REGERINGSKANSLIET

Stockholm, 25 January 2013
UDFMR2012/144/ED

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

IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application no. 35252/08

Centrum för rättvisa

v.

Sweden

SUPPLEMENTARY OBSERVATIONS OF THE GOVERNMENT OF SWEDEN ON ADMISSIBILITY

---

1. These supplementary observations on the admissibility of the application introduced by Centrum för rättvisa (hereinafter the applicant firm) are submitted on behalf of the Swedish Government in response to the letter from the Court dated 6 November 2012, in which the Government is informed that its request to submit supplementary observations is granted.

Introduction

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

3. In this context, the Government would like to refer to the significance of the principle of subsidiarity. An important aspect of this principle is that the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights.

4. The Government would furthermore like to reiterate that in order to assess, in a particular case, whether an individual can claim to be a victim of a violation of the Convention as a result of the mere existence of legislation permitting secret surveillance measures, the Court has found that regard must be had to the availability to the public of any remedies at national level and the risk of secret surveillance measures being applied to him (see recent judgment *Hadzhiev v. Bulgaria*, no. 22373/04, §§ 38–40, 23 October 2012, and the authorities cited therein).

Right to respect for private life

5. The applicant firm has stated that it considers it a major interest in a modern democracy to entitle the applicant firm, and other legal persons in general, to a private life within the meaning of Article 8 of the Convention. In this connection the applicant firm has indicated that the establishment and development of relationships with natural persons is a key element in its

existence, with reference to the case of *Gillberg v. Sweden* (*Gillberg v. Sweden* [GC], no. 41723/06, § 66, 3 April 2012).

6. Although the rights and freedoms laid down in the Convention may apply to both natural and legal persons, the Government contends that some of the rights and freedoms are by their nature not susceptible of being exercised by a legal person. The Court has held that the concept of private life is a broad term not susceptible to exhaustive definition. The Court has however, through its case-law, provided some guidance as to the meaning and scope of the concept of private life for the purposes of Article 8 (see *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 66, ECHR 2008, and the authorities cited therein). In this regard, the Court has held that the concept of private life covers the physical and psychological integrity of a person and that it therefore can embrace multiple aspects of the person's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8. Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family. Information about the person's health is an important element of private life. The Court has furthermore considered that an individual's ethnic identity must be regarded as another such element. The concept of private life moreover includes elements relating to a person's right to their image.

7. Furthermore, the Court has held that the right to respect for private life afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his or her relations with other human beings (see *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 95, ECHR 2012).

8. Looking at how the meaning and scope of the concept of private life within the meaning of Article 8 has been developed through the case-law of the Court, the Government holds that the Court's case-law supports the conclusion that the right to respect for private life is by its nature not susceptible of being exercised by a legal person (cf. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* no. 62540/00, § 60, 28 June 2007 and *Asselbourg and Others v. Luxembourg* (dec.), no. 29121/95, ECHR 1999-VI). In this context, the Government finds it pertinent to reiterate that *Gillberg v. Sweden* (cited above), referred to by the applicant firm, concerned a natural person. Hence, no conclusions can be drawn from this judgment as to whether a legal person can exercise the right to private life.

9. Moreover, the applicant firm has held that the fact that secret surveillance of communications interfered with both the respect for private life and correspondence regarding legal persons was not a matter of dispute in *Liberty and Others v. the United Kingdom* (no. 58243/00, §§ 56–57, 1 July 2008). It may be reiterated that the Government of the United Kingdom had stated in that case that it was prepared to proceed on the basis that the applicants could claim to be victims of an interference with their communications sent to or from their offices. The Court considered that the existence of the intercepting powers in question constituted an interference with the Article 8 rights of the applicants. However, the Court did not state which Article 8 rights were concerned, and hence did not explicitly state that there had been an interference with the right to respect for private life. The Government therefore contends that no conclusions can be drawn from this judgment as to whether a legal person can exercise the right to private life.

10. Consequently, the Government maintains that the only Article 8 right at issue in the present case is the applicant firm's right to respect for its correspondence.

Remedies available to the public at national level

11. The applicant firm has pointed to the fact that the signals intelligence regime is different from the situation where secret measures are being applied to a person during a Swedish criminal investigation, in that the person in question in a criminal investigation is informed *post facto* of the fact that he or she has been subjected to interception. In this context, the Government would like to reiterate that signals intelligence is not a measure used in criminal investigations. Signals intelligence is a tool for foreign intelligence operations and may only be used for specific purposes within those operations.

