



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRAND CHAMBER

CASE OF CENTRUM FÖR RÄTTVISA v. SWEDEN

(Application no. 35252/08)

JUDGMENT

Art 8 • Private life • Convention compliance of secret surveillance regime including bulk interception of communications and intelligence sharing • Need to develop case-law in light of important differences between targeted interception and bulk interception • Adapted test for examining bulk interception regimes through global assessment • Focus on “end-to-end safeguards” to take into account the increasing degree of intrusion with privacy rights as the bulk interception process moves through different stages • Shortcomings through: absence of clear rule on destroying intercepted material not containing personal data; absence of a requirement to consider privacy of individuals when deciding whether to transmit intelligence material to foreign partners; dual role of Foreign Intelligence Inspectorate and absence of reasoned decisions in *ex post facto* control, not sufficiently compensated by safeguards

STRASBOURG

25 May 2021

This judgment is final but it may be subject to editorial revision.

In the case of Centrum för rättvisa v. Sweden,

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Robert Spano, *President*,
Jon Fridrik Kjølbro,
Angelika Nußberger,
Paul Lemmens,
Yonko Grozev,
Vincent A. De Gaetano,
Paulo Pinto de Albuquerque,
Faris Vehabović,
Iulia Antoanella Motoc,
Carlo Ranzoni,
Mārtiņš Mits,
Gabriele Kucsko-Stadlmayer,
Marko Bošnjak,
Tim Eicke,
Darian Pavli,
Erik Wennerström,
Saadet Yüksel, *judges*,


and Søren Prebensen, *Deputy Grand Chamber Registrar*,

Having deliberated in private on 11 July, 4 and 6 September 2019 and on 17 February 2021,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in an application (no. 35252/08) against the Kingdom of Sweden lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by a Swedish foundation, Centrum för rättvisa (“the applicant”), on 14 July 2008.

2. The applicant was represented by Mr F. Bergman and Ms A. Evans, lawyers practising in Stockholm. The Swedish Government (“the Government”) were represented by their Agent, , Director General for Legal Affairs, Ministry for Foreign Affairs.

3. The applicant alleged that the Swedish legislation and practice in the field of signals intelligence violated its rights under Article 8 of the Convention and that it did not have an effective remedy in this regard, contrary to Article 13 of the Convention.

4. The application was allocated to the Third Section of the Court (Rule 52 § 1 of the Rules of Court). On 1 November 2011 (admissibility) and 14 October 2014 (admissibility and merits) the application was

communicated to the respondent Government. On 19 June 2018 a Chamber of that Section, composed of Branko Lubarda, President, Helena Jäderblom, Helen Keller, Pere Pastor Vilanova, Alena Poláčková, Georgios A. Serghides, Jolien Schukking, judges, and Stephen Phillips, Section Registrar, gave judgment. The Chamber unanimously declared the application admissible and held that there had been no violation of Article 8 of the Convention and that there was no need to examine separately the complaint under Article 13.

5. On 19 September 2018 the applicant requested the referral of the case to the Grand Chamber in accordance with Article 43 of the Convention. On 4 February 2019 the panel of the Grand Chamber granted that request.

6. The composition of the Grand Chamber was determined according to the provisions of Article 26 §§ 4 and 5 of the Convention and Rule 24. The President of the Grand Chamber decided that in the interests of the proper administration of justice, the case should be assigned to the same Grand Chamber as the case of *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13 and 2 others) (Rules 24, 42 § 2 and 71).










7. The applicant and the Government each filed observations (Rule 59 § 1) on the merits of the case.

8. The President of the Grand Chamber granted leave to the Governments of Estonia, France, the Netherlands and Norway to intervene in the written procedure, in accordance with Article 36 § 2 of the Convention and Rule 44 § 3.

9. A hearing took place in public in the Human Rights Building, Strasbourg, on 10 July 2019.

There appeared before the Court:

(a) *for the respondent Government*

 Director General for Legal Affairs, Ministry
for Foreign Affairs, *Agent*,
 Deputy Director, Ministry for Foreign Affairs,
 Senior Legal Adviser, Ministry for Foreign Affairs,
 Deputy Director-General, Ministry of Defence,
 Senior Legal Adviser, Ministry of Defence
 Deputy Director, Ministry of Justice,
 Legal Adviser, Ministry of Infrastructure,
 Chief Legal Adviser, National Defence Radio
Establishment,
 Senior Adviser, National Defence Radio
Establishment, *Advisers.*

(b) for the applicant

Mr F. BERGMAN,

Mrs A. EVANS,

Mr A. OTTOSSON,

Mrs E. PALM,

Counsel,

Counsel,

Counsel,

Adviser.

The Court heard addresses by Ms Evans, Mr Bergman and



THE FACTS

10. The applicant, Centrum för rättvisa, is a foundation established in 2002. It has its headquarters in Stockholm.

11. The applicant represents clients in proceedings concerning rights and freedoms under the Convention or related proceedings under Swedish law. It is also involved in education and research projects and participates in the general public debate on issues concerning individuals' rights and freedoms.

12. The applicant communicates on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax. It asserts that a large part of that communication is particularly sensitive from a privacy perspective. Due to the nature of its function as a non-governmental organisation scrutinising the activities of State actors, it believes that there is a risk that its communications have been or will be intercepted and examined by way of signals intelligence.

13. The applicant has not brought any domestic proceedings, contending that there is no effective remedy for its Convention complaints.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. DOMESTIC LAW AND PRACTICE

A. Generally on signals intelligence

14. Signals intelligence can be defined as intercepting, processing, analysing and reporting intelligence from electronic signals. These signals may be processed to text, images and sound. The intelligence collected through these procedures may concern both the content of a communication and its related communications data (the data describing, for instance, how, when and between which addresses the electronic communication is conducted). The intelligence may be intercepted over the airways – usually from radio links and satellites – and from cables. Whether a signal is transmitted over the airways or through cables is controlled by the communications service providers, that is, the telecom, internet, cable and other such companies which provide various forms of electronic transfer of

information. A great majority of the traffic relevant for signals intelligence is cable-based. The term “communications bearers” (or “signal carriers”) refers to the medium used for transmitting one or more signals. Unless indicated below, the regulation of Swedish signals intelligence does not distinguish between the content of communications and their communications data or between airborne and cable-based traffic.

