CENTRUM FÖR RÄTTVISA

Stockholm on 31 August 2015

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 and merits of 8 May 2015

Invited by the President of the Fifth Section to submit written observations on the case together with any claims for just satisfaction, the applicant would like to make the following submissions.

The applicant has in previous submissions developed its view on both the admissibility and on the merits of this case. The following observations will therefore focus on the most pertinent arguments adduced by the applicant and provide an update with the latest relevant developments.

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

Disposition of the observations

A. The case in a larger context

1. The last year's developments of the signal intelligence regime is not an isolated trend but is, on the contrary, the result of a much larger change in society.

2. Technology has evolved in a rapid pace and changed people's patterns of behaviour. We now live in a digital age where almost all our doings and whereabouts leave digital footprints in some way or another. To mention a few examples, we communicate, do our shopping, buy travels and search for information over the Internet, pay our purchases by using credit cards, use Internet banking, access our medical records over the Internet, use applications on smartphones that disclose our position, and we are being intercepted and recorded by both stationary and mobile cameras.

3. It is precisely these digital footprints combined with new technologies able to compile, analyse and store these large amounts of data that has dramatically changed the potential of mass surveillance abuses. In fact, the processing of our digital footprints can give a very detailed understanding of our lives and past in a way that intelligence services historically could not, even in their wildest dreams, have imagined.

4. This potential bulk collection of data with the risk not only of abuse but also of self-censorship caused by the mere fear of abuses, challenges the protection of the right to private life (*cf. The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA*, Elisabet Fura and Mark Klamberg, p. 1). These are challenges that our democracies need to handle.

5. Important steps to this end have recently been taken by the Court of Justice of the European Union (CJEU) in its judgment *Digital Rights v. Ireland* where the Data Retention Directive was declared invalid for failing to pair a far reaching intrusion into the right to private life with adequate safeguards (also *cf*. the CJEU case *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, 2014).

6. Moreover, the United States Court of Appeals (Second Circuit judgment of 7 May 2015) in its judgement *ACLU v. Clapper* criticised the bulk collection program created by the American National Security Agency, the NSA.

7. The present application which concerns the signal intelligence regime conducted by the National Defence Radio Establishment (further on referred to as FRA according to the Swedish abbreviation for Försvarets radioanstalt), together with other similar cases pending (*Big Brother Watch and others v. United Kingdom*, Application No. 58170/13 and *10 Human Rights Organisations v. United Kingdom*, recently submitted case) leaves to this Court to set the standard for states' signal intelligence regimes. A standard that must provide adequate protection against abuses of the right to private life regardless of the ideology of the government in power.

B. Initial remarks

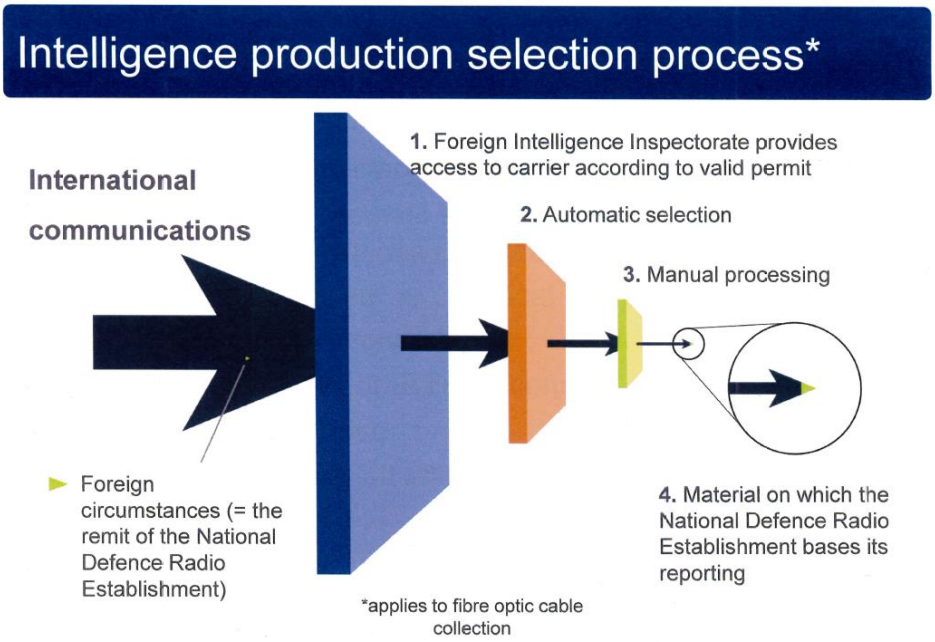
I. Three different time periods at stake in the present application

