in the filtering stage (second stage), it must have matched all the parameters of a selector. It must be borne in mind that the selectors that refer to the contents of the communication are designed with great precision as regards the foreign phenomena targeted by signals intelligence and on the basis of the purposes, as set down in law, for which foreign intelligence may be conducted. The selectors must also conform to the Signals Intelligence Act, the valid permit of the Foreign Intelligence Court and the detailed tasking directives provided by those who commissioned the intelligence based on their specific intelligence requirements.

51. From the description above it is thus clear that it is not until the third stage of the signals intelligence process that the information content resulting from the filtering and selection processes is available for further refinement through automatic and manual means, i.e. this is the earliest stage that the information collected through automated processes may be subjected to human scrutiny. Traffic does not reach the third stage unless it is sifted out in the filtering stage, which in principle only occurs if it matches all the parameters of a selector. The risk of the applicant's communication being sifted out and thus reaching the third stage of the signals intelligence process is very limited. However, the third stage involves no actual analytical examination or consideration of the communication, which is possible only at the fourth stage. It is consequently not until then that a secret surveillance measure can be considered to have been applied in relation to

a natural or legal person. The risk of the applicant's communication reaching the fourth stage of the signals intelligence process is virtually non-existent. The Government therefore argues that the applicant has not shown that, due to its "personal" situation, it is potentially at risk of being subjected to secret surveillance measures.

52. The Government therefore concludes that the applicant cannot claim to be a victim of a violation within the meaning of Article 34 of the Convention occasioned by the mere existence of Swedish legislation on signals intelligence within foreign intelligence.

3. There is no interference with the applicant's rights under Article 8 § 1 of the Convention

53. The Government finds that the question of whether there is an interference with the applicant's rights under Article 8 § 1 of the Convention is most appropriately addressed when examining the admissibility of the application (cf. *Gillberg*, cited above).

54. Initially, the Government holds 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 fourth stage of the signals intelligence process (see paras. 48–51 above).

55. As specifically concerns the applicant, the Government has previously concluded that the risk that a secret surveillance measure has actually been applied to it is virtually non-existent (see para. 51 above). It therefore follows that the applicant cannot complain of an interference with its right under Article 8 of the Convention on account of the signals intelligence regime. Consequently, Article 8 is not applicable in the present case.

The Court's questions no. 1, §§ 1–2, and no. 3, first sentence

56. In reply to the Court's question of *whether there has been an interference with the applicant's rights under Article 8 § 1 of the Convention on account of the Swedish signals intelligence regime*, the Government holds that there has been no such interference (see paras. 53–55 above).

57. Turning to the Court's general question concerning *at which stage(s) the interception and processing of information is capable of affecting the rights of concrete individuals or organisations*, and its invitation to *describe the manner in which the individuals or organisations are affected at the stage(s) identified*, the Government refers to its observations above regarding the signals intelligence process and the risk of secret surveillance measures being applied to the applicant (see paras. 48–55 above). It is thus the Government's position that the rights of concrete individuals or organisations may be affected at the earliest at the fourth stage of the signals intelligence process.

58. As concerns the Court's question on *the extent to which and in what manner, the legal regime applicable in Sweden to communicating intercepted data to other parties is capable of interfering with the rights of concrete individuals or organisations under Article 8 § 1 of the Convention*, the Government initially wishes to underline that the regulation concerning signals intelligence within foreign intelligence aims at supporting Swedish foreign, security and defence policy and to identify external threats to Sweden and that the FRA has a regulated obligation to report to the Swedish authorities concerned. In this context, it is also important to stress that personal data concerning a specific individual may only be reported if it is of relevance for the purposes for which foreign intelligence may be conducted (see para. 111 below).

59. Furthermore, the Government wishes to clarify that the legislation on signals intelligence within foreign intelligence is also applicable to the communication of intercepted data to other parties abroad. In this context, too, the Government therefore finds it pertinent to refer to its observations above regarding the signals intelligence process (see paras. 48–52 above). It is also relevant to take into consideration that data may only be communicated to other parties abroad under certain limited conditions. For further details see paras. 110–117 below and Appendix 1, Section 4.5.2).

IV. On the Merits

1. Article 8

60. The Government would like to reiterate that the Grand Chamber's examination under Article 8 should be limited to the right to respect for the applicant's correspondence (see para. 9 above).

1.1 There is no interference with the applicant's rights under Article 8 § 1 of the Convention

61. As stated above (paras. 53–56), the Government holds that the applicant cannot complain of an interference with its rights under Article 8 of the Convention.

1.2 Any interference is justified

62. In any event, the Government argues that any possible interference is in accordance with the law, pursues a legitimate aim and is necessary within the meaning of Article 8 § 2 of the Convention. The Government will elaborate below on the reasons for this contention.

1.2.1 The signals intelligence regime has a basis in domestic law and pursues a legitimate aim

63. Initially, the Government notes that it has not been disputed by the applicant that the Swedish signals intelligence regime has a basis in domestic law (see the Chamber judgment, § 111).

64. Turning to the issue of legitimate aim, the Government would like to reiterate the following. Foreign intelligence is conducted in support of Swedish foreign, defence and security policy, and to identify external threats to the country. The purpose of the signals intelligence conducted by the FRA is to obtain information and identify phenomena of relevance for foreign intelligence. Reliable intelligence collection capabilities in order to obtain information of relevance to national security interests is of critical importance to Sweden's ability to pursue its independent foreign and security policy. The FRA provides the Government and other Swedish authorities with unique knowledge of foreign developments of relevance to national security and other specified interests. Thus, the use of signal intelligence within foreign intelligence is essential in protecting Sweden's national security and meets intelligence requirements which cannot be satisfied by any other reasonable means (cf. *Big Brother Watch and Others v. the United Kingdom,* nos. 58170/13 and 2 others, § 384, 13 September 2018). At this juncture, the Government finds it relevant to recall its positive obligation under the Convention to protect the lives and safety of the public.

