CENTRUM FÖR RÄTTVISA

Stockholm on 31 August 2012

European Court of Human Rights
Fifth section
Council of Europe
67075 Strasbourg
France

Centrum för rättvisa v. Sweden, Application no. 35252/08

Written observations in reply to the government's observations on the admissibility of 27 April 2012

Initial remarks and disposition

1. In addition to its previous submissions to the Court, Centrum för rättvisa wishes to comment on the government's observations. In the following the applicant will focus on the arguments on the admissibility of the application and leave the arguments on the merits to a later stage of the proceedings.

2. At this initial stage of its observations, the applicant would like to comment on the government's contention that legal persons cannot have a private life within the meaning of Article 8 of the Convention (§ 121 of the government's observations).

3. In this context, the applicant would like to reiterate that the purpose of the respect for private life is to protect a right to personal development and the right to establish and develop relationships with other human beings and the outside world (*Gillberg v. Sweden* [GC], no. 41723/06, § 66, 3 April 2012). In light of the applicant's mandate, as formulated in Centrum för rättvisa's founding articles, the establishment and development of relationships with

Centrum för rättvisa
Skeppsbron 20
Box 2215
103 15 Stockholm
Tel. 08-693 03 80
Fax 08-693 03 89
info@centrumforrattvisa.se
www.centrumforrattvisa.se
Org.nr. 802412-1215
Bankgiro 900-1538
Plusgiro 90 01 53-8

other human beings such as scholars, law students, victims of human rights violations and the general public is a key element in the applicant's existence. The threat of being exposed to secret measures may considerably affect both the applicant and other physical or legal persons negatively from wanting to engage in any sort of relationship. The applicant thus sees a major interest in a modern democracy to entitle the applicant, as well as legal persons in general, to a "private life" within the meaning of Article 8 of the Convention.

4. Furthermore, 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 the Liberty case (*Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 56-57, 1 July 2008).

5. However, the government does not dispute that Article 8 is applicable regarding the applicant's right to protection of correspondence (§ 121 of the government's observations).

6. The Court's case-law in respect of secret surveillance measures in relation to Article 8 of the Convention could be summed up as a need for a potential victim status. Consequently, in the following the applicant will show why it cannot be excluded that signal surveillance has been applied on the applicant or that the applicant risks being subjected to such measures (cf. *Kennedy v. the United Kingdom*, no. 26839/05, § 128 *in fine*, 18 May 2010).

7. The following observations will be disposed in three parts. Firstly, the applicant will reiterate the scope of the present application and, since the government contends that the applicant has failed to exhaust domestic remedies in accordance with Article 35 of the Convention, the applicant will briefly comment why there are no effective domestic remedies available regarding the present complaint. Secondly, the applicant will comment the government's statements on the scope of the signal intelligence conducted by the Swedish National Defence Radio Establishment and the risk that the applicant has been, is or will be subjected to interception. Thirdly, the applicant will provide an analysis of the insufficient effectiveness, both in theory and in practice, of the remedies available on a national level. Finally, the applicant will conclude why, in the present case, there is a strong need for scrutiny by this Court. In these

aforementioned parts, where it is relevant, the applicant will make a separate assessment for each of the three relevant time periods.

The scope of the present application and the exhaustion of domestic remedies

8. In § 119 of the government's observations, the government states that there may be reason to question whether the applicant has exhausted all domestic remedies. In reply to these doubts put forward by the government, the applicant would reiterate that the applicant complains that Swedish legislation has and does enable signal intelligence in violation of Article 8 of the Convention. The question to be answered is not only whether there has been a risk that signal surveillance has been applied on the applicant in the past but also whether the applicant risks being subjected to such measures in the future (cf. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 59, 28 June 2007).

9. In other words, any remedy, in order to qualify as effective within the meaning of Article 35 of the Convention, would need to have the power to declare incompatible with the Convention, the Swedish Constitution or any other legislation the legal provisions in question with the result that the incompatible provision be upheld or annulled (see *Kennedy v. the United Kingdom, §§ 109-110*).

10. Sweden does not have a constitutional court or any other remedy that has the power to uphold or annul legislation. Consequently, none of the remedies enumerated by the government in its observations give evidence of a domestic remedy that with sufficient certainty would qualify as an effective remedy within the meaning of Article 35-1 of the Convention.