12. In reply to the applicant firm's contention that it was not until the second and third periods that there were any legislative attempts to provide adequate safeguards against abuse, the Government would like to draw the Court's attention to the fact that over and above the general supervision bodies, the Swedish Intelligence Commission has had the task of monitoring foreign intelligence operations since 1976 (see para. 49 of the Government's observations of 27 April 2012, hereinafter 'the Government's initial observations'). In 2009, the Swedish Intelligence Commission changed its name to the Swedish Foreign Intelligence Inspectorate.

13. The applicant firm has alleged that although some of the members of the Swedish Foreign Intelligence Inspectorate have been suggested by the opposition in the Riksdag, no parties in opposition other than the Social Democratic Party are represented on the Board of the Inspectorate. In this connection, the Government would like, once again, to describe the organisation of the Swedish Foreign Intelligence Inspectorate. The Board of the Swedish Foreign Intelligence Inspectorate is led by a Chairman and Vice Chairman, both of whom must be senior lawyers or (former) permanent judges. This is to ensure that the Swedish Foreign Intelligence Inspectorate has judicial expertise. The other five members of the board are proposed by the Riksdag party groups. Hence, the parties represented in the Riksdag, including the parties in opposition, are able to affect which parties are represented on the Board of the Swedish Foreign Intelligence Inspectorate. The Government, however, has no influence on this matter.

14. Moreover, the applicant firm has contended that the Foreign Intelligence Court lacks many of the criteria that constitute a court within the meaning of Article 6 of the Convention. In this context, the Government would like to draw the Court's attention to the organisation and tasks of the Foreign Intelligence Court. The Chair of the Foreign Intelligence Court is a permanent judge. The other members are appointed by the Government for a period of four years. The Foreign Intelligence Court has been established to further strengthen due process and privacy protection. Its main task is to consider whether the conditions for issuing permits for signals intelligence are satisfied. The court's examination is to ensure that signals intelligence assignments are not in any way incompatible with the legislation. The court does not, however, determine the civil rights and obligations of any individual, or any criminal charges against individuals. The Foreign Intelligence Court therefore does not have the task stated in Article 6 of the Convention. In addition, the Government finds it pertinent to emphasise that the Foreign Intelligence Court is an independent court and that neither the Riksdag, nor a public authority, may determine how the court shall adjudicate an individual case or otherwise apply a rule of law in a particular case (see Chapter 11, Article 3 of the Instrument of Government).

15. The applicant firm has invited the Government to substantiate its contentions regarding the possibilities for a legal person to request a control if it has been subjected to interception unlawfully or if personal information has been processed by the National Defence Radio Establishment. As the Government stated in its initial observations (see para. 103), the Data Inspection Board may examine complaints that concern the processing of

personal data, i.e. information relating to an identified or identifiable natural person. In addition, under the Signals Intelligence Act (2008:717) a request to the Swedish Foreign Intelligence Inspectorate for a control may be made by an individual, regardless of nationality, place of residence or whether the individual is a natural or legal person (see para. 91 of the Government's initial observations).

16. The applicant firm is correct in asserting that to date no notification under Section 11a of the Signals Intelligence Act has taken place. It is also correct to assert that the operations of the National Defence Radio Establishment are largely surrounded by strict secrecy. The regulations concerning duty of notification and the exemptions available are based on careful consideration of what can be communicated without revealing the objectives and means of Swedish foreign intelligence operations, while at the same time respecting individual privacy as far as possible. An unconditional duty of notification would entail a great risk of damage to Swedish foreign intelligence. Notification reveals not only the tasking directives of foreign intelligence and thus Swedish foreign intelligence needs, but also the collection ability and technical capacity. An exemption from the duty of notification with reference to secrecy is thus a condition for effective foreign intelligence.