15. Foreign intelligence is, according to the Foreign Intelligence Act (*Lagen om försvarsunderrättelseverksamhet*; 2000:130), conducted in support of Swedish foreign, defence and security policy, and in order to identify external threats to the country. The activities should also assist in Sweden’s participation in international security cooperation. Intelligence under the Act may only be conducted in relation to foreign circumstances (section 1(1)). This does not preclude that some of the foreign circumstances may have ramifications in Sweden, for example, when following the espionage operations of a foreign power targeting Sweden (preparatory works to amended legislation on foreign intelligence, prop. 2006/07:63, p. 43).

16. The Government determines the direction of the activities; it also decides which authorities may issue more detailed directives and which authority is to conduct the intelligence activities (section 1(2) and 1(3)). The Government issues general tasking directives annually. Foreign intelligence may not be conducted for the purpose of solving tasks in the area of law enforcement or crime prevention, which come under the mandate of the Police Authority, the Security Police and other authorities and which are regulated by different legislation. However, authorities that conduct foreign intelligence may support authorities dealing with law enforcement or crime prevention (section 4). Examples of such support are cryptanalysis and technical help on information security (preparatory works to amended legislation on foreign intelligence, prop. 2006/07:63, p. 136).

17. The collection of electronic signals is one form of foreign intelligence. It is regulated by the Signals Intelligence Act (*Lagen om signalspaning i försvarsunderrättelseverksamhet*; 2008:717), which entered into force on 1 January 2009. Several amendments were made to the Act on 1 December 2009, 1 January 2013, 1 January 2015 and 15 July 2016. Supplementary provisions are found in the Signals Intelligence Ordinance (*Förordningen om signalspaning i försvarsunderrättelseverksamhet*; 2008:923). The legislation authorises the National Defence Radio Establishment (*Försvarets radioanstalt*; henceforth “the FRA”) to conduct signals intelligence (section 2 of the Ordinance compared to section 1 of the Act).

18. During signals intelligence all cable-based cross-border communications are transferred to certain points of collection. No information is stored at these points and a limited amount of data traffic is

transferred to the FRA by communications bearers (parliamentary committee report SOU 2016:45, p. 107).

19. The FRA may conduct signals intelligence within the area of foreign intelligence only as a result of a detailed tasking directive issued by the Government, the Government Offices, the Armed Forces or, as from January 2013, the Security Police and the National Operative Department of the Police Authority (*Nationella operativa avdelningen i Polismyndigheten*; hereafter “NOA”) (sections 1(1) and 4(1) of the Act) in accordance with the issuer’s precise intelligence requirements. However, the direction of the FRA’s “development activities” may be determined solely by the Government (section 4(2)). A detailed tasking directive determines the direction of the intelligence activities and may concern a certain phenomenon or situation, but it may not solely target a specific natural person (section 4(3)).

20. The mandate of the Security Police and the NOA to issue detailed tasking directives aims to improve these authorities’ ability to obtain data about foreign circumstances at a strategic level concerning international terrorism and other serious international crime that may threaten essential national interests. At the time of introduction of the new rules, the Government stated in the preparatory works (prop. 2011/12:179, p. 19) that the mandate is in accordance with the prohibition on conducting signals intelligence for the purpose of solving tasks in the area of law enforcement or crime prevention.

21. According to the Foreign Intelligence Ordinance (*Förordningen om försvarsunderrättelseverksamhet*; 2000:131), a detailed tasking directive shall include information about (i) the issuing authority, (ii) the part of the Government’s annual tasking directive it concerns, (iii) the phenomenon or situation intended to be covered, and (iv) the need for intelligence on that phenomenon or situation (section 2a).

B. Scope of application of signals intelligence

22. The purposes for which electronic signals may be collected as part of foreign intelligence are specified in the Signals Intelligence Act (section 1 (2)) which provides that signals intelligence may be conducted only to survey:

1. external military threats to the country;
2. conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations;
3. strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests;

4. the development and proliferation of weapons of mass destruction, military equipment and other similar specified products;
 5. serious external threats to society's infrastructure;
 6. foreign conflicts with consequences for international security;
 7. foreign intelligence operations against Swedish interests; and
 8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy.
23. These eight purposes are further elaborated upon in the preparatory works to the legislation (prop. 2008/09:201, pp. 108-109):

“The purposes for which permits to conduct signals intelligence may be granted are listed in eight points. The first point concerns external military threats to the country. Military threats include not only imminent threats, such as threats of invasion, but also phenomena that may in the long term develop into security threats. Consequently, the wording covers the surveying of military capabilities and capacities in our vicinity.

The second point comprises both surveying necessary to provide an adequate basis for a decision whether to participate in international peacekeeping or humanitarian missions and surveying performed during ongoing missions concerning threats to Swedish personnel or other Swedish interests.

The third point refers to strategic surveying of international terrorism or other serious cross-border crime, such as drug or human trafficking of such severity that it may threaten significant national interests. The task of signals intelligence in relation to such activities is to survey them from a foreign and security policy perspective; the intelligence needed to combat the criminal activity operatively is primarily the responsibility of the police.

The fourth point addresses the need to use signals intelligence to follow, among other things, activities relevant to Sweden's commitments in regard to non-proliferation and export control, even in cases where the activity does not constitute a crime or contravenes international conventions.

The fifth point includes, among other things, serious IT-related threats emanating from abroad. That the threats should be of a serious nature means that they, for example, should be directed towards vital societal systems for energy and water supply, communication or monetary services.

The sixth point refers to the surveying of such conflicts between and in other countries that may have consequences for international security. It may concern regular acts of war between States but also internal or cross-border conflicts between different ethnic, religious or political groups. The surveying of the conflicts includes examining their causes and consequences.

The seventh point signifies that intelligence activities conducted against Swedish interests can be surveyed through signals intelligence.