11. The present application should therefore not be declared inadmissible for non-exhaustion of domestic remedies.

The scope of signal intelligence and the risk of interception

12. In accordance with the Court's judgement in the Kennedy case, interference with someone's communication can either be based on establishment of reasonable likelihood of interception, or on the very existence of measures

permitting secret surveillance (*Kennedy v. the United Kingdom,* § 125). The applicant has not based its complaint on a reasonable likelihood of interception, but on the very existence of the measures permitting surveillance. Thus, a risk of surveillance has to be shown (*Kennedy v. the United Kingdom,* 128).

13. Whether a risk of surveillance exists, or has existed, is dependent of under which conditions the communication may be intercepted. This risk has to be assessed with regard to the applicable provisions of the relevant act in force at the time (cf. *Kennedy v. the United Kingdom,* § 128).

14. The government holds that the risk that secret surveillance measures have been applied to the applicant during any of the three periods is virtually non-existent (§ 155 of the government's observations).

15. The applicant wishes to emphasise that the interference with the applicant's right to respect for its private life and correspondence occurs on every stage of the signal surveillance, beginning at so called points of coordination (*samverkanspunkterna*) where the state obtains access to the information. The applicant can consequently not agree with the government's contention that a secret surveillance measure has been applied only when the information content is available to an employee at the Swedish National Defence Radio Establishment and subject to human scrutiny (§§ 37 and 154 of the government's observations).

First time period

16. During the first time period, there were no detailed provisions in Swedish law regarding when or how signal surveillance could be conducted. The government's view was based on the rather naive premise that "the airwaves are free" and that anyone, including the government, therefore were allowed to intercept and listen to radio messages using a suitable receiver (§ 45 of the government's observations).

17. The government has maintained that, during the first and second time period, the Swedish National Defence Radio Establishment intercepted signals intelligence targeting wireless traffic transmitted by terrestrial or satellite radio communications systems (see § 33 of the government's observation). The

government's observations conveys the impression that it would only involve for instance military radio traffic at certain frequency bands for satellite communications (cf. § 22 of the government's observation).

18. However, as is stated by the government, today's signal environment is characterised by a high pace of change with regard to new ways of exchanging information over long distances. Today's commercial mass market technologies – such as the Internet and mobile telephony – are also used by the kinds of actors that would traditionally have used specially built communication solutions. The fact is that commercial mass market technologies are currently used by all types of actors operating within the phenomena against which signals intelligence is targeted (see § 17 of the government's observation).

19. Thus, it is obvious that relevant information such as, for instance, military communication were transmitted through commercial networks such as mobile phone networks which operate through radio waves also before 1 January 2009. It can therefore be assumed that the Swedish National Defence Radio Establishment had a strong interest and the means, before 1 January 2009, to monitor not only satellite communications but also wireless transmissions in public communications networks such as mobile phone networks.

20. In this context it should be noted that on 30 June 2008, there were 10.5 million mobile phone subscriptions and active pre-paid cards in use in Sweden (PTS – Svensk telemarknad första halvåret 2008, page 25). At the end of 2008, there were 877.000 mobile broadband subscriptions in Sweden, a number that rose to 1,3 million at the end of 2009 (PTS – Svensk telemarknad 2009, page15). Consequently, there was a vast amount of communication available for the Swedish National Defence Radio Establishment to intercept, including military traffic at certain satellite frequencies as well as commercial communication (Internet and mobile phone) sent through publicly available networks.

21. With regard to the abovementioned, the applicant's status as an independent non-profit organisation whose mission consists of guarding individuals' human rights and freedoms through *inter alia* litigation against the state, and given that the applicant during this time period used mobile telephony as well as mobile broadband, it must be deemed that a risk existed that these communications

were intercepted. It should also be considered, that there is no technical possibility to distinguish radio signals other than by frequency bands. Since the applicant used such means of communication that utilized frequencies that were of interest to the government (cf. § 17 of the government's observation), it cannot in any way be ruled out that the applicant's communication was not intercepted.

22. The risk assessment shall be made with regard to the provisions of the applicable act, which in principle were non-existent in terms of practical limits on for what reasons mobile and mobile broadband traffic could be monitored. A risk therefore existed that the applicant's communication through mobile phones and mobile broadband were in fact monitored during this time period.

Second time period

23. During the second time period, the Signals Intelligence Act had entered into force. However, not until 1 December 2009 did the obligation for the cable owners to make traffic available arise. The applicant has inquired with the Swedish National Defence Radio Establishment whether access to the traffic nevertheless was given on a voluntary basis by the cable owners but has currently not received any reply.