65. In light of the above, the Government considers it clear that the measures permitted by Swedish law pursue legitimate aims in the interest of national security by supporting Swedish foreign, defence and security policy and identifying external threats to the country (see the Chamber judgment, § 111 and cf. *Kennedy*, cited above, § 155). Furthermore, the Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security. Furthermore, the Court has accepted that bulk interception regimes do not *per se* fall outside this margin (*Weber and Saravia v. Germany* (dec.), no. 54934/00, § 106, ECHR 2006-XI, the Chamber judgment, § 112, and *Big Brother Watch,* cited above, § 314). The Government holds that the decision to operate a signals intelligence regime in Sweden falls within this wide margin of appreciation.

1.2.2 The signals intelligence regime is lawful and necessary in a democratic society

66. In cases where legislation permitting secret surveillance is contested before the Court, the Court has held that the lawfulness of the interference is closely related to the question of whether the "necessity" test has been complied with. The Court has thus found that that it is appropriate to address the "in accordance with the law" and "necessity" requirements jointly (*Roman Zakharov,* cited above, § 236 with further references and the Chamber judgment, § 107). For the reasons set out by the Court, the Government will address these two requirements jointly.

The Court's question no. 2 a)

67. In reply to the Court's question of *the extent to which the standards developed in the Court's case-law on secret measures of surveillance should apply to the signals intelligence regime*, the Government would like to put forward the following.

The standards developed in the Court's case-law should be adapted

68. In its case-law, the Court has developed minimum safeguards that should be set out in law in order to avoid abuses of power of secret interception regimes (*Roman Zakharov,* cited above, §§ 231 and 238). These minimum safeguards have essentially developed in case-law concerning secret measures of surveillance in criminal investigations (see the Chamber judgment, § 103; see also *Big Brother Watch*, § 307). As noted by the Chamber, the Convention compatibility of regimes which expressly permit strategic surveillance has only been considered on two

occasions (see the Chamber judgment, § 108; see also *Big Brother Watch*, § 311). For its part, the Government notes that *Weber and Saravia* also concerned secret measures of surveillance in order, *inter alia*, to investigate and prosecute offences (§ 33). A direct consequence of the fact that the minimum safeguards have developed in case-law concerning criminal investigations is that some of the minimum safeguards presupposes that the secret surveillance measures at issue are linked to a certain individual or to a certain place and concern a criminal offence.

69. However, signals intelligence within foreign intelligence cannot be used to investigate criminal offences and it is one of the duties of the Foreign Intelligence Court to ensure that this does not happen (see Appendix 1, Section 4.1.6 and para. 75 below). On the contrary, the purpose of the signals intelligence conducted by the FRA is to obtain information and identify phenomena of relevance for foreign intelligence. To obtain such information, in many cases signals intelligence has to target specific individuals' communications. Still, in the context of signals intelligence within foreign intelligence, individuals are most often not of interest *per se,* but only as carriers of information.

70. Indeed, the Court has in certain cases already made some adaptations to the first two minimum requirements concerning "the nature of the offences" and "categories of persons". Firstly, it is clear from the cases of *Roman Zakharov* and *Kennedy*, both 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 (§§ 229 and 244 and § 159 respectively). 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.[2]

71. The Government is of the opinion that the two requirements concerning "the nature of the offences" and "categories of persons targeted" may lead to misconceptions as regards interception regimes that are <u>not</u> used to investigate criminal offences. Those two requirements should therefore be reformulated more explicitly, e.g., to "the circumstances in which the measures may be used".

[2] Cf. the Venice Commission's "Report on the democratic oversight of signals intelligence agencies", 15 December 2015, paras. 15 and 86–87.

72. Against this backdrop, the Government holds that the minimum safeguards set out in the Court's case-law should be adapted to reflect the fact that the legislation to be examined by the Court exclusively concerns national security issues in the context of foreign intelligence and does not permit the use of signals intelligence to investigate criminal offences (cf. the Chamber judgment, § 114; see also *Big Brother Watch*, § 320). The Government invites the Court to draw this conclusion in the case at hand.

Reasonable suspicion shall not be included as a minimum requirement

73. The applicant contends that the minimum safeguards should include a requirement of "reasonable suspicion", at least when selectors that can be linked to a specific individual is used, and that such a requirement follows from *Roman Zakharov* (cited above) and *Szabó and Vissy v. Hungary* (no. 37138/14, 12 January 2016). The applicant further argues that signals intelligence may otherwise be used to circumvent the regulation concerning, *inter alia*, coercive measures under criminal law (paras. 24–32 of the request for referral). The Government strongly disagrees.

74. Initially, the Government argues that it does not follow from either *Roman Zakharov* or *Szabó and Vissy* that there is a requirement of "reasonable suspicion" and that those judgments have to be seen in their respective context.

75. In this context, it is also important to reiterate that one of the duties of the Foreign Intelligence Court is to ensure that signals intelligence is not used to circumvent the regulations concerning coercive measures under criminal law. Moreover, the authorisation carried out by the Foreign Intelligence Court ensures that any use of selectors that may be linked to a specific individual is necessary and proportionate. Such an examination provides the necessary level of protection concerning signals intelligence within foreign intelligence.

76. The Government also notes that in the *Big Brother Watch* judgment, the Chamber held that:

> "requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of

> "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime." (§ 317).