8. The present application was lodged on 14 July 2008 following the passing of a new Signal Intelligence Act (2008:717) in the Swedish Parliament on 18 June 2008. The Act triggered a major debate and caused great concern among the public that a mass surveillance regime was put in place that would intrude on people's right to private life. While pending before the Court and partly as a result of this pending application, the Signal Intelligence Act was partly amended.

9. As a result, which also follows from the Court's questions to the government, the current application covers three time periods; the first time period when signal intelligence was virtually unregulated, the second time period when the Signal Intelligence Act was in force and the third time period when the amended Signal Intelligence Act entered into force.

10. The applicant will refer to the signal intelligence regime in general and where necessary specify the particularities of each time period.

II. The structure of the signal intelligence regime



The FRA's description of the signal intelligence regime (also referred to by the government as appendix 3 to its observations of 8 May 2015)

11. As appears from the above picture, the signal intelligence regime can be divided into four stages; the interception (1), the automatic selection (2), the manual processing (3) and the reporting (4). To be noted, is that a number of authorities are given direct access to the various data collections at the FRA (see below §§ 56 and 61-64). Moreover, signal intelligence is not only conducted to report information to the government and other authorities, nations and international organisations but is also conducted for internal development of search techniques and similar (see below §§ 40-43).

III. The level of intrusion in the right to private life at the various stages of the signal intelligence regime

12. The interference with the right to private life begins as soon as any state authority is given access to the communication – *i.e.* as of stage one in the description above. The government has argued that the level of intrusion is

lower at the initial stages of surveillance (see the government's observations of 27 April 2012, §§ 37 and 154).

13. The applicant is not convinced by this. It is the applicant's position that the contrary would give a more accurate picture of how the level of intrusion should be perceived. As held by the CJEU and the US Court of Appeals – the automatic collection of metadata without examining the content of a communication can reveal very sensitive information about a person; such as civil, political or religious affiliations. They can also reveal social status, habits of everyday life, one's daily movements, social relationships and environments as well as involvement of intimate relationships (*ACLU v. Clapper, p. 9* and *Digital Rights v. Ireland*, § 27).

14. The fact that metadata is protected by Article 8 of the Convention has also been established by the Court a long time ago (see *e.g. Malone v. United Kingdom*, Application no. 8691/79, judgment of 26 April 1985, § 84).

15. With the technology and capacities to store data constantly developing, it can be argued that the largest risk of abuses of the right to private life, does in fact lie with the bulk collection of metadata.

IV. Attempt to assess the scope of today's signal intelligence regime

16. In the US, two official reports have followed the revelations made by Edward Snowden, the *Privacy and Civil Liberties Oversight Board report on the Telephone Records Program under Section 215 of the US Patriot Act and on the Operations on the Foreign Intelligence Surveillance Court* (the PCLOB Report) and *Liberty and Security in a Changing World – Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (the White House Report). These reports have at least to a certain extent, explained the scope of the signal intelligence surveillance conducted by the NSA to the public. These reports made it clear that enormous amounts of data was being intercepted and stored (the PCLOB report pp. 8-10, the White House Report pp. 94-97).

17. In Germany, newspapers maintain that surveillance of metadata amounts to 220 million "telephone data" a day (http://www.zeit.de/digital/datenschutz/2015-02/bnd-nsa-mass-surveillance). However, the special investigative committee

instructed by the German Bundestag to look into the veracity of revelations made by Edward Snowden has not yet produced any official report (http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf and https://www.washingtonpost.com/world/germany-opens-hearings-on-us-spying/2014/04/03/cf58f2d0-b42b-4e59-a403-75f968d6edb0_story.html).

18. However, the extent to which the Swedish signal surveillance is conducted in practice is still basically unknown.

19. The tasking directives made by the government that set the frame for the initiation of signal surveillance are covered by complete secrecy (Enclosure 1 – Decision by the government on 6 August 2015, registration no. Fö2015/01013/RS). The government has furthermore established that the activities of the Foreign Intelligence Court are covered by complete secrecy, *i.e.* no information about the number of hearings, the number of permits being granted or rejected or any reasoning in its decisions, the amount or type of selectors being used can be imparted on the public (*cf*. Enclosure 6 to the applicant's observations of 31 August 2012).