17. The applicant firm has questioned the reliability of any scrutiny *post facto* since it will depend on the material scrutinised and the moment in time when the control is carried out. In this context, the Government would like to draw the Court's attention to the fact that the control conducted by the Swedish Foreign Intelligence Inspectorate at the request of an individual refers to the collection of the individual's messages. The control would concern messages that, through the selection process involving selectors, have become available to the signals intelligence agency for further processing and analysis. The scope of the type of control requested by the applicant firm, for example control of messages not selected for further processing and analysis, would involve considerable processing and significantly increased intrusion into the privacy of a large number of individuals. This would naturally run counter to the interest of privacy protection.

18. As has been described in the Government's initial observations as well as above, there is an established system of permanent control mechanisms and supervisory elements as regards signals intelligence. When the legislation that entered into force as from the third period was adopted by the Riksdag, the Riksdag was, however, of the view that, from a privacy protection perspective,

there was a need for special follow-up (a temporary control mechanism). This special follow-up was conducted by the parliamentary Signals Intelligence Committee and the Data Inspection Board. Furthermore, the Government is required to report annually on the review of operations conducted under the Signals Intelligence Act. The report is made in a special written communication from the Government to the Riksdag (*regeringens skrivelse*). This has been done in 2010 (*Regeringens skrivelse 2010/11:41 Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet*) for the years 2009 and 2010, in 2011 (*Regeringens skrivelse 2011/12:48 Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet*) and most recently in December 2012 (*Regeringens skrivelse 2012/13:59 Integritetsskydd vid signalspaning i försvarsunderrättelse-verksamhet).*

19. In its 2011 communication, the Government also reports the results of the follow-up and examination of signals intelligence in foreign intelligence operations decided on by the Government and implemented by the Data Inspection Board and the parliamentary Signals Intelligence Committee. Also, in the communication the Government states that, as a complement to on-going follow-up, it intends within a few years to instruct the Swedish Foreign Intelligence Inspectorate to conduct a new in-depth follow-up of the signals intelligence performed by the National Defence Radio Establishment.

20. In its response to the 2011 Government communication, the Riksdag noted that the scrutiny made of signals intelligence activities conducted by the National Defence Radio Establishment was functioning effectively. Furthermore, the Riksdag welcomed the Government's announcement of a forthcoming in-depth follow-up of the signals intelligence performed by the National Defence Radio Establishment. The Riksdag considered that such an in-depth follow-up should be presented to the Riksdag (*Försvarsutskottets betänkande, bet. 2011/12:FöU6, rskr. 2011/12:179*).

21. Thus, apart from the existing permanent control mechanisms and supervisory elements, which are viewed as well-functioning by the Riksdag, temporary control mechanisms will also be conducted in the future.

22. In conclusion, the Government maintains that the control mechanisms, supervisory elements and remedies described in the Government's initial observations and above provided possibilities for the public to challenge the signals intelligence work conducted by the National Defence Radio Establishment during all three time periods. Hence, the secrecy of such activities did not result in these activities being effectively unchallengeable and outside the supervision of the national authorities and the Court.

Risk of secret surveillance measures being applied to the applicant

23. The applicant firm has contended that, during the first time period, there were no detailed provisions in Swedish law regarding when or how signals intelligence could be conducted. As the Government has already explained in its initial observations (see paras. 40–54), foreign intelligence operations were regulated during this period by various acts and ordinances. Even during this time period there was a clear regulatory framework which stated the purposes for which signals intelligence in foreign intelligence operations could be conducted. Foreign intelligence operations were undertaken to identify external military threats against the country and to support Swedish foreign, security and defence policy. It is therefore incorrect to assert that there was virtually no regulation during the first time period.

24. The Government has also described the regulatory framework for the second and third time periods in its initial observations (see paras. 55–65 and 72–87). The purposes for which signals intelligence may take place were clarified and defined as from the second period in the Signals Intelligence Act and in the Signals Intelligence Ordinance (2008:923). The term *external threats against the country* was explained – as is customary in a Swedish legislative context – in the preparatory materials for the Act, from which it was evident that these threats, as in the previous Act, were of a military nature, but also included terrorism and the proliferation of weapons of mass destruction. However, the threat must be of such a sophisticated nature that it can be considered to be targeted at national security or structures that are vital to the functioning of society.

25. Foreign intelligence operations are hence undertaken to identify external military threats against the country and to support Swedish foreign, security and defence policy. In addition, operations are required to support Swedish participation in international security cooperation and strengthen society in times of severe peacetime emergencies. The Government fails to see that the applicant firm's activities have anything whatsoever to do with these purposes.