The eighth point provides the opportunity to conduct signals intelligence against foreign powers and their representatives in order to survey their intentions or actions that are of substantial importance to Swedish foreign, security or defence policy. Such activities may relate only to those who represent a foreign power. Through the condition “substantial importance” it is emphasised that it is not sufficient that the phenomenon is of general interest but that the intelligence should have a direct impact on Swedish actions or positions in various foreign, security or defence policy matters. ...”

24. The FRA may collect electronic signals also in order to monitor changes in the international signals environment, technical advances and signals protection and to develop the technology needed for signals intelligence (section 1(3)). This is regarded as “development activities” and, according to the relevant preparatory works (prop. 2006/07:63, p. 72), they do not generate any intelligence reports. Signals intercepted in the context of the FRA’s development activities do not interest the authorities for the data they might contain but only for the possibility to analyse the systems and routes through which information is transmitted. The FRA may share experiences gained on technological issues with other authorities. Development activities usually do not focus on communications between individuals, although information on individuals’ identities may be intercepted.

25. Signals intelligence conducted on cables may only concern signals crossing the Swedish border in cables owned by a communications service provider (section 2). Communications between a sender and receiver within Sweden may not be intercepted, regardless of whether the source is airborne or cable-based. If such signals cannot be separated at the point of collection, the recording of or notes about them shall be destroyed as soon as it becomes clear that such signals have been collected (section 2a).

26. Interception of cable-based signals is automated and must only concern signals that have been identified through the use of selectors (or “search terms”). Such selectors are also used to identify signals over the airways, if the procedure is automated. The selectors must be formulated in such a way that the interference with personal integrity is limited as far as possible. Selectors directly relating to a specific natural person may only be used if this is of exceptional importance for the intelligence activities (section 3).

27. The preparatory works to the Signals Intelligence Act (prop. 2006/07:63, p. 90) clarify that the exceptional importance requirement under section 3 is needed in view of the fact that the use of search terms that are attributable to a particular individual, such as personal names, telephone numbers, email or IP addresses, involves special risks from a privacy protection perspective. The use of such search terms should only be considered under special conditions and should be preceded by a thorough necessity assessment, notably, as to whether the information which can thereby be obtained is of such importance that it justifies the measure. As an example, the text refers to the following hypothetical situation: a national crisis caused by an IT attack against systems of crucial importance to society where immediate action needs to be taken to identify the individual actors.

28. After the signals have been intercepted they are processed, which means that they are, for example, subjected to cryptanalysis or translation.

Then the information is analysed and reported to the authority that gave the FRA the mission to collect the intelligence in question.

29. The process has been described by the respondent Government as comprising six stages, as follows:

1. a choice is made of segments of the signals intelligence environment that are most relevant;
2. selectors are applied automatically to signals in the chosen segments in order to intercept and gradually reduce what is collected;
3. the data is further processed through automatic and manual means using, among others, cryptanalysis, structuring and language translation;
4. the processed information is analysed by an analyst in order to identify intelligence within;
5. a report is written and disseminated to selected recipients of foreign intelligence; and
6. feedback on the use and effects of the intelligence provided is requested and shared with those involved in the process.

C. Authorisation of signals intelligence

30. For all signals intelligence, including the development activities, the FRA must apply for a permit to the Foreign Intelligence Court (*Försvarsunderrättelsesdomstolen*). The application shall contain the mission request that the FRA has received, with information on the relevant detailed tasking directive and the need for the intelligence sought. Also, the communications bearers to which the FRA requires access have to be specified, along with the selectors or categories of selectors that will be used. Finally, the application must state the duration for which the permit is requested (section 4a).

31. A permit may only be granted if the mission is in accordance with the provisions of the Foreign Intelligence Act and the Signals Intelligence Act, if the purpose of the interception of signals cannot be met in a less interfering manner, if the mission can be expected to yield information whose value is clearly greater than the possible interference with personal integrity, if the selectors or categories of selectors are in accordance with the Signals Intelligence Act and if the application does not concern solely a specific natural person (section 5).

32. If granted, the permit shall specify the mission for which signals intelligence may be conducted, the bearers to which the FRA will have access, the selectors or categories of selectors that may be used, the duration of the permit and other conditions necessary to limit the interference with personal integrity (section 5a).

33. The FRA itself may decide to grant a permit, if the application for a permit from the Foreign Intelligence Court might cause delay or other inconveniences of essential importance for one of the specified purposes of

the signals intelligence. If the FRA grants a permit, it has to report to the court immediately and the court shall without delay decide in the matter. The court may revoke or amend the permit (section 5b).

34. The composition of the Foreign Intelligence Court and its activities are regulated by the Foreign Intelligence Court Act (*Lagen om Försvarsunderrättelsesdomstol*; 2009:966). The court consists of one president, one or two vice-presidents and two to six other members. The president is a permanent judge, nominated by the Judges Proposals Board (*Domarnämnden*) and appointed by the Government. The vice-presidents, who must be legally trained and have previous experience as judges, and the other members, who are required to have special expertise of relevance for the court's work, are appointed by the Government on four-year terms. The applications for signals intelligence permits are discussed during hearings, which may be held behind closed doors, if it is clear that information classified as secret would be exposed as a result of a public hearing. During the court's examination, the FRA as well as a privacy protection representative (*integritetsskyddsombud*) are present. The representative, who does not represent any particular person but the interests of individuals in general, monitors integrity issues and has access to the case file and may make statements. Privacy protection representatives are appointed by the Government for a period of four years and must be or have been permanent judges or attorneys. The court may hold a hearing and decide on an application without the presence of a representative only if the case is of such urgency that a delay would severely compromise the purpose of the application. The court's decisions are final.

D. The duration of signals intelligence

35. A permit may be granted for a specific period of time, maximum six months. An extension may, after a renewed examination, be granted for six months at a time (Signals Intelligence Act, section 5a).