24. Even if monitoring occurred only of wireless communication, the state obviously had access to a very large volume of information, as previously illustrated (see § 20 above).

25. The applicant was therefore at least as likely to be subjected to surveillance during this time period, as during the first time period. The entry into force of the Signals Intelligence Act did not reduce this risk. Furthermore, the scope of the act was too broad, as illustrated in the application §§ 33 and 60, to provide any practical limitations. Signals intelligence was carried out for the identification of "external threats" against Sweden, a term not sufficiently defined and precise in order to rule out that the applicant was not exposed to a risk of being monitored.

26. The applicant also wishes to clarify a few technical aspects of signal intelligence with relevance to, in particular, the monitoring that was conducted by the government during the first and second time periods.

27. It is up to the network service provider (Internet or mobile phone) to decide how a signal shall be transmitted. The choice of communication, whether it is e.g. via the Internet (wired or mobile), land telephone lines, mobile telephone or fax, mean that the signal sent can pass both via radio waves and/or cables. It is moreover impossible for a user of any of the aforementioned communication services to foresee whether the signal will pass a Swedish border or not or exactly which cable the signal will pass through (SOU 2011:13 Uppföljning av signalspaningslagen betänkande av Signalspaningskommittén, Stockholm 2011, available on the Internet, henceforth the Signal Intelligence Committee report, page 32).

28. It is thus not satisfactory to compare radio communication to a postcard since it is not a conscious choice of the sender whether the sent signal will pass through radio waves or cable (cf. § 25 of the government's observations). It is therefore, as previously stated by the applicant, a matter of chance as seen from the user's point of view, whether the signal traffic will travel through cable or wireless (cf. § 20 of the government's observation). It is to be noted that, at the end of 2009 there were 4 596 000 Internet subscriptions in Sweden. The number had increased with 13 percent since 2008 (PTS – Svensk telemarknad 2009, page 16).

Third time period

29. During the third time period, the Signals Intelligence Act had been amended and *inter alia* provided eight purposes for which signals intelligence could be conducted. However, as it is not possible due to technical reasons to separate traffic until after it has been intercepted, access to all the information in the relevant signal carrier (a fiber optics cable) must be obtained. To be noted is that one signal carrier covers at least 1 million household using broadband internet connections (Enclosure 1 – Vi blev lurade, article in Aftonbladet published on 3 February 2009).

30. Since all traffic in a signal carrier must be intercepted, there is no practical difference from how signal intelligence was gathered prior to the amended Signal Intelligence Act. An infringement occurs when the state acquires the communication. Which communication may be intercepted can only be determined after the interference has taken place, the eight purposes for which

signals intelligence may be conducted have thus no practical significance. Regardless of this, the applicant will below illustrate why there is a significant risk of an interference with applicant's right to correspondence at the later stages of the interception as well.

31. The applicant suggests that the interception be divided into four different stages in accordance with the report by the Signal Intelligence Committee (the Signal Intelligence Committee report, pages 73-75).

32. The first stage of interference only concerns signals in cable and occurs when the owners of the cables transmit traffic to the so called points of coordination (*samverkanspunkterna*). At this stage the Swedish Foreign Intelligence Inspectorate has the right of disposition (*rådighet*) of the signals. This part of the interference concerns everybody whose communication passes Swedish borders, thus an enormous amount of communication is concerned. However, the signals that are not transmitted to the Swedish National Defence Radio Establishment in the second stage disappear immediately. Nevertheless, it is important to note that it is an interference in itself as soon as the communication is made available to the State (cf. the submission by the Council on Legislation (*Lagrådet*) prop 2006/07:63, enclosure 11).

33. The second stage is the collection by the Swedish National Defence Radio Establishment of the signal i.e. the communication. The collection is automatic with the support of selectors referring to mainly traffic data (*tratikdata*) i.e. technical information about the signal but not of its content. For the purpose of the developing operation (*utvecklingsverksamheten*) a large number of frequencies are used but for a short period of time. Whereas, for the purpose of the secret intelligence operation (*underättelseverksamheten*) the number of frequencies is lower but covers a longer period of time (the Signal Intelligence Committee report, page 50).