20. Regardless of this, it has been established that the current signal intelligence regime is unprecedented, that the FRA is processing very large amounts of data (*cf*. §§ 41 and 45 of the applicant's observations of 31 August 2012). Consequently, the system as such opens up for bulk collection of data

C. The admissibility of the application

21. In their observations of 8 May 2015, the Government maintains its position regarding the admissibility of the case and does not raise any new arguments.

22. The applicant will therefore not elaborate on the arguments regarding the admissibility but is satisfied to refer to its previous submissions regarding the admissibility.

23. The applicant thus maintains that Article 8 of the Convention is applicable not only in respect of its "correspondence" but also in respect of its "private life". This is even more important since the applicant is an organisation active in the field of human rights and freedoms and much of its communications is of the same character as between a lawyer and its client.

24. The government has also stressed that the Court must not make an examination of Swedish law *in abstracto* (government's observations of 8 May 2015, §§ 138 and 157). In this respect, the applicant can agree with the government that the present application, to some extent, is abstract since most of the FRA's activities are secret. This does not, however, mean that the applicant is asking the Court to make an *in abstracto* analysis of the case. However, the applicant is asking the Court to make the examination according to the principles set out in its previous case-law (*Kennedy. v. United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, § 119). A different approach than the one established in the Court's case-law would exclude secret surveillance regimes from the Court's scrutiny.

25. On a very general note, the applicant also wishes to reiterate the importance of domestic remedies so that the general public is not left with a justified and widespread suspicion and concern about the possibility to abuse the Swedish signal intelligence regime (*cf. Kennedy v. United Kingdom*, § 124).

26. In this context, it is important to recall that the only remedy available to the applicant is the possibility to request an inquiry by the Swedish Foreign Intelligence Inspectorate. This inquiry does not entail a complete inquiry into the FRA's activities but only covers the stages after which the collected data has been made available for further processing, *i.e.* as far as the applicant understands as from stages 3 and 4 in the scheme presented above (see prop. 2008/09:201, p 92). The first two stages of interception and storage, and consequently large amounts of data, are thus left without any possibility for scrutiny (Enclosure 2 – Email reply of 2 July 2015 from Anders Herrström at the Swedish Foreign Intelligence Inspectorate).

27. Furthermore, the Inspectorate will only scrutinise data that is available to the FRA at the time of the inquiry. Thus, the applicant would not be informed if illegal surveillance had taken place and even been accessed by other authorities, nations or international organisations but then erased before the date of inquiry.

D. The violation of Article 8 of the Convention

I. Introduction

28. The Court has asked the government to reply to the following questions.

"1. Assuming that the applicant firm can claim to be a victim in the present case, has there been an interference with its rights under Article 8 § 1 of the Convention, and, if so, was that interference in accordance with the law and necessary in terms of Article 8 § 2?

In particular, did such secret surveillance measures comply with the requirements of minimum legislative safeguards and of supervision of the regime as set out in the Court's case-law (see, for instance, Weber and Saravia v. Germany (dec.), no. 54934/00, §95, ECHR 2006-XI, and Kennedy v. United Kingdom, no. 26839/05, §§ 159-169, judgment of 18 May 2010) during each of the three time-periods: a) before 1 January 2009, b) from 1 January to 30 November 2009, and c) as from 1 December 2009?

2. Have the applicant's concerns about secret surveillance measures being applied to it required that it has access to an effective remedy within the meaning of Article 13 of the Convention? If so, has the applicant had an effective remedy at its disposal?"

29. The Court has established that the requirement that any interference must be "in accordance with the law" under Article 8 § 2 of the Convention will only be met where the quality of the legislation meets certain standards. The Court has also noted that the requirement of "foreseeability" in the context of secret interception of communications cannot be the same as in many other fields (see *Kennedy v. United Kingdom*, §§ 151-152).

30. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has stated that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Kennedy v. United Kingdom*, § 153 with further references).

31. Since the “in accordance with the law” and “necessity” requirements in part overlap in the field of secret surveillance regimes, the Court has examined these jointly (*cf*. *Kennedy v. United Kingdom*, § 155). The applicant will follow that disposition.