77. The Government strongly agrees with the reasoning of the Chamber in the *Big Brother Watch* case when reaching the logical conclusion that "reasonable suspicion" cannot be required. Such a requirement would render the operation of the Swedish regime on signals intelligence within foreign intelligence impossible as its purpose is to look for hitherto unknown dangers, not monitoring known ones. As stated above, signals intelligence within foreign intelligence meets intelligence needs which cannot be satisfied by any other reasonable means.

The Court should consider the totality of the safeguards against abuse within the system

78. Moreover, the Government holds that when the Court is to examine a system of secret surveillance *in abstracto*, it should have regard to the relevant legislation and other information concerning the system in order to assess whether, on the whole, there are sufficient minimum safeguards in place to protect the public from abuse (see the Chamber judgment, § 180). Hence, an overall assessment of the whole system should be made and if there are robust safeguards as regards some aspects of a system, the State may be afforded a greater discretion in other aspects.

The Court's question no. 2 b)

79. In reply to the Court's question *to what extent safeguards have to be made public* the Government holds, with reference to the *Roman Zakharov* judgment, that states do not have to make public all the details of the operation of a secret surveillance regime in order to avoid abuses of power, provided that sufficient information is available in the public sphere (see §§ 243–244 and 247). As noted by the Chamber in *Big Brother Watch*, it is inevitable that not all safeguards are public (§ 326). Even if they are not made public, detailed internal regulations and routines nevertheless provide further important safeguards against abuse, especially if they are subject to independent supervision. As specifically concerns the signals intelligence regime in Sweden, it is pertinent to note that the supervision conducted by the Swedish Foreign Intelligence Inspectorate encompasses all internal regulations and routines, even those not available to the public. The FRA must also consult the Swedish Data Protection Authority concerning the FRA's internal regulations on processing of personal data. In addition, the FRA has a Privacy Protection Council

with the special task to monitor the FRA's internal regulations and routines. The Council's members are appointed by the Government.

The Court's question no. 2 d)

80. In response to the Court's question of *whether the same principles should apply to both content and related communications data*, the Government would like to state the following. As concerns the Swedish regime on signals intelligence within foreign intelligence, the Foreign Intelligence Act, the Signals Intelligence Act, the FRA Personal Data Processing Act and the related ordinances, regulate the collection and processing of communications data (including related communications data) as well as content data. Accordingly, no distinction is made between content and communications data in the legislation and a permit is required also for the collection and processing of communications data.

81. As noted by the Chamber (§§ 62 and 122), the selectors used for interception of communications data are generally less specific than those used for interception of the content of a communication. However, it must be borne in mind that the Foreign Intelligence Court's examination includes an assessment of the proportionality and necessity also of such selectors. Through the collection and processing of communications data, it is possible to rapidly gain an idea of the traffic between countries on a given signal, without having to examine the content of the communications or understand the language. Communications data is also used to establish a picture of normal communications patterns for reference when detecting anomalies.

82. Even when communications data is collected in order to provide a detailed picture of the communication patterns of a specific individual, which may reveal information that is sensitive and private, a greater degree of intrusion is always involved if the content of the individual's communication is examined. Consequently, the Government holds that intercepting communications is in general more intrusive than obtaining communications data (see *Malone v. the United Kingdom*, 2 August 1984, § 84, Series A no. 82).

1.2.2.1 Accessibility of domestic law

83. All legal provisions relevant to signals intelligence have been officially published and are accessible to the public and the Government notes that this fact has not been questioned by the applicant (see the Chamber judgment, § 115).

1.2.2.2 Scope of application of signals intelligence

84. The Court has held that national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures. The Court has furthermore stated that the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (*Roman Zakharov*, §§ 243 and 247, with further references).

85. The Government wishes to reiterate that foreign intelligence may only be conducted in support of Swedish foreign, defence and security policy, and to identify external threats to the country. Furthermore, according to the Signals Intelligence Act signals intelligence within foreign intelligence may only be conducted for eight stipulated purposes and for development activities. The content of the Act is further elaborated upon in the preparatory works, which are an essential source of Swedish legislation (see Appendix 1, Section 4.1.1 and the Chamber judgment, § 120).

86. Moreover, the Government would like to point to the fact that signals intelligence conducted on fibre-optic cables may only concern communications crossing the Swedish border in cables owned by a network operator. Communications between a sender and a receiver in Sweden may not be intercepted, regardless of whether the source is airborne or cable-based (see the Chamber judgment, § 15 and 26 and Appendix 1, Section 4.1.4).

87. As concerns the FRA's signals intelligence development activities, the Government argues that these are as rigorously regulated – and subject to supervision to the same extent – as signals intelligence in general. The provisions applicable to foreign intelligence are also relevant to the development activities, including the requirement for tasking directives from the Government and the requirement of a permit issued by the Foreign Intelligence Court. The data obtained within the signals intelligence development activities may only be used in regular foreign intelligence if such use is in conformity with the purposes established by law and the applicable tasking directives.

88. Furthermore, the Swedish Data Protection Authority has found no evidence that personal data had been collected for purposes other than those stipulated for the signals intelligence activities (see Appendix 1, Section 5.2).

89. In this context, the Government notes that the Court has accepted that the requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness, and that such judicial authorisation may serve to limit the authorities' discretion (*Roman Zakharov,* cited above, § 249, and see further paras. 91–97 below).

90. In view of what has been stated above, the Government concludes that the legislation on signals intelligence within foreign intelligence indicates with sufficient clarity the scope of mandating and performing signals intelligence conferred on the competent authorities and the manner of its exercise (cf. *Roman Zakharov,* cited above, §§ 246 and 248 and see the Chamber judgment, §§ 118–124).