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

36. The Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten* (SIUN); see further paragraphs 50-54 below) oversees access to the communications bearers. Communications service providers are obliged to transfer cable-based signals crossing the Swedish borders to "collaboration points" agreed upon with the Inspectorate. The Inspectorate, in turn, provides the FRA with access to bearers in so far as such access is covered by a signals intelligence permit and, in so doing, implements the permits issued by the Foreign Intelligence Court (Chapter 6, section 19a of the Electronic Communications Act (*Lagen*

om elektronisk kommunikation; 2003:389)). The Council on Legislation (*Lagrådet*), the body giving opinions on request by the Government or a Parliamentary committee on certain draft bills, has expressed the view that an interference with private life and correspondence already arises at this point, because of the State obtaining access to the telecommunications (prop. 2006/07:63, p. 172).

37. According to the Signals Intelligence Act, intercepted data must be destroyed immediately by the FRA if it (i) concerns a specific natural person and lacks importance for the signals intelligence, (ii) is protected by constitutional provisions on secrecy for the protection of anonymous authors and media sources, (iii) contains information shared between a suspect and his or her legal counsel and is thus protected by attorney-client privilege, or (iv) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information (section 7).

38. If communications have been intercepted between a sender and receiver who are both in Sweden, despite the prohibition on such interception, they shall be destroyed as soon as the domestic nature of the communications has become evident (section 2a).

39. If a permit urgently granted by the FRA (see paragraph 21 above) is revoked or amended by the Foreign Intelligence Court, all intelligence collected which is thereby no longer authorised must be immediately destroyed (section 5b(3)).

40. The FRA Personal Data Processing Act (*Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:259) contains provisions on the treatment of personal data within the area of signals intelligence. The Act entered into force on 1 July 2007, with amendments effective from 30 June 2009, 15 February 2010 and 1 March 2018. The purpose of the Act is to protect against violations of personal integrity (Chapter 1, section 2). The FRA shall ensure, *inter alia*, that personal data is collected only for certain expressly stated and justified purposes. Such purpose is either determined by the direction of the foreign intelligence activities through a detailed tasking directive or by what is necessary in order to follow changes in the signals environment, technical advances and signals protection. Also, the personal data treated has to be adequate and relevant in relation to the purpose of the treatment. No more personal data than what is necessary for that purpose may be processed. All reasonable efforts have to be made to correct, block and obliterate personal data that is incorrect or incomplete (Chapter 1, sections 6, 8 and 9).

41. Personal data may not be processed solely because of what is known of a person's race or ethnicity, political, religious or philosophical views, membership of a union, health or sexual life. If, however, personal data is treated for a different reason, this type of information may be used if it is

absolutely necessary for the treatment. Information about a person's physical appearance must always be formulated in an objective way with respect for human dignity. Intelligence searches may only use the above-mentioned personal indicators as selectors if this is absolutely necessary for the purpose of the search (Chapter 1, section 11).

42. Personnel at the FRA who process personal data go through an official security clearance procedure and are subject to confidentiality with regard to data to which secrecy applies. They could face criminal sanctions if tasks relating to the processing of personal data are mismanaged (Chapter 6, section 2).

43. Personal data that has been subjected to automated processing is to be destroyed as soon as it is no longer needed (Chapter 6, section 1).

44. Further provisions on the treatment of personal data are laid down in the FRA Personal Data Processing Ordinance (*Förordningen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:261). It provides, *inter alia*, that the FRA may keep databases for raw material containing personal data. Raw material is unprocessed information which has been collected through automated treatment. Personal data in such databases shall be destroyed within one year from when it was collected (section 2).

F. Conditions for communicating the intercepted data to other parties

45. The intelligence collected is to be reported to the authorities concerned, as determined under the Foreign Intelligence Act (Signals Intelligence Act, section 8).

46. The Government Offices, the Armed Forces, the Security Police, the NOA, the Inspectorate of Strategic Products (*Inspektionen för strategiska produkter*), the Defence Material Administration (*Försvarets materialverk*), the Defence Research Agency (*Totalförsvarets forskningsinstitut*), the Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*) and the Swedish Customs (*Tullverket*) may have direct access to completed intelligence reports to the extent the FRA so decides (section 9 of the FRA Personal Data Processing Ordinance). However, to date, no decisions permitting direct access have been taken by the FRA.

47. The FRA may also grant the Security Police and the Armed Forces direct access to data which constitute analysis results in a data collection for analyses and which is needed for the authorities to be able to make strategic assessments of the terrorist threat against Sweden and Swedish interests (Chapter 1, section 15 of the FRA Personal Data Processing Act, and section 13a of the Ordinance).

48. According to the preparatory works (prop 2017/18:36), the above-mentioned access is given within the framework of cooperation between the

FRA, the Security Police and the Armed Forces in a working group called the National Centre for Assessment of Terrorist Threats (*Nationellt centrum för terrorhotbedömning*; “NCT”) where a number of analysts from the three authorities work together and write reports containing strategic assessments of terrorist threats. With the FRA’s permission and as long as the data is relevant for such terrorist threat assessments, the NCT analysts have direct access to “analysis results” contained in the FRA databases. The analysts do not, however, have direct access to the FRA’s databases to conduct their own free searches. Furthermore, while the information made available to the analysts through direct access may contain personal data, the assessments made by the NCT are of a strategic, general nature and are not, as such, directed at individual persons.

49. Personal data may be communicated to other States or international organisations only if this is not prevented by secrecy and if necessary for the FRA to perform its activities within international defence and security cooperation. The Government may adopt rules or decide in a specific case to allow such communication of personal data also in other cases, where necessary for the activities of the FRA (Chapter 1, section 17 of the FRA Personal Data Processing Act). The FRA may disclose personal data to a foreign authority or an international organisation if it is beneficial for the Swedish government (*statsledningen*) or Sweden’s comprehensive defence strategy (*totalförsvaret*); information so communicated must not harm Swedish interests (section 7 of the FRA Personal Data Processing Ordinance).