34. Generally speaking, the selectors for traffic data are less specific than selectors for the content of communications. For technical reasons, it also is difficult to separate communication where both the sender and the receiver is within Swedish territory. Consequently, the Swedish National Defence Radio Establishment can and has, particularly when intercepting signals from cables, collected and stored also these communications even though they fall outside

the Swedish National Defence Radio Establishment legal mandate (see Section 2a of the Signal Intelligence Act, the Signal Intelligence Committee report, page 16 and Datainspektionens redovisning av regeringsuppdraget Fö 2009/355/SUND, 6 December 20120, available on the Internet, henceforth the Swedish Data Inspection Board report, page 4).

35. Consequently, in the second stage, communications that have no relevance for defence intelligence can be collected and stored by the Swedish National Defence Radio Establishment. In fact, there is a relatively high likelihood that the Swedish National Defence Radio Establishment is collecting and storing communications from persons that communicate in a signal carrier from which the Swedish National Defence Radio Establishment is collecting signals (the Swedish Data Inspection Board report, page 4).

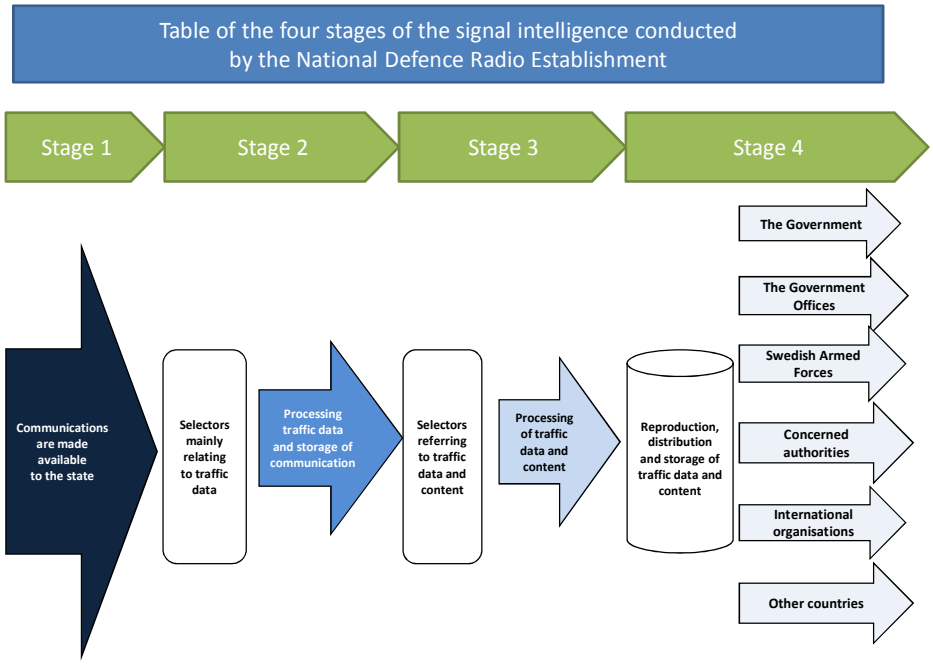
36. In this context, the applicant finds it important to stress that the storage of only traffic data might be an equally severe interference with the right to private life and correspondence since it can be used to map out a person's social network and position. Traffic data is also considerably easier to process with automatic devices.

37. The third stage is the processing and analysis of the signals with the use of various selectors. The number of selectors used is very vast (the Signal Intelligence Committee report, page 52). The interference consists in the processing and storing of both traffic data and the actual content of the communication. To be noted is that this concerns both surveillance within development operations and secret intelligence operation (the Signal Intelligence Committee report, page 64).

38. With respect to the second and third stages, the applicant would like to draw the Court's attention to the fact that Section 3 of the Signal Intelligence Act provides that attributes pertaining to a particular individual may only be used as selectors if such usage is of crucial relevance (*synnerlig vikt*) to the operations. The wording gives an impression that the use of such selectors is exceptional. However, it appears from the reports of the Signal Intelligence Committee and the Swedish Data Inspection Board that selectors as a rule refer to particular persons (the Signal Intelligence Committee report, page 17 and the Swedish Data Inspection Board report, page 5). The applicant thus maintains that the

guarantees provided for are not respected and/or are given a too broad interpretation.