26. The applicant firm is correct in asserting that even prior to 1 January 2009 there was traffic of interest to the National Defence Radio Establishment, on mobile telephony networks for example. However, at this time signals intelligence in foreign intelligence operations only took place over the air and the purposes of foreign intelligence operations specified by law

still had to be met (cf. paras. 23–25 above). The focus was, and is still, on foreign circumstances.

27. In this context, the Government finds it pertinent to clarify some technical aspects as concerns the conditions for signals intelligence over the air. When radio waves are broadcast freely on the airwaves, it follows from the laws of physics that anyone can set up an antenna and pick up the signal in the area where it is sufficiently strong to be received. In Sweden there are no restrictions on the possession and use of radio receivers (unlike radio transmitters) (see Chapter 3 of the Electronic Communications Act [2003:389]). Many different types of receivers capable of receiving a broad range of frequencies ('scanners') are available for purchase from retailers.

28. Anyone transmitting a radio wave signal is therefore taking a risk that someone will listen in on the signal. Hence, there is no protection from interception of the transmitted signal in the wireless segments of an operator's network, no matter whether it is the state or some other party that is intercepting signals. Consequently, in practice, some form of encoding or encryption is required to protect the contents of the signal from being understood. Such protection can be provided by the operator. Some radio systems (e.g. GSM, UMTS and RAKEL, the civil defence and emergency services network) use encryption, while others (e.g. civil aviation and maritime systems) do not.

29. The way in which a mobile telephony/mobile broadband network functions is that it is the access, i.e. the connection between the user's terminal (e.g. mobile telephone) and the edge node of the network (the base station), that is wireless. The network has a cellular structure, so that a terminal can move between the coverage areas (cells) of different base stations without the conversation or communication being interrupted. The base stations are connected with the network by fibre cable or fixed wireless link (fixed point-to-point radio communication).

30. In practice, intercepting communications in mobile telephone networks by wireless means is impossible. It would require an antenna in every cell so that a terminal could be followed when it moves in the network. By the same token, intercepting communications via just one link between a base station and the network would not be particularly meaningful. To be able to follow a conversation, interception equipment needs to be installed at higher levels in the network (switches and transport networks).

31. The applicant firm has contended that there is no technical possibility to distinguish radio signals other than by frequency bands. In this context, the Government would like to clarify that if a radio receiver is set to a certain frequency, it picks up the signals existing at that frequency. The way modern digital radio technology works is that many data streams are multiplexed into a single channel. If the channel is picked up, given the necessary technical knowledge, it can be demultiplexed and only the streams that are of interest can be separated out.

32. Naturally, a client of an operator of an electronic communications network that is open to the public has little possibility in practice to check that the signals are transmitted in the network in a manner that is secure from interception. Chapter 6, Section 3 of the Electronic Communications Act states that the operator must maintain a high security level. The Swedish Post and Telecom Agency (*Post- och telestyrelsen*) supervises compliance with this provision, which is the protection provided to the individual client. It is conceivable that clients with special needs enter into commercial agreements on even higher levels of protection. Individuals using mobile broadband internet connections may also set up encrypted Virtual Private Networks (VPNs) in order to make their communications more secure.

33. The Government does not dispute that the applicant firm has used wireless networks for its communications. In light of what is said above about the technical conditions for signals intelligence and the purposes for which signals intelligence in foreign intelligence operations can be conducted, it is however very difficult to see that these have been the subject of any secret surveillance measure by the National Defence Radio Establishment.

34. As stated in the Government's initial observations, collection from cables was not possible until after 1 December 2009, i.e. from the third period onwards, when the regulation concerning the obligation on the part of the cable owners to make traffic available entered into force.

35. The applicant firm has inquired with the National Defence Radio Establishment whether the cable owners nevertheless gave access to the traffic on a voluntary basis by at an earlier stage. The Government would like to inform the Court that on 26 September 2012 the National Defence Radio Establishment responded essentially as follows to the applicant firm. The obligation, under Chapter 6, Section 19a of the Electronic Communications Act, on operators who own cables to transmit signals to interaction points entered into force as described on 1 December 2009. In addition to this obligation, all operators who transmit signals via cables across Sweden's

borders are to provide to the National Defence Radio Establishment any information they possess that will make it easier to handle the signals. This requirement, which has applied since 1 January 2009, concerns the input values regarding, for example, the connections' naming, their architecture, bandwidth, direction, type of signalling and who is renting connections from the operator. The obligation only covers information in the operator's possession and does not involve any requirement to adapt it.