G. Supervision of the implementation of signals intelligence

50. The Foreign Intelligence Act (section 5) and the Signals Intelligence Act (section 10) provide that an authority is to oversee the foreign intelligence activities in Sweden and verify that the FRA’s activities are in compliance with the provisions of the Signals Intelligence Act. The supervisory authority – the Foreign Intelligence Inspectorate – is, among other things, tasked with monitoring the implementation of the Foreign Intelligence Act and the associated Ordinance and reviewing whether foreign intelligence activities are performed in compliance with the applicable directives (section 4 of the Foreign Intelligence Inspectorate Instructions Ordinance (*Förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*; 2009:969)). It also reviews compliance with the Signals Intelligence Act by examining in particular the selectors used, the destruction of intelligence and the communication of reports; if an inspection reveals that a particular intelligence collection is incompatible with a permit, the Inspectorate may decide that the operation shall cease or that the intelligence shall be destroyed (section 10 of the Signals Intelligence Act). The FRA shall report

to the Inspectorate the selectors which directly relate to a specific natural person (section 3 of the Signals Intelligence Ordinance).

51. The Foreign Intelligence Inspectorate is led by a board whose members are appointed by the Government for terms of at least four years. The president and the vice-president shall be or have been permanent judges. Other members are selected from candidates proposed by the party groups in the Parliament (section 10 (3) of the Signals Intelligence Act).

52. Any opinions or suggestions for measures arising from the Inspectorate's inspections shall be forwarded to the FRA, and if necessary also to the Government. The Inspectorate also submits annual reports on its inspections to the Government (section 5 of the Foreign Intelligence Inspectorate Instructions Ordinance), which are made available to the public. Furthermore, if the Inspectorate notices potential crimes, it shall report the matter to the Prosecution Authority (*Åklagarmyndigheten*), and, if deficiencies are discovered that may incur liability for damages for the State, a report shall be submitted to the Chancellor of Justice (*Justitiekanslern*). A report may also be submitted to the Data Protection Authority (*Datainspektionen*), which is the supervisory authority on the treatment of personal data by the FRA (section 15).

53. From the establishment of the Inspectorate in 2009 until 2017 the Inspectorate conducted 102 inspections in total. Those resulted in 15 opinions submitted to the FRA and one to the Government. No inspections have revealed reasons to cease an intelligence collection or to destroy the results. According to the Inspectorate's annual reports, which contain brief descriptions of the inspections, those have included numerous detailed examinations of the selectors used, the destruction of intelligence, the communication of reports, the treatment of personal data and the overall compliance with the legislation, directives and permits relevant to the signals intelligence activities. For instance, between 2010 and 2014 the use of selectors was inspected on seventeen occasions, which led to one opinion and a proposal for changes to the FRA's processing routines. During the same period the destruction of data related to signals intelligence was audited on nine occasions. Those also resulted in one opinion, in 2011, inviting the FRA to amend its internal regulations, which it did the same year. During 2011 the Inspectorate also verified whether the FRA was conducting data collection for other countries in accordance with the law, which did not lead to any opinion being issued. An inspection in 2014 concerned a general review of the FRA's cooperation with other States and international organisations in intelligence matters. It did not give rise to any opinion or suggestion to the FRA. In 2015 and 2016 an overall review to assess compliance with the limitations stated in permits issued by the Foreign Intelligence Court resulted in one observation. In 2016 and 2017 the Inspectorate carried out a detailed inspection of the treatment by the FRA of personal data. The inspection concerned the processing of sensitive

personal data in connection with strategic circumstances relating to international terrorism and other serious cross-border crime threatening significant national interests. The inspection did not give rise to any opinion or suggestion. However, during that year, one opinion was submitted to the Government following an inspection of whether the FRA's intelligence activities complied with the tasking directives given. During the years 2009-2017 the Inspectorate found reason to make a report to another authority – the Data Protection Authority – on one occasion, concerning the interpretation of a legal provision. In its annual reports, the Inspectorate has noted that it has been given access to all the information necessary for its inspections.

54. The supervisory activities of the Foreign Intelligence Inspectorate have been audited by the National Audit Office (*Riksrevisionen*), a body answerable to Parliament. In a report published in 2015 the Office noted that the FRA had routines in place for handling the Inspectorate's opinions and that the supervision helped develop the activities of the FRA. Suggestions were dealt with in a serious manner and, when called for, gave rise to reforms. With the exception of one case when the FRA referred the matter to the Government, the FRA took the action decided by Inspectorate. At the same time the Office criticised the Inspectorate's lack of documentation of inspections and the fact that there were no clearly specified goals for the inspections.

55. Within the FRA there is a Privacy Protection Council tasked with continuously monitoring measures taken to ensure protection of personal integrity. The members are appointed by the Government. The Council reports its observations to the FRA management or, if the Council finds reasons for it, to the Inspectorate (section 11 of the Signals Intelligence Act).

56. Further provisions on supervision are found in the FRA Personal Data Processing Act. The FRA shall appoint one or several data protection officers and report the appointment to the Data Protection Authority (Chapter 4, section 1). The data protection officer is tasked with independently monitoring that the FRA treats personal data in a legal and correct manner and point out any deficiencies. If deficiencies are suspected and no correction is made, a report shall be submitted to the Data Protection Authority (Chapter 4, section 2).

57. The Data Protection Authority, which is an authority under the Government, has, on request, access to the personal data that is processed by the FRA and to documentation on the treatment of personal data along with the security measures taken in this regard as well as access to the facilities where personal data is processed (Chapter 5, section 2). If the Authority finds that personal data is or could be processed illegally, it shall try to remedy the situation by communicating its observations to the FRA (Chapter 5, section 3). It may also apply to the Administrative Court

(*förvaltningsrätten*) in Stockholm to have illegally processed personal data destroyed (Chapter 5, section 4). According to copies of an email exchange of April 2019 between the applicant and the Administrative Court, there was no trace in that court's electronic records of the latter possibility having been used by the Data Protection Authority.

H. Notification of secret surveillance measures

58. If selectors directly related to a specific natural person have been used, he or she is to be notified by the FRA, according to the Signals Intelligence Act. The notification shall contain information on the date and purpose of the measures. Such notification shall be given as soon as this can be done without detriment to the foreign intelligence activities, but no later than one month after the signals intelligence mission has been concluded (section 11a).