39. The fourth and last stage is the reporting of the communication. The interference consists in the reproduction and distribution of all data relating to the communication. In this respect the applicant notes that the Swedish National Defence Radio Establishment not only reports back to agencies requesting the surveillance i.e. the Government, the Government Offices (*Regeringskansliet*) and Swedish Armed Forces (*Försvarsmakten*) but, according to Section 9 of the Secret Surveillance Act, also to other countries and international organisations (Enclosure 2 – Sverige samarbetar med diktaturer, article in Dagens Nyheter, published on 14 September 2008) and, according to Section 8 of the Secret Surveillance Act, furthermore to "concerned authorities" (*berörda myndigheter*). The law does not specify which authorities qualify as concerned. However, it appears from the yearly report of the Swedish Foreign Intelligence Inspectorate that reporting has been made unduly to the Swedish Security Service (*Säpo*) (Enclosure 3 – SIUN Inspektionsprotokoll, 19 May 2011, Enclosure 4 – Inspektionsprotokoll, 14 December 2011 and Enclosure 5 – FRA brister i integritetsskyddet, article in Ny teknik, published on 20 January 2012).



40. The applicant does not question that the amount of data is being filtered and reduced at every stage of the surveillance. However, the applicant maintains that the interference occurs at every stage of the interception and begins with the obtaining of information from the so called points of coordination. The exact extent of signal intelligence is impossible to establish since this information is being classified both as regard the number of permits given by the Foreign Intelligence Court, the selectors used or the number of signals or communications being intercepted (Enclosure 6 - Protocol of 8 December 2010 of the Signal Intelligence Court and Enclosure 7 – Government decision of 20 January 2011).

41. However, the fact that signal intelligence concerns a large amount of communications is confirmed by both the Swedish Data Inspection Board and the Signal Intelligence Committee. It is clear that already the signal surveillance in radio signals is very vast. It is also clear that, due to the methods used when intercepting signals from cables, the extension of signal intelligence to cover cables is considerably vaster (according to the Swedish National Defence Radio Establishment 95 % of international traffic passes through cable, the Signal Intelligence Committee report, page 41, the Swedish Data Inspection Board report, pages 3, 12 and 22 and §§ 37 and 75 of the government's observations). Thus, there is no doubt that Swedish National Defence Radio Establishment is intercepting a very large amount of communications and that, due to the technical methods used, unwanted signals are intercepted.

42. The applicant would furthermore like to draw the Court's attention to the fact that the scope of the signal intelligence is likely to increase in the future. For example the governments' ambition is that, both the Secret Police (*Säpo*) and the National Criminal Police (*Rikskrimialpolisen*) should, as of 1 January 2013, have the authority to request signal intelligence measures from the Swedish National Defence Radio Establishment. The new legislation might enter into force despite criticism by the Council on Legislation, the Swedish Data Inspection Board and the Bar Association (Enclosure 8, 9 and 10).

43. Furthermore, the following should also be noted. The government's assurance that data of superfluous nature is deleted after a certain time is too imprecise to

afford any guarantee against abuse in this respect (cf. §§ 92 and 151 *in fine* of the government's observations).

44. The existing rules on destruction of data regard three main categories of data; signals where both the sender and the receiver are within Swedish territory, communications that are covered by certain types of secrecy and data concerning a physical person (Sections 2a and 7 of the Signal Intelligence Act).

45. Generally speaking it is not only until the third stage, when the actual content of the communication is being intercepted, that the Swedish National Defence Radio Establishment has enough information about the communication to be able to determine if the communication should be destroyed. Thus, there is potentially a very large amount of data that is neither passed on to the third stage nor destroyed (see the Signal Intelligence Committee report, pages 51 and 54 and the Swedish Data Inspection Board report, pages 5 and 17).

46. Another weakness concerning the guarantees that unduly collected data is destroyed regards the possibility to reconstruct destroyed data (the Swedish Data Inspection Board report, page 5).

47. Consequently, with regard to the above and in the light of the applicant's activities as a non-governmental organisation scrutinising the activities of state actors, the applicant maintains that it cannot be excluded that secret surveillance has been applied on the applicant and that there is a substantial risk that its communications has been or will be subjected to measures of secret surveillance.

The insufficient effectiveness of national remedies

48. Having established above that the secret surveillance regime during all three time periods entailed a substantial risk that the applicant has been, is or will be subjected to interception, the applicant would like to elaborate on the insufficient effectiveness of national remedies. The weaker the national control mechanisms are, the lower the risk of secret surveillance must be before there is a need for the Court's scrutiny (*Kennedy v. the United Kingdom*, § 124 *in fine*).