1.2.2.3 Authorisation of signals intelligence

91. As regards authorisation of secret surveillance measures, the Court has stated that it will take into account a number of factors in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation (*Roman Zakharov,* cited above, § 257). The Court has found that, although prior judicial authorisation of secret surveillance measures is not a requirement, it may serve to limit the authorities' discretion in interpreting the scope of mandating and performing such measures. As stated above, the Court has therefore held that prior judicial authorisation constitutes an important safeguard against arbitrariness (*Roman Zakharov*, cited above, § 249).

92. The Government firstly reiterates that signals intelligence conducted by the FRA must be authorised in advance by the Foreign Intelligence Court. The President of the Court is a permanent judge and the vice president and other members are appointed by the Government on four-year terms. Neither the Parliament nor the Government or other authorities may interfere with the court's decision-making, which is legally binding.

93. As a main rule, a court shall hold public hearings but, when secrecy applies, hearings may be held in private. Due to the nature of signals intelligence within foreign intelligence, the Court has accepted that, where there is a system of prior authorisation, sensitive aspects of the authorising body's activities are withheld from the public for as long as required in the individual case, in order not to defeat the purpose of the signals intelligence. However, such a procedure could only be accepted where there are adequate safeguards in place (see the Chamber judgment, § 136).

94. The Government argues that such safeguards are in place. Any lack of transparency due to the fact that the Foreign Intelligence Court's hearings are held in private is compensated by the presence of a privacy protection representative. Such a representative must be present during the court's examination, except in very urgent cases. The representative is either a present or former permanent judge or member of the Swedish Bar Association. He or she has access to all the case documents and may make statements. The representative does not appear on behalf of any individual concerned by the signals intelligence permit at issue, but protects the interests of the general public.

95. In this context, it may also be relevant to note that in exceptional instances the FRA itself may decide to grant a signals intelligence permit, if it is feared that applying for a permit from the Foreign Intelligence Court might cause delay or other inconvenience of critical importance for one of the specified purposes of signals intelligence. Such a decision must be followed by an immediate notification to the Foreign Intelligence Court and a subsequent rapid review, whereby the permit may be changed or revoked (cf. *Szabó and Vissy*, cited above, § 81, and see the Chamber judgment, § 140). If revoked, all data collected on the basis of that permit must be immediately destroyed. Furthermore, if the permit granted by the FRA also contains access to certain signals carriers, such access can only be effectuated by the Swedish Foreign Intelligence Inspectorate (see Appendix 1, Sections 4.2 and 4.6.1.3). The Inspectorate will thus have the possibility to estimate the legal aspects of the permit granted by the FRA. It is therefore clear that also this exception is subject to clear safeguards.

96. As regards the scope of the Foreign Intelligence Court's review, the Government would like to reiterate that, after receiving the Government's annual tasking directives and the competent authorities' detailed tasking directives, the FRA must submit an application for a permit in respect of each signals intelligence mission. In its applications, the FRA must specify not only the collection

assignment in question and the intelligence requirements, but also the signal carriers to which access is requested and the selectors – or at least the categories of selectors – that will be used. The Foreign Intelligence Court examines whether the mission is compatible with applicable legislation and whether the collection would be proportionate to the expected interference with personal integrity (see Appendix 1, Section 4.2). A permit must state the signals intelligence mission for which signals intelligence is permitted, which signal carriers and selectors may be used, and which other conditions are needed to limit interferences with personal integrity.

97. In view of the above, the Government holds that the provisions and procedures relating to the authorisation of signals intelligence within foreign intelligence provide sufficient guarantees against abuse (cf. *Roman Zakharov,* cited above, §§ 267 and 270, and see the Chamber judgment, §§ 133–141).

1.2.2.4 The duration of signals intelligence

98. The Court has held that it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled (*Roman Zakharov,* cited above, § 250, with further references).

99. The Government would like to reiterate that a permit for signals intelligence within foreign intelligence may be granted for a maximum of six months and that it may be extended, following a renewed examination, for six months at a time. The examination preceding a renewal encompasses a full review by the Foreign Intelligence Court. The Government thus holds that the legislation on signals intelligence within foreign intelligence gives clear indications of the period after which a permit will expire, and of the conditions under which it can be renewed.

100. As regards the circumstances in which interception must be discontinued, the following should be clarified.

- FRA may only conduct signals intelligence within foreign intelligence in accordance the Government's annual tasking directives and in accordance with detailed tasking directives issued by the Government, the Government

Offices, the Swedish Armed Forces, the Swedish Security Police or the National Operations Department of the Swedish Police Authority.
- If a tasking directive is revoked or expires, the FRA would have to terminate the collection even if there is a valid permit issued by the Foreign Intelligence Court.
- The Swedish Foreign Intelligence Inspectorate may decide that a signals intelligence collection must cease if, during an inspection, it is evident that the interception is not in accordance with a permit.
- A renewal of a permit requires a review of whether the conditions for the permit are still met.
- The FRA continuously reviews whether the specific personal data it has intercepted is still needed for its signals intelligence activities.

101. In this context, it is pertinent to reiterate that the purpose of signals intelligence within foreign intelligence is to obtain information and identify phenomena of relevance for foreign intelligence. In order to be able to do so, the signals intelligence missions by necessity often extend over a period of several years in order to make it possible to monitor a given phenomenon that is relevant to the objectives of signals intelligence within foreign intelligence (see above, paras. 13–24 and Appendix 1, Section 2). Hence, in this context, a duration of six months is a well-balanced time period for a permit.

102. To sum up, the Government argues that there are safeguards in place that adequately regulate the duration, renewal and cancellation of signals intelligence within foreign intelligence (cf. *Roman Zakharov,* cited above, § 252, and see the Chamber judgment, §§ 127–130).