59. However, the notification may be delayed if secrecy so demands, in particular defence secrecy or secrecy for the protection of international relations. If, due to secrecy considerations, no notification has been given within a year from the conclusion of the mission, the person does not have to be notified. Furthermore, notification shall not be given if the measures solely concern the conditions of a foreign power or the relationship between foreign powers (section 11b).

60. In its 2010 report, the Data Protection Authority noted, *inter alia*, that the procedure for notification to individuals had never been used by the FRA, due to secrecy considerations (see paragraph 75 below).

I. Remedies

61. The Signals Intelligence Act provides that the Foreign Intelligence Inspectorate, at the request of an individual, must investigate if his or her communications have been intercepted through signals intelligence and, if so, verify whether the interception and treatment of the information have been in accordance with the law. The Inspectorate shall notify the individual that such an investigation has been carried out (section 10a). A request can be made by legal and natural persons regardless of nationality and residence. During the period 2010-2017, 132 requests were handled and no unlawfulness was established. In 2017, ten such requests were processed; in 2016 the number was 14. The Inspectorate's decision following a request is final.

62. Under the FRA Personal Data Processing Act, the FRA is also required to provide information upon request. Once per calendar year, an individual may demand information on whether personal data concerning him or her is being or has been processed. If so, the FRA must specify what information on the individual is concerned, from where it was collected, the

purpose of the treatment and to which recipients or categories of recipients the personal data is or was reported. The information is normally to be given within one month from the request (Chapter 2, section 1). However, this right to information does not apply if disclosure is prevented by secrecy considerations (Chapter 2, section 3).

63. Following a request from an individual who has had personal data registered, the FRA shall promptly correct, block or destroy such data that has not been processed in accordance with law. The FRA shall also notify any third party who has received the data, if the individual so requests or if substantial harm or inconvenience could be avoided through a notification. No such notification has to be given if it is impossible or would involve a disproportionate effort (Chapter 2, section 4).

64. The FRA's decisions on disclosure and corrective measures in regard to personal data may be appealed against to the Administrative Court in Stockholm (Chapter 6, section 3). According to copies of an email exchange of April 2019 between the applicant and the Administrative Court, there was no trace in that court's electronic records of that possibility having been used.

65. The State is liable for damages following a violation of personal integrity caused by treatment of personal data not in accordance with the FRA Personal Data Processing Act (Chapter 2, section 5). A request for damages shall be submitted to the Chancellor of Justice.

66. In addition to the above remedies, laid down in the legislation relating to signals intelligence, Swedish law provides for a number of other means of scrutiny and complaints mechanisms. The Parliamentary Ombudsmen (*Justititeombudsmannen*) supervise the application of laws and regulations in public activities; courts and authorities are obliged to provide information and opinions at the request of the Ombudsmen (Chapter 13, section 6 of the Instrument of Government – *Regeringsformen*), including access to minutes and other documents. The Ombudsmen shall ensure, in particular, that the courts and authorities observe the provisions of the Instrument of Government on objectivity and impartiality and that citizens' fundamental rights and freedoms are not encroached upon in public activities (section 3 of the Parliamentary Ombudsmen Instructions Act – *Lagen med instruktion för Riksdagens ombudsmän*; 1986:765). The supervision, under which the Foreign Intelligence Court and the FRA come, is conducted by means of examining complaints from the public and through inspections and other investigations (section 5). The examination is concluded by a decision in which, although not legally binding, the opinion of the Ombudsman is given as to whether the court or authority has contravened the law or otherwise taken a wrongful or inappropriate action; the Ombudsman may also initiate criminal or disciplinary proceedings against a public official who has committed a criminal offence or neglected his or her duty in disregarding the obligations of the office (section 6).

67. With a mandate similar to the Parliamentary Ombudsmen, the Chancellor of Justice scrutinises whether officials in public administration comply with laws and regulations and otherwise fulfil their obligations (section 1 of the Chancellor of Justice Supervision Act – *Lagen om justitiekanslerns tillsyn*; 1975:1339). The Chancellor does so by examining individual complaints or conducting inspections and other investigations, which could be directed at, for instance, the Foreign Intelligence Court and the FRA. According to copies of an email exchange of April 2019 between the applicant and the office of the Chancellor of Justice, twelve such complaints were received in 2008 and one in 2013. Following examination, none of those had been judged to require action.

68. At the request of the Chancellor, courts and authorities are obliged to provide information and opinions as well as access to minutes and other documents (sections 9 and 10). The decisions of the Chancellor of Justice are similar in nature to the decisions of the Parliamentary Ombudsmen, including their lack of legally binding power. By tradition, however, the opinions of the Chancellor and the Ombudsmen command great respect in Swedish society and are usually followed (see *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 118, ECHR 2006-VII). The Chancellor has the same power as the Ombudsmen to initiate criminal or disciplinary proceedings (sections 5 and 6).

69. The Chancellor of Justice is also authorised to determine complaints and claims for damages directed against the State, including compensation claims for alleged violations of the Convention. The Supreme Court and the Chancellor of Justice have developed precedents in recent years, affirming that it is a general principle of law that compensation for Convention violations can be ordered without direct support in Swedish statute to the extent that Sweden has a duty to provide redress to victims of Convention violations through a right to compensation for damages (see *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, §§ 58-62 and 67, 20 December 2016, with further references). On 1 April 2018, through the enactment of a new provision – Chapter 3, section 4 – of the Tort Liability Act (*Skadeståndslagen*; 1972:207), the right to compensation for violations of the Convention was codified.

70. In addition to its above-mentioned supervisory functions under the Foreign Intelligence Inspectorate Instructions Ordinance and the FRA Personal Data Processing Act (see paragraphs 52, 56 and 57 above), the Data Protection Authority is generally entrusted with protecting individuals against violations of their personal integrity through the processing of personal data, under the Act with Supplementary Provisions to the EU General Data Protection Regulation (*Lagen med kompletterande bestämmelser till EU:s dataskyddsförordning*) which entered into force on 25 May 2018, the same day as the new EU regulation it supplements (see paragraph 94 below). In regard to the signals intelligence conducted by the

FRA, the Personal Data Act (*Personuppgiftslagen*; 1998:204) continues to apply, although it is otherwise replaced by the new EU Regulation and the supplementary act. It gives the Data Protection Authority the same general supervisory task. In performing this task, the Authority may receive and examine individual complaints.