49. The applicant has chosen to divide the control mechanisms into two categories, remedies for individuals to lodge complaints that they have been exposed to unlawful surveillance and general control mechanisms supervising the work of the Swedish National Defence Radio Establishment.

50. As an overall remark, the applicant accepts that the possibilities for the public or an individual person to gain insight in any secret surveillance regime are for natural reasons extremely restricted. As a consequence, remedies available to persons who wish to ascertain that they have not been subjected to unlawful surveillance are overall of a lower practical importance. However, the lack of transparency must be counterbalanced by other safeguards such as clear and foreseeable legislation and effective control organs that can guarantee the respect of the prevailing legislation.

Remedies for individuals

51. A natural or legal person will normally not be informed of the fact that he, she or it has been subjected to surveillance by the Swedish National Defence Radio Establishment. The obligation under Section 11a of the Signal Intelligence Act, which was introduced for the third period, to inform individuals if selectors attributable to their person have been used has, due to secrecy, to today's date never been used. Both the Signal Intelligence Committee and the Data Inspection considers this safeguard to be without practical significance (the Signal Intelligence Committee report, page 14 and the Swedish Data Inspection Board report, page 6). This remedy must therefore be considered to be theoretical and illusory and not practical and effective.

52. The secret surveillance regime in question is thus different from the one under scrutiny in the case of Julien Mersch v. Luxembourg. It is also different from the situation where secret measures are being applied to a person during a Swedish criminal investigation. In both the Mersch case and during a Swedish criminal investigation the person in question is informed *post facto* of the fact the he or she has been subjected to interception (cf. *Julien Mersch and others v.* Luxembourg, nos. 10439/83, 10440/83, 10452/83, 10512/83 and 10513/83, 10 May 1985 and Chapter 27 of the Swedish Code of Judicial Procedure).

53. There are indeed possibilities for physical persons to request a control if he or she has been subjected to interception unlawfully or if personal information

(*personuppgifter*) i.e. any information that can directly or indirectly be attributed to a physical person about him or her has been processed by the Swedish National Defence Radio Establishment (Section 10a of the Signal Intelligence Act and Chapter 2 Section 1 of the Act (2007:259) on Processing of Personal Data in the Foreign Intelligence and Development Operations of the Swedish National Defence Radio Establishment). The competent authorities are the Swedish Signal Intelligence Inspectorate and the Swedish Data Inspection Board. However, to the applicant's knowledge these remedies are not available to legal persons such as the applicant. The applicant would invite the government to substantiate its contentions in this respect (cf. § 103 of the government's observations).

54. Furthermore, few natural persons have availed themselves of the remedies to request a control of abuse and those who have done so, have received a standardised reply that no unlawful surveillance has taken place (Annual reports of the Swedish Signal Intelligence Inspectorate for 2009 to 2011 and Enclosure 11 – example of decision by the Swedish Signal Intelligence Inspectorate. Between 2009 and July 2012, the Swedish Data Inspection Board has not received any complaints regarding Signal Intelligence conducted by the Swedish National Defence Radio Establishment. The Board received five complaints before the Signal Intelligence Act entered into force in 2008). It is thus not possible to know from the information given if the person in question has been subjected to surveillance or not and if information to that end has been classified.

55. The applicant also questions 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. Unless a signal was intercepted and transmitted to the Swedish National Defence Radio Establishment at the first stage of the surveillance, there will be no trace of the interference. If the information in a signal has been stored at the second stage of the surveillance but not selected for further processing and analysis, the information can in theory still be stored at the Swedish National Defence Radio Establishment (see §§ 33-35 above). It is the applicant's understanding that any scrutiny *post facto* does not go through all communications stored with the Swedish National Defence Radio Establishment but limits itself to scrutinising the last and fourth stage of surveillance. It is also to be noted that an individual who has been subjected to

surveillance but who lodges a complaint after the data has been destroyed will, from what the applicant can understand, not be informed of the fact that he has been exposed to surveillance, illegal or not.

56. Regarding the remaining remedies mentioned by the government, the applicant sees not prospects of success unless there is evidence to establish that a natural or legal person has been subjected to unlawful interception.

57. There is no precedent regarding the possibility to obtain compensation and attempts before domestic courts to this end have so far been dismissed (Enclosure 12 – decision by the District Court of Stockholm of 24 February 2012 and Enclosure 13 – decision by the Swedish Supreme Court of 27 August 2012).