36. The applicant firm has made a number of assertions regarding the conditions for and application of signals intelligence. The Government would like to reply to some of these assertions. Firstly, the Government disputes the assertion that the sheer number of mobile telephony and broadband users in Sweden would mean that the state has access to the information transmitted between these users. This assertion cannot be considered to be relevant.

37. The applicant firm has furthermore alleged that one signal carrier covers at least 1 million households using broadband internet connections. This figure is a theoretical estimate based on possible transmission capacity. A signal carrier could theoretically contain zero (0) home broadband traffic.

38. Also, the assertion that chance determines the route taken by signal traffic is of little relevance in this context, as the legislation from 1 January 2009 is technology-neutral and covers both over-the-air and cable traffic. This is one of several reasons behind the new regulations surrounding signals intelligence operations. As from the second period, the signals intelligence process was governed by the tasking directives determined by those commissioning the intelligence, on the basis of their precise intelligence needs, permits from the Signals Intelligence Board (as from the third period the Foreign Intelligence Court), collection plans for various types of signals, the exact formulation and use of selectors, etc.

39. Moreover, the applicant firm has alleged that communications that have no relevance for foreign intelligence can be collected and stored by the National Defence Radio Establishment. In relation to this, the Government would like to clarify that it is difficult to separate out Swedish-Swedish traffic, but not impossible. The applicant firm's comments are obtained from two reports which reflect the purely technical position of the National Defence Radio Establishment at that time with regard to collection in cables. Since then, the methods have been refined and the National Defence Radio Establishment works continuously to sift out such signals. Swedish-Swedish traffic is dealt with in Section 2a of the Signals Intelligence Act and

accordingly does not fall outside the scope of the legislation. According to the provisions, if such signals cannot be separated on collection, recordings or notes are to be destroyed as soon as it becomes clear that such signals have been picked up. The National Defence Radio Establishment complies with the legislation.

40. Furthermore, the applicant firm has asserted that the National Defence Radio Establishment picks up traffic that is prohibited to collect because the selectors for the traffic data are unspecific. This assertion is incorrect. In this context, the Government would like to reiterate the crucial role of the Foreign Intelligence Court in limiting interferences in personal privacy when, for example, permitting the selectors to be used in a specific collection assignment (cf. paras. 80–82 of the Government's initial observations). The applicant firm has also stressed that the storage of only traffic data might be an equally severe interference since it can be used to map out a person's social network and position. In relation to this, the Government would like to clarify that traffic data consists of information that describes how, when and between which telecommunications addresses communication takes place, without describing the content of the transmitted communication. This concerns, for example, IP addresses, email addresses and telephone numbers. Through the collection and processing of traffic data, it is possible for the National Defence Radio Establishment to rapidly gain an idea of the traffic between countries on a given signal, without needing to examine the content of the traffic or understand the language. Traffic data is also used to enable the National Defence Radio Establishment to create a picture of normal traffic patterns and thus locate anomalies. The collection and handling of traffic data is regulated in the Signals Intelligence Act and the Act on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment (2007:259). Since traffic data does not provide information about the content of messages, it may be said to be less of an intrusion of privacy than collection for the purpose of studying message content.

41. The applicant firm has maintained that the guarantees provided for in Section 3 of the Signals Intelligence Act, namely, that attributes pertaining to a particular individual may only be used as selectors if such usage is of crucial relevance, are not respected and/or are given too broad an interpretation. In this connection, the Government would like to reiterate that any selector must be approved by the Foreign Intelligence Court and a proportionality assessment is always conducted in which any possible intrusion of privacy is taken into account. IT-related threats against systems that are vital to the

functioning of society can be mentioned as an example of when it may be of great importance to conduct a search specific to a certain natural person. Selectors may then comprise, for example, IP or email addresses.

42. Moreover, the applicant firm has stated that the Government's assurance that data of a superfluous nature is deleted after a certain time is too imprecise to afford any guarantee against abuse in this respect. The applicant firm has also contended that it is not until the third stage of the signals intelligence process that the National Defence Radio Establishment has enough information about the communication to be able to determine whether the communication should be destroyed.