J. Secrecy at the FRA

71. The Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslagen*; 2009:400) contains a specific provision on the FRA's signals intelligence activities. Secrecy applies to information on an individual's personal or economic circumstances, unless it is evident that the information can be disclosed without the individual concerned or any other person closely related to him or her being harmed. The presumption is for secrecy (Chapter 38, section 4).

72. According to the Act, secrecy also generally applies to foreign intelligence activities in regard to information concerning another State, international organisation, authority, citizen or legal person in another State, if it can be presumed that a disclosure will interfere with Sweden's international relations or otherwise harm the country (Chapter 15, section 1).

73. Secrecy further applies to information on activities related to the defence of the country or the planning of such activities or to information that is otherwise related to the country's comprehensive defence strategy, if it can be presumed that a disclosure will harm the country's defence or otherwise endanger national security (Chapter 15, section 2).

74. Information which is protected by secrecy under the Public Access to Information and Secrecy Act may not be disclosed to a foreign authority or an international organisation unless (i) such disclosure is permitted by an express legal provision (cf. section 7 of the FRA Personal Data Processing Ordinance, paragraph 34 above), or (ii) the information in an analogous situation may be communicated to a Swedish authority and the disclosing authority finds it evident that the communication of the information to the foreign authority or the international organisation is consistent with Swedish interests (Chapter 8, section 3 of the Act).

K. The reports of the Data Protection Authority

75. On 12 February 2009 the Government ordered the Data Protection Authority to examine the handling of personal data at the FRA from an integrity perspective. In its report, published on 6 December 2010, the Authority stated that its conclusions were overall positive. Issues relating to the processing of personal data and to personal integrity were given serious consideration by the FRA and a considerable amount of time and resources

were spent on creating routines and educating its personnel in order to minimise the risk of unwarranted interferences with personal integrity. Moreover, no evidence had been found which indicated that the FRA was handling personal data for purposes not authorised by the legislation in force. However, the Authority noted, *inter alia*, that there was a need to improve the methods for separating domestic and cross-border communications. Even if the FRA had implemented mechanisms in that area, there was no guarantee that domestic communications were never intercepted, and, although the occasions had been very few, such communications had in fact been intercepted. The Authority further noted that the procedure for notification to individuals (paragraphs 58-60 above) had never been used by the FRA, due to secrecy considerations.

76. A second report was issued by the Authority on 24 October 2016. Again, the Authority found no evidence that personal data had been collected for other purposes than those stipulated for the signals intelligence activities. It also noted that the FRA continuously reviewed whether data intercepted was still needed for those purposes. A similar review was made concerning the communications bearers from which the FRA obtained intelligence. Moreover, there was nothing to indicate that the provisions on destruction of personal data had been disregarded (see paragraphs 37-39 above). However, the FRA was criticised for not adequately monitoring logs used to detect unwarranted use of personal data, a shortcoming that had been pointed out already in 2010.

L. The report of the Signals Intelligence Committee

77. On 12 February 2009 the Government also decided to appoint a committee predominantly composed of members of parliament, the Signals Intelligence Committee (*Signalspaningskommittén*), with the task of monitoring the signals intelligence conducted by the FRA in order to examine the implications for personal integrity. The report was presented on 11 February 2011 (*Uppföljning av signalspaningslagen*; SOU 2011:13). The Committee's examination focused primarily on signals intelligence conducted over the airways, as such activities on cable-based traffic had not yet commenced on a larger scale.

78. The Committee concluded that concerns of personal integrity were taken seriously by the FRA and formed an integral part of the development of its procedures. It noted, however, that there were practical difficulties in separating domestic cable-based communications from those crossing the Swedish border. Any domestic communications that were not separated at the automated stage were instead separated manually at the processing or analysing stage. The Committee further observed that the selectors used for communications data were less specific than those used for interception of

the content of a communication and that, consequently, a larger number of individuals could have such data stored by the FRA.

79. Another finding in the report was that the FRA's development activities (see paragraph 24 above) could lead to non-relevant communications being intercepted and possibly read or listened to by FRA personnel. However, the Committee noted that the development activities were directly essential for the FRA's ability to conduct signals intelligence. Moreover, information obtained through the development activities could be used in regular intelligence activities only if such use conformed with the purposes established by law and the relevant tasking directives issued for the signals intelligence.

80. Like the Data Protection Authority, the Committee pointed out that, in reality, the obligation on the FRA to notify individuals who had been directly and personally subjected to secret surveillance measures was very limited due to secrecy; it concluded therefore that this obligation served no purpose as a guarantee for legal certainty or against integrity interferences. The Committee found, however, that, in particular, the authorisation procedure before the Foreign Intelligence Court, in deciding on permits to conduct signals intelligence measures (see paragraphs 30-34 above), and the supervisory functions performed by the Foreign Intelligence Inspectorate (see paragraphs 36 and 50-54 above) and the Privacy Protection Council (see paragraph 55 above) provided important protection for individuals' personal integrity. It noted, in this respect, that, although the Privacy Protection Council formed part of the FRA, it acted in an independent manner.

II. RELEVANT INTERNATIONAL LAW

A. The United Nations

81. Resolution no. 68/167, on The Right to Privacy in the Digital Age, adopted by the General Assembly on 18 December 2013, reads as follows:

“The General Assembly,

...

4. *Calls upon* all States:

...

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for

State surveillance of communications, their interception and the collection of personal data ...”

B. The Council of Europe

1. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and its Additional Protocol (CETS No. 108)

82. The Convention, in force for Sweden since 1 October 1985, sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides, in so far as relevant, as follows:

Preamble

“The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:”

Article 1 – Object and purpose

“The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (“data protection”).”

Article 8 – Additional safeguards for the data subject

“Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

CENTRUM FÖR RÄTTVISA v. SWEDEN JUDGMENT

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.”