1.2.2.5 Procedures to be followed for storing, accessing, examining, using and destroying the intercepted data

103. As regards the procedures to be followed for storing, accessing, examining, using and destroying intercepted data, it is relevant to determine whether national law contains clear rules, making it possible to minimise the risk of unauthorised access or disclosure (*Roman Zakharov,* cited above, § 254).

104. The Government would like to underline that the FRA must ensure that personal data is collected only for certain expressly stated and justified purposes, determined by the direction of the foreign intelligence activities through tasking directives. The personal data processed must also be adequate and relevant in

relation to the purpose of the processing, and no more personal data than is necessary for that purpose may be processed. All reasonable efforts must be made to correct, block or delete personal data that is incorrect or incomplete in relation to the purpose. Furthermore, the FRA staff who process personal data undergo vetting and, if secrecy applies to the personal data, have a duty of confidentiality. They are under an obligation to handle the personal data in a secure manner. Access to data is limited by the official's level of authorization and his or her need for the data in order to fulfil a work assignment. If they mismanage tasks relating to the processing of personal data, they could also face criminal sanctions. Furthermore, all measures taken by those processing the data are logged, which provides protection against improper handling of personal data.

105. Furthermore, it is pertinent to reiterate that there are clear provisions regulating the situations in which intercepted data must be destroyed. For example, intelligence must be destroyed immediately if it 1) concerns a specific natural person and it has been determined that it lacks importance for the purpose of the signals intelligence, 2) is protected by constitutional secrecy provisions for the protection of anonymous authors or media sources, 3) contains information shared between a criminal suspect and his or her counsel and is thus protected by legal professional privilege, or 4) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information. Moreover, if communications have been intercepted between a sender and receiver both in Sweden, they must be destroyed as soon as their domestic nature has become evident. In addition, where a temporary permit granted by the FRA has been revoked by the Foreign Intelligence Court, all data collected on the basis of that permit must be immediately destroyed. The logs in the FRA's computer system contain the time and reason for destruction, the identity of the person who carried out the destruction and what kind of material that was destroyed. The Swedish Foreign Intelligence Inspectorate shall, inter alia, control the FRA's destruction of data. For more details, see Appendix 1, Section 4.6.1.

106. The FRA has developed clear routines for reviewing the personal data processed, and for assessing when personal data is no longer required for operational purposes and must therefore be discarded[3]. It should also be recalled

[3] According to decisions from the National Archives report data and intelligence reports of the FRA are to be retained for historical, statistical and scientific purposes (see Appendix 1, Section 4.4.1).

that supervision of the processing of personal data is exercised by the Swedish Foreign Intelligence Inspectorate and the Swedish Data Protection Authority.

107. In the FRA's foreign intelligence and development activities, personal data are as a rule processed in data compilations. The data compilations that may be held are exhaustively listed in the legislation, which also contains clear rules on how long the data can be retained in each of the compilations (see Appendix 1, Section 4.4.1).

108. As specifically regards data compilations for raw material, the FRA may retain personal data in such data compilations for up to one year. However, it has to be kept in mind that raw material is unprocessed information which has yet to be subjected to manual processing. The Government argues that it is necessary for the FRA to store raw material before it can be manually processed (see the Chamber judgment, § 146).

109. In view of what is stated above, the Government holds that the legislation on storing, accessing, examining, using and destroying intercepted data provides adequate safeguards against abuse of personal data processing and thus serves to protect individuals' personal integrity (cf. *Roman Zakharov*, cited above, §§ 253–256 and see the Chamber judgment, §§ 144–147).

1.2.2.6 Conditions for communicating the intercepted data to other parties

110. The Court has found that it naturally follows from the purpose of signals intelligence that its result is reported to concerned national authorities, in particular the authority which issued the tasking directives. The Court has furthermore held that it is evident that there must be a possibility of exchanging intelligence collected with international partners, given the context (see the Chamber judgment, § 150).

111. The FRA has a regulated obligation to report to the Swedish authorities concerned. However, it is important to stress that personal data concerning a specific individual may only be reported if it is of relevance for the purposes for which foreign intelligence may be conducted (see Appendix 1, Section 4.5.1). It is clearly stated in the Signals Intelligence Act that the Swedish Foreign Intelligence Inspectorate is specifically tasked to control the FRA's reporting.

112. As concerns the communication of personal data to other states and international organisations, the Chamber considered that the there was a lack of

specification in the provisions on signals intelligence in this regard, but that supervisory elements sufficiently counterbalanced the regulatory shortcomings (see the Chamber judgment, § 150). The Government does not agree that there are shortcomings and will therefore provide a few clarifications below.

113. Swedish legislation is in conformity with Sweden's international obligations. The Government would like to point out that there are provisions on the transfer of personal data to other countries in the Additional Protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 181). Under Article 2, paragraph 1, a party to the Convention may only allow the transfer of personal data to a recipient that is subject to the jurisdiction of a state or organisation that is not party to the Convention if that state or organisation ensures an adequate level of protection for the intended data transfer. By way of derogation from paragraph 1, a party may allow the transfer if it is permitted under domestic law because of the specific interests of the data subject, or where there are legitimate prevailing interests, especially important public interests. Sweden is a party to the Convention and the Additional Protocol.