32. Moreover, when making this assessment, the Court has acknowledged that the state enjoy a *certain* margin of appreciation (*Kennedy v. United Kingdom,* § 154, *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, § 49 and *Kvasnica v. Slovakia*, Application no. 72094/01, judgment of 9 June 2009, § 80). The applicant thus disagrees with the government’s contention that the state has a fairly wide margin of appreciation in the field (*cf*. §§ 62 and 81 in the government’s observations of 8 May 2015).

II. The signal intelligence regime does not meet the requirements of minimum legislative safeguards

33. The applicant would first of all like to recall that the convention system, which the Court has to safeguard, is governed by the principle of rule of law. However, in a situation like the present one where the activities under scrutiny are covered by very strict secrecy, the principle of rule of law risks to be undermined unless very high standards apply to the quality and foreseeability of the law.

34. The Court’s case-law on the requirements on the law in a context of measures of secret surveillance and interception of communications, as in the present case, can be summed up in six criteria that must be sufficiently addressed to meet the standard of the Convention (*cf. e.g*. *Kennedy v. United Kingdom*, § 152): 1) The nature of the offences which may give rise to an interception order, 2) a definition of the categories of people susceptible to surveillance, 3) a limit on the duration of such surveillance, 4) the procedure to be followed for examining, using and storing the data obtained, 5) the precautions to be taken when communicating the data to other parties and 6) the circumstances in which data obtained may or must be erased and records destroyed.

35. The applicant will in the following comment on these requirements one by one.

a. First requirement - the nature of the offences which may give rise to an interception order

36. In its observations of 8 May 2015, the government emphasises that intelligence gathering is distinct from investigation of crime and seems to question if this first requirement is appropriate in the present case (§§ 23 and 65). The applicant is not convinced this distinction can be fully upheld in practice and consequently finds it important that the Court maintains its case-law in this respect. Already the fact that authorities whose task lie with the investigation of crime can request signal intelligence undermines this distinction (*cf.* the government's observations of 8 May 2015, §§ 103-106).

37. Moreover, even if signal surveillance by the FRA cannot solely be initiated for the purpose of investigating crime, if the FRA has obtained information to this end, this information can either be accessed directly by crime investigating authorities in accordance with Section 9 of the Ordinance (2007:261) on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment (further on the Personal Data Ordinance) or be passed on by the FRA according to Section 8 of the Signal Intelligence Act. To be born in mind is also the fact that illegally obtained evidence is not as such inadmissible in Swedish criminal proceedings.

38. Turning to the first two periods, the law only specified that signal intelligence could be conducted for the purpose of foreign intelligence. The preparatory works further explaining the meaning of foreign intelligence were also very broadly phrased, referring to for example different types of supply crises, ecological imbalances and economic challenges such as currency or interest speculations (prop. 2006/07:63 p. 17, the meaning being even more unclear during the first period, *cf.* the government's observations of 8 May 2015, § 71). In other words, the purpose for which signal intelligence could be conducted was very broadly defined and very hard to adduce any conclusions from. Thus it did not meet the first requirement (*cf. Liberty and Others v. United Kingdom*, Application no. 58243/00, judgment of 1 July 2008, §§ 64-65).

39. The Swedish legislator recognised this legislative deficiency and in the amended law applicable on the third time period, it elaborated further upon the meaning of foreign intelligence (*cf*. Section 1 § 2 subsections 1 to 8 of the Signal Intelligence Act). This was undoubtedly an improvement.

40. However, the amended law still opens up for signal intelligence to be conducted for the purpose of so called development activities. The third paragraph of Section 1 the Signal Intelligence Act states that:

> "If it is necessary for the Foreign Intelligence electronic signals may also be retrieved to
>
> 1. follow changes in the signal environment in the world, the technical development and signal protection, as well as,
>
> 2. to continuously develop the technique and methodology that is needed for the activities under the Signal Intelligence Act."
>
> [applicant's translation]

41. In this respect, the Swedish signal intelligence regime has clear similarities to the signal intelligence regime in the US where bulk collection of data was used to create a repository "necessary to the application of certain analytic techniques". This expansive practice was rejected by the US Court of Appeals in *ACLU v. Clapper* as being "unprecedented and unwarranted" (pp. 58-59).