General control mechanisms

58. The government has also enumerated a number of general control mechanisms that the applicant will comment upon in the following.

59. As an overall remark, the general control mechanisms afforded at a national level reveal a certain immaturity and much of the efforts have so far focused on capacity building such as training in signal intelligence and recruitment of staff. Thus, the Signal Intelligence Court and the Swedish Foreign Intelligence Inspectorate have laid a large part of their efforts on recruitment and training (Annual report of the Signal Intelligence Court for 2011 and annual reports of the Swedish Foreign Intelligence Inspectorate for 2009 to 2011. Also cf. the Swedish Data Inspection Board report, pages 7-8 and the Signal Intelligence Committee report. Pages 26-27).

60. The immaturity of the system is remarkable in light that the Swedish National Defence Radio Establishment has conducted signal intelligence for several decades. It is further remarkable that it was not until second and third period that there were any legislative attempts to provide any adequate safeguards against abuse.

Permanent control mechanisms

The Signal Intelligence Court / the Signal Intelligence Board

61. During the first period, there was no organ giving authorisations to conduct signal intelligence. During the second period, authorisations were given by the Signal Intelligence Board and during the third period they were given by the Signal Intelligence Court.

62. The applicant firstly wishes to comment on the choice of terminology since, in its view, the Signal Intelligence Court lacks many of the main criteria that constitute a court within the meaning of Article 6 of the Convention. For example, the members of the Signal Intelligence Court are appointed by the government for four years. There impartiality and independence from the government which is one of the three organs that can request permits is therefore questionable (cf. Section 2 of the Signal Intelligence Court Act). Moreover, it follows from Section 13 of the Signal Intelligence Act that no appeal lies against a permit to conduct surveillance given by the Signal Intelligence Court.

63. Furthermore, Section 14 of the Signal Intelligence Court Act states that the President of the court may order that a hearing be held behind closed doors if it is clear that information that is covered by secrecy will be revealed during the hearing. The wording of the Signal Intelligence Court Act gives a *prima facie* impression that the Signal Intelligence Court's work is transparent and open to the public. However, from the inception of the Court to today's date not a single hearing has been open to the public. In fact, not even information such as the number of hearing or the number of permits given by the Signal Intelligence Court is available to the public (Enclosure 6 and the Annual Report of the Signal Intelligence Court 2011). The same goes for any indication as to the type or number of selectors allowed or number of signal carriers (*signalbärare*) i.e. cables included in the permit. Based on this complete secrecy surrounding the Signal Intelligence Court work, the applicants position is that it is not possible to assess the effectiveness of the Signal Intelligence Court (cf. §§ 86-87 of the Government's observations).

The Swedish Foreign Intelligence Inspectorate/ the Swedish Intelligence Commission

64. It appears from the Swedish Foreign Intelligence Inspectorate (before 1 January 2009 the Swedish Intelligence Commission) last three annual reports (2009, 2010 and 2011) that the Inspectorate is in a capacity building phase and lacks resources to provide an adequate scrutiny of the Swedish National Defence Radio Establishment's work.

65. The importance of giving Swedish Foreign Intelligence Inspectorate sufficient means to fulfil its mission was also stressed by the Signal Intelligence Committee (the Signal Intelligence Committee report, page 78).

66. Although some of the members of the Swedish Foreign Intelligence Inspectorate have been suggested by the opposition in parliament, only the members from the Social Democratic Party have members represented whereas the other parties in opposition are not represented.

67. The applicant reiterates that the Court stressed in the Klass v. Germany judgment (*Klass v. Germany*, no. 5029/71, §56, 6 September 1978) that the composition of the control mechanisms have an important function in providing an adequate safeguard against abuse. A first step towards an undemocratic regime is likely to invade on the political opposition's fundamental rights and freedoms. To include members of the political opposition in the control mechanisms to secret surveillance is therefore an important factor when assessing the efficiency of the mechanisms.

68. To sum up, the Swedish Foreign Intelligence Inspectorate has an important role to play as a safeguard against abuse of the signal intelligence regime in question. The applicant will not speculate on when the Swedish Foreign Intelligence Inspectorate will be apt to effectively exercise that role but will limit itself to establishing that it has, regrettably, not done so yet.