114. The Foreign Intelligence Act and Ordinance, the Signals Intelligence Act and Ordinance and the FRA Personal Data Processing Act and Ordinance all contain provisions on which conditions the FRA may co-operate with other states and international organisations. Co-operation may only be conducted if the purpose is of benefit to the Swedish Government and Sweden's comprehensive defence strategy. The legislation furthermore only permits that the FRA communicates data to other states and international organisations as long as it does not harm Swedish interests. The communication of personal data to other states or international organisations may only occur if it provides added value for the FRA's support of Swedish foreign intelligence and enhances its capabilities to meet the requirements of the tasking directives or if it is necessary for the activities of the FRA within international defence and security cooperation, and as long as it is not prevented by secrecy. The Government may decide to communicate personal data to states or organisations in other cases when necessary for the activities of the FRA. These requirements serve to limit the scope for the transfer of data to other states and international organisations.

115. The FRA must report to the Ministry of Defence before it establishes and maintains cooperation with other states and international organisations and inform the ministry about important issues that occur within a cooperation. Furthermore,

the FRA must inform the Swedish Foreign Intelligence Inspectorate of the principles that apply to its cooperation on intelligence matters with other countries and international organisations, and provide details of the countries and organisations with which such cooperation takes place. When cooperation is established, the FRA must inform the Inspectorate of the scope of the cooperation and, where deemed warranted, of the results, experience and continued direction of the cooperation.

116. Given the context that the data is exclusively communicated to parties that are themselves engaged in foreign intelligence – there is a corresponding need and interest at the recipient's end to protect the data received. The trust between the parties is based on a mutual interest in maintaining the security of the data. These facts evidently also serve the purpose of safeguarding the integrity of any individual concerned.

117. To sum up, the Government holds that the legislation on communicating data to others provides adequate safeguards against abuse of processing of personal data, and thus serves to protect individuals' personal integrity.

The Court's question no. 3, second and third sentences

118. In response to the Court's question of *whether the legal regime applicable in Sweden to communicating intercepted data to other parties is in accordance with the law and necessary within the meaning of Article 8 § 2*, the Government holds, with reference to what has been stated above in paras. 110–117, that any possible interference is in accordance with the law and necessary.

119. As regards the Court's question concerning *the extent to which the standards developed in the Court's case-law on secret measures of surveillance apply to the legal regime applicable in Sweden to communicating intercepted data to other parties*, the Government notes that one of the minimum safeguards developed in the Court's case-law does indeed concern communication of data *to* other parties (see *Roman Zakharov,* cited above, § 238) and that the Court has held that precautions should be taken in order to provide adequate safeguards for the protection of data in this context (see *Kennedy,* cited above, § 163). The Government argues, in view of what is stated above in paras. 110–117, that the Swedish legal regime provides such adequate safeguards.

1.2.2.7 Supervision of the implementation of signals intelligence

120. The Court has found that supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control (see *Roman Zakharov*, cited above, § 275, with further reference).

121. With respect to the requirement of independence, the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. As regards the supervisory body's powers and competence, the Court has held that it is essential that it has access to all relevant documents, including closed materials, and that all those involved in interception activities have a duty to disclose to it any material required. Other important elements to take into account when assessing the effectiveness of the supervision are the supervisory body's powers with respect to any breaches detected and the possible scrutiny of its activities (*Roman Zakharov,* cited above, §§ 278 and 281–283, with further references).

122. The Swedish Foreign Intelligence Inspectorate is independent. It has the task of supervising the signals intelligence conducted by the FRA. The members of the board of the Inspectorate, which may be a maximum of seven, are appointed by the Government for terms of at least four years and the president and vice-president are current or former permanent judges. The other members are proposed by the parliamentary party groups.

123. The Inspectorate has access to all relevant documents and is in particular to examine the selectors used, the destruction of data and the FRA's reporting to competent authorities. It is within the Inspectorate's powers to decide that the data collection must cease, or that data collected must be destroyed if, during an inspection, it becomes evident that the data has not been collected in accordance with a particular permit. The Inspectorate is also in charge of providing access to the signal carriers, which includes ensuring that the FRA is only provided access to signal carriers insofar as such access is covered by a permit. The Inspectorate has an additional supervisory function concerning the FRA's processing of personal data. The Inspectorate is to forward any opinions or suggestions for measures to which the inspections give rise to the FRA, and if necessary, to the Government. For further details, see Appendix 1, Sections 4.6.1 and 4.7.2.

124. Concerning public scrutiny, the Inspectorate submits annual reports to the Government on its activities. These reports are available to the public. The Inspectorate's activities are also subject to audit by the National Audit Office and supervision by the Parliamentary Ombudsmen and the Chancellor of Justice. The National Audit Office has found that the Inspectorate has been able to carry out its supervisory task efficiently and that the FRA has taken the Inspectorate's views and suggestions seriously and has implemented measures based on them (see the Chamber judgment, § 40 and Appendix 1, Section 4.6.1.2).

125. As regards personal data, the Swedish Data Protection Authority has general supervisory functions (see Appendix 1, Sections 4.6.2 and 4.7.6). The Authority has submitted two special reports published in 2010 and 2016, stating that issues of personal data and personal integrity had generally been dealt with in a satisfactory manner (see the Chamber judgment, §§ 59–60 and Appendix 1, Section 5.2).

126. Taking into account the manner of appointment and the legal status of the members of the Swedish Foreign Intelligence Inspectorate, the Government holds that the Inspectorate is independent. In view of what is stated above, the Government further argues that the Inspectorate is vested with sufficient powers and competence to exercise an effective and continuous control and that its activities are open to public scrutiny. Moreover, the report of the National Audit Office shows that the Inspectorate's supervision is effective, not only in theory but also in practice. Considering also the supervision provided by the Swedish Data Protection Authority, the Parliamentary Ombudsmen and the Chancellor of Justice, the Government holds that the supervision of the implementation of signals intelligence provides sufficient guarantees against abuse (cf. *Roman Zakharov,* cited above, § 285, and see the Chamber judgment, §§ 153–161).