42. Whereas activities for which signal intelligence can be conducted for foreign intelligence have clear affinities to various criminal offences in the Swedish Criminal Code such as crimes against the security of the nation, this cannot be said for activities for which signal intelligence conducted for the so called development activities.

43. Thus, Swedish signal intelligence is done not only for traditional foreign intelligence but also for so called development activities. This opens up for bulk collection of data that fails to meet the requirement to specify for which offence interception can be ordered. Consequently, also the third time period fails to meet the first requirement.

b. Second requirement - a definition of the categories of people susceptible to surveillance

44. During the first time period, the categories of people susceptible to surveillance was not specified at all. During the second time period, it was specified that signals in cables could only be collected if the signal crossed Swedish borders (Section 2 of the Signal Intelligence Act). During the third time period, it was specified that signals between a sender and recipient that are both in Sweden should not be collected. However, this requirement is circumvented by the exception that, if such signals cannot be separated at the collection, the data should be destroyed as soon as it is clear that such signals have been collected.

45. The specification added during time periods two and three lacks practical significance since any signal, sent from Sweden to a recipient in Sweden, when transmitted via cable can still pass Swedish borders, even more than once, before it reaches the recipient.

46. The Internet Foundation In Sweden (an independent organization for the benefit of the public responsible for certain semi-official duties such as registration of domain names at .se and the administration and technical maintenance of the national domain-name) has also explained that when a signal passes a border it is not technically possible to establish the location of the sender or the receiver. In fact, the establishment of the location of the sender and receiver demands considerable analysis of the data collected and it is the applicant's understanding that such analysis is not made on a regular basis. The location of the sender and receiver thus remain unknown regarding the majority of the data collected and is consequently not destroyed. It has furthermore also been established that the FRA has collected signals where both the sender and receiver are in Sweden (*cf.* the government's observations of 8 May 2015, § 108 and the report of the Data Inspection Board of 6 December 2010, p. 4).

47. The applicant therefore maintains that the categories of people susceptible to surveillance is not sufficiently defined to meet the second requirement.

c. Third requirement - a limit on the duration of such surveillance

48. The applicant is satisfied that the legislation in force during the second and third time periods which provide that permits to conduct signal intelligence should be limited to six months with possible renewal for a maximum period of six months for each renewal, is sufficient to fulfil the third requirement of a limit of the duration of surveillance. The applicant notes that this means that, in practice, surveillance can continue endlessly.

49. However, no corresponding limitation of the duration existed during the first time period. The first time period thus failed to meet the third requirement.

d. Fourth requirement - the procedure to be followed for examining, using and storing the data obtained

50. The applicant maintains that the procedure for examining, using and storing data is only regulated through legislation in very broad terms.

51. Thus, the initiation of signal surveillance can be instructed by the government and a number of authorities specified in the law. The instructions should be in line with the tasking directives as defined by the government (which are not known to the public, see Enclosure 1) and then further specified by a number of other authorities.

52. During the first time period the FRA was not required to ask permission before initiating signal surveillance. During the second time period the FRA could still initiate surveillance without any prior permission when instructed by the government. As of the third time period, any signal intelligence conducted by the FRA requires prior permission from the Foreign Intelligence Court (whose activities are secret and whose members, except for the chair, are elected for a limited time period, see § 19 above).

53. The procedure for using the collected data is also to a large extent unclear. From what the applicant can understand, the data collected is used for two main purposes.

54. Firstly, the data collected for foreign intelligence under Section 1 § 2 of the Signal Intelligence Act after being analysed is used to produce reports that are transmitted to other authorities, nations or international organisations (Sections

8 and 9 of the Signal Intelligence Act). There is no exhaustive list of whom this sharing can be done with.

55. Secondly, the data collected for the so called development activities under Section 1 § 3 of the Signal Intelligence Act appears to be used for among others things; the development of technology and software to enable effective signal intelligence.

56. Furthermore, a number of authorities have direct access to the collected data (Section 9 of the Ordinance Personal Data Ordinance, also see §§ 61-64 below). How these authorities use these collections is not specified by law. This flaw furthermore undermines the government's contention that the data collected is only being used for intelligence gathering and is not used for other purposes (see the government's observations of 8 May 2015, §§ 23-24 and *cf.* Section 4 of the Signal Intelligence Act).