43. In this context, the Government would firstly like to clarify that traffic that does not reach what is described by the applicant as the 'third stage' is never collected since the selector does not result in a hit. Traffic in which selectors do not result in hits cannot be assessed since it is not retained. Traffic that has been collected and found not to be relevant is destroyed. In addition, traffic that has not been assessed at all is discarded. Deletion and destruction of data takes place in accordance with laws, ordinances and provisions. Furthermore, the Swedish Foreign Intelligence Inspectorate has instructions to review data destruction by the National Defence Radio Establishment.

44. The Government would like to once again fully describe the situations in which data destruction is to occur under the Signals Intelligence Act (see para. 65 of the Government's initial observations).

45. Recordings or notes of information picked up in accordance with the Act are to be destroyed immediately if their content concerns a specific natural person and is assessed to lack relevance for foreign intelligence operations or other permitted operations. This of course applies regardless of whether the data has been collected automatically or manually. One example of recordings or notes that typically lack relevance for operations are those concerning communications that fall entirely outside the framework of the purpose of operations, e.g. because they concern domestic circumstances. The requirement to destroy traffic also applies to recordings or notes that include information that is subject to the duty of confidentiality under Chapter 3, Article 3 of the Freedom of the Press Act or Chapter 2, Article 3 of the Fundamental Law on Freedom of Expression, or that is covered by the enquiry prohibition in Chapter 3, Article 4 of the Freedom of the Press Act or Chapter 2, Article 4 of the Fundamental Law on Freedom of Expression. Recordings of or notes on information in messages referred to in Chapter 27,

Section 22 of the Swedish Code of Judicial Procedure, i.e. between a suspect and his or her defence counsel, must be destroyed. The obligation to destroy recordings or notes applies to all copies of the recordings or notes in question.

46. In this context it is also relevant to inform the Court that the Swedish Foreign Intelligence Inspectorate has submitted an opinion to the National Defence Radio Establishment that a provision should be introduced into the National Defence Radio Establishment's internal policy document to the effect that nothing that has been destroyed may be regenerated. The National Defence Radio Establishment has introduced such a provision. The National Defence Radio Establishment has also developed technical mechanisms to prevent regeneration in the organisation and the National Defence Radio Establishment's director-general has taken a decision prohibiting regeneration where it would be possible.

47. In relation to enclosure 2 of the applicant firm's observations, the Government finds it pertinent to clarify that the National Defence Radio Establishment does not work on behalf of other countries or organisations. The National Defence Radio Establishment reports to Swedish principals and relevant government agencies in accordance with the legislation. International cooperation may be conducted in accordance with the Foreign Intelligence Act (2000:130) and Section 9 of the Signals Intelligence Act.

48. Moreover, the applicant firm has alleged that it appears from the yearly report of the Swedish Foreign Intelligence Inspectorate that reporting has been made unduly to the Swedish Security Service. The Government would like to clarify that the supervisory authority only maintains that on two occasions the National Defence Radio Establishment was unable to clearly explain how information was important to the purposes of foreign intelligence operations and that, on one of these occasions, the National Defence Radio Establishment was unable to clearly account for why a certain agency was involved. The National Defence Radio Establishment has followed up these supervision observations and tightened its routines.

49. The applicant firm has also pointed to the fact that the Swedish Security Service and the National Criminal Police are to be given the right to direct the signals intelligence operations of the National Defence Radio Establishment. The Government finds it pertinent to reiterate that the purposes of signals intelligence are not changed when other agencies are given the right to direct the signals intelligence operations of the National Defence Radio Establishment.

50. Turning to the recent case-law of the Court in this context, the Government has taken note of the Court's judgment in the case of *Hadzhiev v. Bulgaria* (cited above) and finds it relevant to make the following remarks.