The Court's question no. 2 c)

127. As regards the Court's question of *whether Article 8 § 2 requires supervision and review by an independent body and, if so, what level of independence from the Government is needed,* the Government finds that the standards concerning supervision and review developed in the Court's case-law are reasonable (see *Roman Zakharov,* §§ 275, 278 and 281–283). The Government holds that supervision by non-judicial bodies should be considered compatible with the Convention, especially when there is a judicial permit procedure.

1.2.2.8 Notification of signals intelligence and available remedies

128. Like the Chamber, the Government finds it relevant to examine the issue of notification together with available remedies; two issues that are inextricably linked (see the Chamber judgment, § 167, and *Roman Zakharov*, cited above, § 286).

129. The Court has found that it may not be feasible in practice to require subsequent notification in all cases, for the following reasons. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (see *Roman Zakharov*, cited above, § 287, with further references, and *Kennedy,* cited above, § 167).

130. Furthermore, the Venice Commission has found that notification is not an absolute requirement of Article 8 of the Convention, and that a general complaints procedure to an independent oversight body could compensate for non-notification.

131. The Government would firstly like to reiterate the fact that the FRA is obliged to inform a natural person if selectors directly related to him or her have been used, and of when and why the collection took place. The person must be notified as soon as this can be done without detriment to the foreign intelligence activities, but at the latest one month after the signals intelligence mission was concluded. However, the obligation to notify does not apply where secrecy applies (see Appendix 1, Section 4.7.1).

132. Also, the Government wishes to emphasise the control carried out by the Swedish Foreign Intelligence Inspectorate upon request by an individual of

whether his or her communication has been collected in connection with signals intelligence (see paras. 39–41 above). The Inspectorate may decide on the discontinuation of data collection or the destruction of data. If deficiencies are discovered that may incur liability for damages for the state, a report must be submitted to the Chancellor of Justice. This remedy is not dependent on prior notification (cf. *Kennedy,* cited above, § 167). 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.

133. Moreover, it is relevant to note the control carried out by the FRA upon request by an individual of whether personal data concerning him or her has been processed (see para. 46 above). There are also several remedies of a general nature that are relevant in this context, namely the possibility to apply to the Parliamentary Ombudsmen, the Chancellor of Justice or the Swedish Data Protection Authority, the possibility to bring an action for damages, the possibility to report a matter for prosecution and the possibility to bring a claim for compensation for violations of the Convention (see paras. 42–45 above).

134. In sum, the Government holds that there are several remedies by which an individual may initiate an examination of the lawfulness of measures taken during the operation of the signals intelligence system. In this connection, it is also relevant to reiterate the earlier stages of supervision of the signals intelligence regime, including the detailed judicial examination by the Foreign Intelligence Court and the extensive and partly public supervision by several bodies, in particular the Swedish Foreign Intelligence Inspectorate. The Government argues that the aggregate of remedies is sufficient in the present context, which involves a request for an examination of the legislation on signals intelligence *in abstracto* and does not concern a complaint against a particular intelligence measure (cf. *Roman Zakharov,* cited above, § 300, and see the Chamber judgment, §§ 164–167 and 171–178).

The Court's question no. 2 e)

135. Concerning the Court's question on *individual requests for review after the impugned intelligence has been carried out*, the Government holds, in view of what has been stated above in paras. 129–134, that the system applicable in Sweden meets the relevant Convention requirements.

1.3 Conclusion

136. When examining the Swedish regime on signals intelligence within foreign intelligence *in abstracto*, consideration should be given to the relevant legislation and the other information available in order to assess whether, overall, there are sufficient minimum safeguards in place to protect the public from abuse. Consideration should also be given to the margin of appreciation enjoyed by the national authorities in protecting national security. In that context it is relevant to reiterate that the Venice Commission has noted the value that signals intelligence regimes could have for security operations, since it enables the competent authorities to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones.

137. The Government holds that the regime on signals intelligence within foreign intelligence reveals no significant shortcomings in its structure and operation. The regulatory framework on signals intelligence minimises the risk of interference with privacy and compensates for the lack of openness inherent in any secret surveillance regime. In particular, the scope of the signals intelligence measures and the treatment of intercepted data are clearly defined in law, the authorisation procedure is detailed and entrusted to a judicial body, and there are several independent bodies tasked with the supervision and review of the system.

138. Accordingly, the Government argues that the Swedish system of signals intelligence within foreign intelligence provides adequate and sufficient guarantees against arbitrariness and the risk of abuse. The relevant legislation meets the "quality of law" requirement and any possible interference is "necessary in a democratic society". Furthermore, the structure and operation of the regime are proportionate to the legitimate aim of protecting national security. Consequently, the Government holds that there is no violation of Article 8 of the Convention.

2. Article 13

139. While the Government agrees with the Chamber that the present complaint raises no separate issue under Article 13 of the Convention, it would nevertheless like to clarify its view concerning Article 13 (see the Chamber judgment, § 184).

2.1 Article 13 is not applicable

140. 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 *Weber and Saravia*, cited above, § 155).

141. In view of this, the Government argues that it takes more than mere *concern* that it has been subjected to signals intelligence within foreign intelligence for the applicant to establish an arguable claim for the purposes of Article 13. Further, the Government would like to reiterate that it considers that the applicant cannot claim to be a victim of a violation of Article 8 occasioned by the mere existence of Swedish legislation concerning signals intelligence within foreign intelligence (see paras. 32–52 above). Consequently, the Government holds that the applicant has no arguable claim for the purposes of Article 13.