57. The government's argument that the recipient, if a Swedish authority, is also subjected to secrecy regulations is a scarce comfort to the applicant (the government's observations of 8 May 2015, § 42).

58. When it comes to the storing of data obtained, it appears from the Personal Data Ordinance that data is being stored in seven different data collections (Section 2 to 6b of the Personal Data Ordinance).

59. Different collections are governed by different rules regarding the destruction of data. It is thus of utmost importance that data is stored in the correct collection. However, it is unclear which data should be stored in which collection – something that has been criticised by the Swedish Foreign Intelligence Inspectorate (Enclosure 3 – Swedish Foreign Intelligence Inspectorate, decision of 19 June 2013, registration no. 27-2013H:5 – this resulted in the creation of two additional collections under Sections 6a and b of the Personal Data Ordinance, for which no destruction of material is required).

60. The procedure to be followed for examining, using and storing the data obtained is thus not sufficiently specified to meet the fourth requirement.

e. Fifth requirement – the precautions to be taken when communicating the data to other parties

61. It appears that data collected by the FRA can be shared with other Swedish authorities, other nations and international organisations. The conditions for such sharing are broadly held and leave a large discretion to the FRA (Section 8 of the Signal Intelligence Act, Chapter 1 Section 17 of the Act (2007:259) on processing of personal data in the foreign intelligence and development operations of the National Defence Radio Establishment, further on the Personal Data Act, and Section 9 of the Personal Data Ordinance). Such vague legislation opens up for abuses which is indeed illustrated by, the FRA's inability to justify that information had been shared with the Secret Security Service (Enclosure 4 - Swedish Foreign Intelligence Inspectorate, decision of 14 December 2011, registration no. 5-2011KH:4 in which the following was clarified: "The FRA also informed that even if it cannot assess if information that is reported to authorities that cannot initiate surveillance, for example the Secret Security Service, is required by these authorities since there is no dialogue with them to this end. FRA stated that it, in these situations, considered the needs these authorities had before the current legislation entered into force" p. 2(6) [applicant's translation]).

62. The applicant also has concerns about the fact that a number of authorities, namely the Government Offices, the Swedish Security Service, the Swedish Police (the Department of National Operations), the Inspectorate of strategic products, the Swedish Armed Forces, the Swedish Defence Materiel Administration, the Swedish Defence Research Agency, the Swedish Civil Contingencies Agency and Swedish Customs, to the extent decided by the FRA, has direct access to the data collections (Section 9 Personal Data Ordinance).

63. The right to direct access is limited to persons within these authorities that need access to the data in their work. However, there are no further details of the arrangements provided for. For example there are no particular security clearance or limitation to the access (a "need to know" selection), such as in the *Kennedy v. United Kingdom* case (§ 163).

64. The applicant therefore maintains that precautions to be taken when communicating data to other parties must be more explicit and leave less discretion to the FRA in order to satisfy the fifth requirement.

f. Sixth requirement - the circumstances in which data obtained may or must be erased and records destroyed

65. The Court has established that the law must in detail provide when data must be destroyed (*Weber and Saravia v. Germany*, Application no. 54934/00, 29 June 2006, § 100). This should be contrasted with the current legislation that does not, and has not during any of the three time periods, entailed a general obligation to destroy data. On the contrary, the main rule is that the FRA stores the data according to its own discretion.

66. Personal data, *i.e.* data that directly or indirectly can be referred to a living physical person, should be destroyed when no longer needed (Chapter 6 Section 1 Personal Data Act and Sections 2 to 6b of the Personal Data Ordinance). However, the majority of data collections are not bound by any further instructions on when sorting out should take place and who has the responsibility to make sure that the data is destroyed (*cf*. Sections 3, 4, 6a and 6b of the Personal Data Ordinance).

67. It should also be noted that the data about the applicant, since it is an organisation, cannot be regarded as personal data within the meaning of the Personal Data Act. The legislative protection for legal persons is thus lower than for physical persons.

68. The obligation under Section 7 of the Signal Intelligence Act to destroy content that concerns a certain physical person is limited to information that has been considered to lack relevance under Section 1 of the Signal Intelligence Act, *i.e.* foreign intelligence or the so called development activities. This obligation thus becomes void of any practical relevance when the obligation to destroy content is not paired with any statutory time limit when a consideration of the relevance of the material should be done.