The Privacy Protection Council

69. The Privacy Protection Council is an organ within the Swedish National Defence Radio Establishment. It claims to have contributed to reforms within the Swedish National Defence Radio Establishment strengthening the

protection of the integrity aspects. (Signal Intelligence Committee report, page 39). However, due to the secrecy surrounding its work, it is impossible to assess its relevance as a control mechanism.

Temporary general control mechanisms

The Signal Intelligence Committee and the Swedish Data Inspection Board

70. As a part of the political agreement that followed the stormy debates in the summer of 2008, the government put in place two temporary general control mechanisms which have served well in elucidating the secret surveillance regime.

71. The mandate of Signal Intelligence Committee spanned from 12 February 2009 to 7 February 2011. The Committee published its report on 8 February 2010. The government further gave the Swedish Data Inspection Board a special mission to scrutinise the Swedish National Defence Radio Establishment during the period 12 December 2009 to 6 December 2010 which resulted in a report published on 6 December 2010.

72. The applicant finds the report of the Signal Intelligence Committee and the Swedish Data Inspection Board to be, in practice, the only documents that shred any light on the otherwise concealed operations of the Swedish National Defence Radio Establishment.

73. Unfortunately there are no known intentions of repeating this exercise.

74. Due to various circumstances, neither the Swedish Data Inspection Board nor the Signal Intelligence Committee was able to scrutinise the signal intelligence conducted in cables.

75. The composition of the Signal Intelligence Committee was preceded by a large controversy and in the end only members from the Social Democratic Party were represented from the opposition. It is further of great concern that the Committees report is undermined by the fact that three out of eight members of the Committee finds that the work of the Committee was not conducted in a manner as to enable serious scrutiny (Signal Intelligence Committee report, pages 83-84).

76. The applicant also maintains that temporary committees cannot alone serve as a sufficient remedy and do not remedy the deficiencies put forward regarding the Signal Intelligence Court and the Swedish Foreign Intelligence Inspectorate.

Summary and conclusion

77. Secret surveillance and signal intelligence is by its nature surrounded by a high degree of secrecy and confidentiality. The applicant accepts that it lies in the nature of the signal intelligence regime that individual measures by the Swedish National Defence Radio Establishment cannot not be scrutinised to the same extent as measures taken by state actors in other fields.

78. The present application is not based on the contention that the applicant has actually been subjected to interception but to the fact that there is a risk that the applicant has been, is or will be subjected to interception contrary to Article 8 of the Convention.

79. The interference in the applicant's right to private life and correspondence under Article 8 of the Convention occurs at every stage of interception of communications, *i.e.* when communications are made available to the state, when communications are being stored, filtered, processed, analysed or distributed.

80. Even if the exact number of intercepted communications is not known to the public, it can be deducted from the information revealed to the public that a very large amount of communications has been intercepted by the Swedish National Defence Radio Establishment. The amount of communications intercepted is furthermore likely to grow in the future. Due to the technical methods used for signal intelligence, communications that fall outside the scope of the legislation are also being intercepted. Moreover, the safeguards regarding the destruction of stored communications are too imprecise to provide adequate protection against abuse.

81. Thus, the applicant maintains that it cannot be excluded that secret surveillance has been applied on the applicant and that there is a substantial risk that its communications has been or will be subjected to measures of secret surveillance.

82. Remedies available to individuals have, due to secrecy, little effect in practice. Legal persons, such as the applicant, furthermore virtually lack individual remedies. Moreover, the general control mechanisms reveal a certain immaturity and are inadequate in relation to the scope of signal intelligence being conducted by the Swedish National Defence Radio Establishment. The reports by the Signal Intelligence Committee and the Swedish Data Inspection Board are laudable efforts in providing the general public with more insight and understanding to signal intelligence regime. However, these reports were a result of temporary missions and can therefore not remedy the insufficiency of the permanent control mechanisms.

83. The secrecy surrounding the signal intelligence regime gives the applicant and the general public a justified suspicion and concern that the regime is or can be abused. Moreover, the lack of effective remedies, the insufficiency of the domestic control mechanisms and the vast scope of communications intercepted by the Swedish National Defence Radio Establishment, call for a greater scrutiny by this Court (*Kennedy v. the United Kingdom*, § 124). A lesser scrutiny by this Court would risk to materially weaken the Convention (*Klass v. Germany*, § 34).

84. The applicant therefore considers it to be of crucial importance to the effectiveness of the Convention system and the protection of the rights of the individual that the Court declares the present application admissible.

Clarence Crafoord Anna Rogalska Hedlund