51. In the *Hadzhiev* case the Court held that the applicant could claim to be a victim on account of the very existence of legislation permitting secret surveillance, although there was no evidence that the applicant in that case was a person who was of particular interest to the authorities. For its part, the Government contends that there must be some degree of risk that secret surveillance measures have been applied also in cases where the law is challenged *in abstracto,* even though it seems clear from the case-law that the applicant does not need to establish a reasonable likelihood that such measures have been applied. In *Kennedy v. the United Kingdom* (no. 26839/05, § 124, 18 May 2010), the Court, after having reiterated its previous case-law, for the first time in this context made a distinction between the remedies available at national level, on the one hand, and the risk of secret surveillance measures being applied to the applicant in question, on the other hand. In this connection the Court held that where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. The Court furthermore held that in such cases, even where the actual risk of secret surveillance is low, there is a greater need for scrutiny by the Court. In the Government's view, this distinction made by the Court aimed at further clarifying in which cases there was a need for the Court to depart from its general approach that individuals cannot challenge a law *in abstracto.* The Government holds that these statements by the Court support the Government's contention that even where the law is challenged *in abstracto*, there must be some degree of risk that secret surveillance measures have been applied to the applicant. In addition, if no degree of risk at all is required in this context, the Government cannot see the point of this distinction between remedies and risk made by the Court (see also the question put forward by the Court in the present case).

52. Moreover, in the Government's view, the Court's reasoning as regards the victim status of the applicant in *Hadzhiev v. Bulgaria* (cited above) and other recent judgments concerning Bulgaria (*Natsev v. Bulgaria*, no. 27079/04, 16 October 2012 and *Lenev v. Bulgaria*, no. 41452/07, 4 December 2012), do not seem to follow the Court's logic and reasoning in *Kennedy v. the United Kingdom* (cited above), which is reflected in the question put forward by the

Court in the present case. The Government would therefore find it desirable for the Court to take the opportunity to further clarify the assessment to be made when an individual claims to be victim of a violation as a result of the mere existence of legislation permitting secret surveillance measures. In particular, the Court is invited to elaborate on the remedies required and the degree of risk to be applied in relation to this.

53. In relation to this, the Government would furthermore like to draw the Court's attention to the fact that the Court has on several occasions examined the Bulgarian law on secret surveillance measures *in abstracto*. In 2007, the Court found in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (cited above) that the Bulgarian law did not provide sufficient guarantees against the risk of abuse of the system of secret surveillance, or effective remedies in that respect. Recently, the Court has come to the same conclusion in three further judgments concerning the same legislation (*Hadzhiev v. Bulgaria*, *Natsev v. Bulgaria* and *Lenev v. Bulgaria*, all cited above). As regards the issue of victim status, the Court has stated that the reason for its departure, in cases concerning secret measures, from its general approach that individuals cannot challenge a law *in abstracto* is to ensure that the secrecy of such measures does not result in them being effectively unchallengeable and outside the supervision of the national authorities and the Court. In the Government's view, once the legislation in question has been assessed by the Court, it is no longer 'outside the supervision of the national authorities and the Court' and consequently there should be no need for the Court to make yet another assessment of the law in question *in abstracto*. According to the Government, the Bulgarian judgments cited indicate the need for the Court to reconsider the basis for when a departure from its general approach that individuals cannot challenge a law *in abstracto* is called for, and hence when an applicant may claim to be a victim of a violation of the Convention in such cases.

54. To sum up, in view of what has been mentioned above concerning the legal framework surrounding signals intelligence in foreign intelligence operations, especially as regards the purposes for which signals intelligence in foreign intelligence operations can be conducted, and concerning the technical conditions for signals intelligence over the air and via cable, the Government maintains that the risk that a secret surveillance measure has been applied to the applicant firm during any of the time periods is virtually non-existent.

Conclusion

55. In conclusion, the Government wishes to emphasise that it fully maintains its position as outlined in its initial observations. A general reference is therefore made to what was stated there. Accordingly, the Government maintains that the applicant firm cannot claim to be a victim of a violation occasioned by the mere existence of Swedish state practice and legislation concerning secret surveillance measures within the meaning of Article 34 of the Convention.

56. However, since the Court's question at this stage of the proceedings only concerns the issue of victim status on the part of the applicant firm, the Government assumes that any decision taken by the Court at this stage will only concern the applicant firm's victim status and that it will be given the opportunity to submit observations regarding other aspects of the admissibility of the application introduced by the applicant firm.

57. Finally, for the sake of clarity, the Government maintains that it prefers to submit any further observations in writing and that the Government, consequently, does not find it necessary to hold an oral hearing at this stage of the proceedings.