69. Consequently, there is much uncertainty regarding *if* and *when* data is being destroyed, which leads to the conclusion that also the sixth requirement is not fulfilled.

III. The supervision of the signal intelligence regime is inadequate

70. As stated above, the Court has stated that the assessment of a secret surveillance regime depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy that is provided by the national law (*Kennedy v. United Kingdom*, §153).

71. The applicant has above explained why the signal intelligence regime at stake fails to meet legislative safeguards such as the nature, scope and duration of the possible measures and the grounds required for ordering them. These deficiencies also pinions any supervisory regime.

a. The authorities competent to authorise signal surveillance

72. The requirement for a prior authorisation to conduct signal surveillance has varied during the three time periods. The applicant reiterates that the Foreign Intelligence Court, the organ now competent to give such prior authorisations, acts in secrecy and lacks impartiality in that its members, except for the chair, are not permanently elected (see § 52 above).

b. The authorities competent to supervise signal surveillance

73. The applicant has in its previously submissions to the Court criticised the fact that the Swedish Foreign Intelligence Inspectorate was not fully operative (§§ 64-68 of the applicant's observations of 31 August 2012). This has to some extent been rectified over time. However, the review of the Swedish National Audit Office recently pointed out that the Inspectorate's own documentation of its supervisory work is scarce and therefore hard to evaluate. Moreover, the audit also concluded that the Inspectorate lack specified goals for its activities (*Control of foreign intelligence*, RIR 2015:2, pp. 10 and 12).

74. Another important shortcoming in the supervision of the signal intelligence regime is that it lies outside the mandate of the Swedish Foreign Intelligence Inspectorate to assess the signal intelligence regime's compatibility with the Convention. Similarly, it falls outside the scope of Inspectorate's mandate to assess if a very large bulk collection of data is necessary for an effective

foreign intelligence. This has not been evaluated by any independent authority (*cf. Do NSA's Bulk Surveillance Programs Stop Terrorists?,* Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahall, National Security Program, the New America Foundation, January 2014).

c. The kind of remedy provided by national law

75. The applicant reiterates that the Swedish Foreign Intelligence Inspectorate can, on the request of legal or physical persons, control that the FRA has not acted illegally. As stated above, the Inspectorate's scrutiny is limited to the final two stages of the surveillance regime and only to data available to the FRA at the time of the inquiry. The Inspectorate can furthermore order the abortion of surveillance and the destruction of data stored. However, it lacks the power to grant compensation (*cf. Kennedy v. United Kingdom*, § 168).

76. It can be noted that physical persons, thus not a remedy available to the applicant, can request that the selectors that have been used which are linked to their person be scrutinised. This remedy was only introduced during the third time period.

77. The requirement to *post factum*, inform a person that secret surveillance measures have been applied is also void of practical meaning since, due to secrecy, it has to today's date never been used.

IV. Conclusion

78. To conclude, there are serious loopholes in the current legislation and the law can therefore not be said to provide safeguards against arbitrary interference with the right to private life. These deficiencies overspills on the supervisory regime which to a large extent operates in secret or has very scarce documentation. The remedies available to the applicant furthermore only cover a fraction of the FRA's activities.

79. The Swedish signal intelligence regime therefore fails to meet the requirements of "in accordance with law" and "necessary in a democratic society" and is thus in violation of the applicant's rights under Article 8 of the Convention.

E. The violation under Article 13 of the Convention

80. The remedies available to the applicant have already been discussed above when making an overall assessment if a surveillance regime meets the requirements of “in accordance with law” and “necessity” provided for under Article 8 § 2 of the Convention.

81. However, to meet the standards of Article 13 it is required that the remedies available to the applicant are effective as such. However, Article 13 does not require that a domestic remedy can challenge the existence of the legislation putting in place the signal surveillance regime (*Kennedy v. United Kingdom*, § 197).

82. The government refers to a large number of remedies such as the Parliamentary Ombudsmen, The Chancellor of Justice, the Data Inspection Board (the government’s observations of 8 May 2015, §153). The government further suggests that it is possible to ask the FRA to disclose a public document and that a rejection by the FRA could be appealed to the final two administrative court instances (§ 154). The government also suggests that the applicant could claim compensation before the ordinary courts (§§ 133 and 153).