142. If the Court were to find that the applicant could 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*, 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 can claim to be a victim of a violation of Article 8, it has no arguable claim for the purposes of Article 13.

143. If the Court were to find that the applicant has an arguable claim for the purposes of Article 13 of the Convention, the Government would like to emphasise once again that the present complaint concerns a 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 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*, cited above, § 197). Furthermore, 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. *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, §§ 3 and 121, ECHR 2006-VII and, *mutatis mutandis*, *Kennedy*, cited above, § 155).

144. In view of this, the Government argues that the applicant's *concerns* about being subjected to signals intelligence do not require that it should have access to an effective remedy within the meaning of Article 13. Consequently, Article 13 is not applicable in the present case. In any event, the Government holds that the applicant has had effective remedies at its disposal.

2.2 There are effective remedies available to the applicant

145. Where an individual does have an arguable claim to be the victim of a violation of the rights set forth in the Convention, he or she should have a remedy before a national authority in order both to have his or her 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, even if no single remedy itself entirely satisfies the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so (see *Klass and Others v. Germany*, 6 September 1978, § 67, Series A no. 28, *Leander*, cited above, § 77, and *Nada v. Switzerland*, [GC], no. 10593/08, § 207, ECHR 2012).

146. 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 it can be, having regard to the restricted scope for recourse inherent in such a system (see *Klass*, § 69; *mutatis mutandis*, *Leander*, § 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*, no. 62540/00, § 99 28 June 2007).

147. Moreover, it is relevant to note that, in the context of secret surveillance measures, the Court has in several cases concluded 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*, § 68, and, *mutatis mutandis*, *Leander*, § 78, cf. *Mersch*, § 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.

148. Turning to the facts of the present case, the Government wishes to refer to the account of remedies outlined in the Government's description on domestic law and practice (Appendix 1). In particular, the Government wishes to draw the Court's attention to the following.

149. A primary remedy available to any individual (including businesses and organisations), is the possibility to make a request to the Swedish Foreign Intelligence Inspectorate. Upon such a request, the Inspectorate must control whether the requesting party's communications have been the subject of signals intelligence (see paras. 39–41 above and cf. *Kennedy*, cited above, § 167).

150. Furthermore, if, in the course of its supervision, the Swedish Foreign Intelligence Inspectorate notices circumstances that may constitute a criminal offence, the Inspectorate must report this to the Swedish Prosecution Authority (Prosecutor-General). If there is cause to believe that an offence has been committed, a prosecutor must initiate a preliminary investigation and must thereafter – if the conditions are met – prosecute the offence. 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 the FRA Personal Data Processing Act. If the Swedish Foreign Intelligence Inspectorate discovers circumstances that should be brought to the attention of the Swedish Data Protection Authority, the Inspectorate must report this to the Authority. The Authority is responsible for working to ensure that people are protected against violations of their privacy via processing of personal data. For further details, see Appendix 1, Section 4.6.2.

151. It is also relevant to reiterate that the FRA is obliged to provide information free of charge, once per calendar year, to any individual who applies, about whether or not personal data concerning the applicant is being processed (see para. 46 above).

152. Additionally, an individual has the possibility to apply to the Parliamentary Ombudsmen, the Chancellor of Justice or the Swedish Data Protection Authority, the possibility to bring an action for damages, the possibility to report a matter for prosecution and the possibility to bring a claim for compensation for violations of the Convention (see Appendix 1, Section 4.7).

153. Moreover, the principle of public access to official documents applies to foreign intelligence and thus to the signals intelligence conducted by the FRA. A decision by the FRA 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 Appendix 1, Sections 4.7.3 and 5.1). 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.

154. To sum up, several remedies are open to an individual who believes that he or she has been subjected to signals intelligence. In the Government's view, these remedies are effective considering the context of signals intelligence within foreign intelligence (cf. *Klass*, cited above, §§ 70–71, and cf. *Segerstedt-Wiberg,* cited above, § 120). Furthermore, 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*, cited above, § 155). Hence, 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 (cf. *Leander*, cited above, § 84 and *Klass*, cited above, § 72). Consequently, there is no violation of Article 13 in the present case.

2.3 Conclusion

155. With reference to what has been submitted in paragraphs 140–154 above, the Government holds that the applicant'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. Thus, Article 13 is not applicable in the present case. In any event, the applicant has had effective remedies at its disposal and the case consequently reveals no violation of Article 13 of the Convention.

V. Conclusions

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

concerning the **admissibility**,

– that the applicant's complaint regarding "receiving information from other parties" should be declared inadmissible *ratione materiae*,

– that the rest of the application should be declared inadmissible

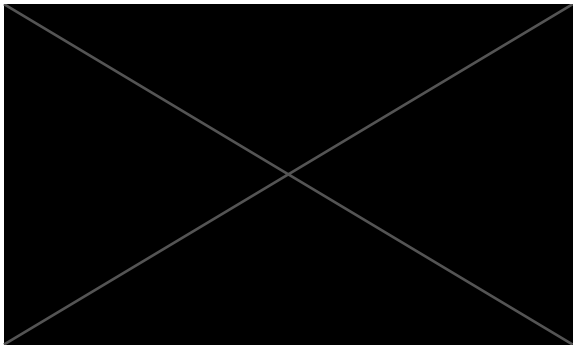
– *ratione personae,* since the applicant cannot claim to be a victim of a violation of the Convention, or

– *ratione materiae,* since neither Article 8 nor Article 13 is applicable, and, in any event,

– as being manifestly ill-founded; and

concerning the **merits**,

– that the case reveals no violation of the Convention.



Appendices

1. Domestic Law and Practice
2. List of relevant legislation (Acts and Ordinances)
3. List of relevant authorities