83. All these suggestions appear farfetched, tedious and in the end ineffective to the applicant.

84. Due to the secrecy surrounding the FRA’s activities, the Swedish Foreign Intelligence Inspectorate and the Data Inspection Board have been given the explicit competence to overview the work of the FRA. Again, the Data Inspection Board’s mandate is limited to the control of the use personal data. A term that does not include the applicant firm.

85. In light of the foregoing, the applicant will again reiterate that the only remedy available to the applicant is the control by the Swedish Foreign Intelligence Inspectorate. This control is, as mentioned before, limited to the last two stages of the surveillance conducted by the FRA and does not cover all data stored with the FRA.

86. The control is also limited to data available at the moment in time when the request is made which further limits the effectiveness of The Swedish Foreign Intelligence Inspectorate as an effective remedy (see also prop. 2008/09:201 pp. 80-82).

87. The applicant's right to an effective remedy under Article 13 of the Convention has thus been violated.

F. Claims for just satisfaction

88. The applicant does not claim any compensation for either pecuniary or non-pecuniary damages but is satisfied that the finding of a violation is sufficient redress.

89. However, the applicant would ask the Court to order the reimbursement for its costs for legal assistance. The written submissions on behalf of the applicant have been done by the applicant's employees. The time consumed for the written submissions, including the present one, amount to a total of 217 hours (for the application - 50 hours, observations of 25 February 2009 - 2 hours, observations of 3 January 2011 – 50 hours, observations of 31 August 2012 – 50 hours, observations of 2 April 2013 – 15 hours and the current observations of 31 August 2015 – 50 hours).

90. In domestic proceedings, the applicant normally charges the lowest legal aid rate which for 2015 amount to SEK 1 302 per hour. Using this rate, the legal costs would in total amount to SEK 282 534.

G. Summary

91. Pinning down the most pertinent arguments, the applicant maintains that the scope of the signal intelligence surveillance conducted by the FRA is unprecedented. The applicant's concerns that it has been illegally intercepted by the FRA cannot be fully scrutinised by any control mechanism.

92. All stages of interception constitute an interference in the applicant's private life and the contention that interception of metadata is less intrusive is, especially against the background of the technical developments, not adequate.

93. The applicant can therefore claim to be a victim of a violation of the right to private life under Article 8 of the Convention and the application should be declared admissible.

94. When assessing if a secret surveillance regime meets the standards of Article 8 of the Convention, the Court has developed a set of requirements regarding the quality of the legislation and supervision set in place.

95. It can be concluded that the Swedish signal intelligence regime is phrased in broad terms making it difficult to foresee in practice. The legislation also has obvious loopholes since a number of authorities have direct access to the FRA's data collections and FRA has the possibility to pass on information to any Swedish authority, other countries and international organisations. The rule of direct access or the passing on of information are very broadly held.

96. Moreover, there is no general rule to destroy data and the rules to destroy personal data that do exist, lack practical effect since they are not always paired with any time limits to sort out data that should be destroyed.

97. The government has referred to a large number of remedies that it claims would, at least seen together, constitute an effective remedy to the applicant. In the applicant's view the majority of the remedies suggested lack relevance and would if they were all used.

98. In fact, the only adequate remedy available to the applicant is that to make a request to the Swedish Foreign Intelligence Inspectorate. However, the Inspectorate's control does not cover all data stored with the FRA but only a limited amount. It is thus an insufficient remedy.

99. The Swedish signal intelligence regime thus fails to meet the requirements on the legislative safeguards and the supervisory regime. The applicant's right to private life under Article 8 of the Convention has consequently been violated.

100. The deficiencies of the supervisory regime furthermore constitutes a violation of the applicant's right to an effective remedy under Article 13 of the Convention.

101. The applicant considers that the finding of a violation constitutes sufficient redress.

Clarence Crafoord Anna Rogalska Hedlund

H. List of enclosures:

Enclosure 1 – Decision by the government on 6 August 2015, registration no. Fö2015/01013/RS

Enclosure 2 – Email reply of 2 July 2015 from Anders Herrström at the Swedish Foreign Intelligence Inspectorate

Enclosure 3 – Swedish Foreign Intelligence Inspectorate, decision of 19 June 2013, registration no. 27-2013H:5

Enclosure 4 - Swedish Foreign Intelligence Inspectorate, decision of 14 December 2011, registration no. 5-2011KH:4