Article 9 – Exceptions and restrictions

“1. No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

...”

Article 10 – Sanctions and remedies

“Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.”

83. The Explanatory Report to the above-mentioned Convention explains the following as regards its Article 9:

“...

55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of ‘necessary measures’ that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

56. Littera a in paragraph 2 lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.

States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

The notion of ‘State security’ should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State...”

84. The Additional Protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal

Data, regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181), in force for Sweden since 1 July 2004, provides as follows, in so far as relevant:

Article 1 – Supervisory authorities

“1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

...”

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

“1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of:

– specific interests of the data subject, or

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.”

2. Recommendation of the Committee of Ministers of the Council of Europe on the protection of personal data in the area of telecommunication services

85. Recommendation No. R (95) 4 of the Committee of Ministers on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, adopted on 7 February 1995, reads, insofar as relevant, as follows:

“2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

- a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;
- b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

- a. the exercise of the data subject’s rights of access and rectification;
- b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;
- c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference.”

3. *The 2015 Report of the European Commission for Democracy through Law (“the Venice Commission”) on the Democratic Oversight of Signals Intelligence Agencies*

86. In this report, published in December 2015, the Venice Commission noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data were accessed and/or processed by the agencies. For this reason, the computer analysis (usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

87. According to the report, the two most significant safeguards were the authorisation (of collection and access) and the oversight of the process. It was clear from the Court’s case-law that the latter had to be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where

authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the conditions and limitations set by the court was problematic.

88. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention, since a general complaints procedure to an independent oversight body could compensate for non-notification.

89. The report also considered internal controls to be a “primary safeguard”. Recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

90. The report also considered the position of journalists. It accepted that they were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. It acknowledged, however, that the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

91. Finally, the report considered briefly the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

III. EUROPEAN UNION LAW

A. Charter of Fundamental Rights of the European Union

92. Articles 7, 8 and 11 of the Charter provide as follows:

Article 7 – Respect for private and family life

“Everyone has the right to respect for his or her private and family life, home and communications.”

Article 8 – Protection of personal data

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

Article 11 – Freedom of expression and information

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.”

B. European Union directives and regulations relating to protection and processing of personal data

93. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. As the activities of Member States regarding public safety, defence and State security fell outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

94. The General Data Protection Regulation, adopted in April 2016, superseded the Data Protection Directive and became enforceable on 25 May 2018. The regulation, which is directly applicable in Member States, contains provisions and requirements pertaining to the processing of personally identifiable information of data subjects inside the European Union, and applies to all enterprises, regardless of location, doing business with the European Economic Area. Business processes that handle personal data must be built with data protection by design and by default, meaning that personal data must be stored using pseudonymisation or full anonymization, and use the highest-possible privacy settings by default, so that the data are not available publicly without explicit consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or if the data controller or processor has received explicit, opt-in consent from the data’s owner. The data owner has the right to revoke this permission at any time.

95. A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, how long data are being retained, and if they are being shared with any third-parties or outside of the European Union. Users have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public

authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

96. The Privacy and Electronic Communications Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), adopted on 12 July 2002, states, in recitals 2 and 11:

“(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.”

The Directive further provides, in so far as relevant:

Article 1 – Scope and aim

“1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.”

Article 15 – Application of certain provisions of Directive 95/46/EC

“1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.”

97. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) was adopted. Prior to the judgment of 2014 declaring it invalid (see the paragraph below), it provided, *inter alia*, as follows:

Article 1 - Subject matter and scope

“1. This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.”

Article 3 – Obligation to retain data

“1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

...”

C. Relevant case-law of the Court of Justice of the European Union (“CJEU”)

1. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238)*

98. In a judgment of 8 April 2014 the CJEU declared invalid the Data Retention Directive 2006/24/EC laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation to retain the data constituted in itself an interference with the right to respect for private life and communications guaranteed by Article 7 of the Charter of Fundamental Rights of the EU and the right to protection of personal data under Article 8 of the Charter.

99. The access of the competent national authorities to the data constituted a further interference with those fundamental rights, which the CJEU considered to be “particularly serious”. The fact that data were retained and subsequently used without the subscriber or registered user being informed was, according to the CJEU, likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. The interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security. However, it failed to satisfy the requirement of proportionality.

100. Firstly, the directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population. It applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

101. Secondly, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each Member State in its national law, the directive failed to lay down any objective criterion by which to determine

which offences might be considered to be sufficiently serious to justify such an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued.

102. Thirdly, the directive required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

2. *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970)*

103. In *Secretary of State for the Home Department v. Watson and Others*, the applicants had sought judicial review of the legality of section 1 of the United Kingdom Data Retention and Investigatory Powers Act 2014 (“DRIPA”), pursuant to which the Secretary of State could require a public telecommunications operator to retain relevant communications data if he or she considered it necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (“RIPA”). The applicants claimed, *inter alia*, that section 1 was incompatible with Articles 7 and 8 of the Charter and Article 8 of the Convention.

104. By judgment of 17 July 2015, the High Court held that the *Digital Rights* judgment laid down “mandatory requirements of EU law” applicable to the legislation of Member States on the retention of communications data and access to such data. Since the CJEU, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. In fact, it followed from the underlying logic of the *Digital Rights* judgment that legislation that established a general body of rules for the retention of communications data was in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation was complemented by a body of rules for access to

the data, defined by national law, which provided sufficient safeguards to protect those rights. Accordingly, section 1 of DRIPA was not compatible with Articles 7 and 8 of the Charter as it did not lay down clear and precise rules providing for access to and use of retained data and access to that data was not made dependent on prior review by a court or an independent administrative body.

105. On appeal by the Secretary of State, the Court of Appeal sought a preliminary ruling from the CJEU.

106. Before the CJEU this case was joined with the request for a preliminary ruling from the Administrative Court of Appeal (*kammarrätten*) in Stockholm in Case C-203/15 *Tele2 Sverige AB v Post- och telestyrelsen*. Following an oral hearing in which some fifteen EU Member States intervened, the CJEU gave judgment on 21 December 2016. The CJEU held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, had to be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, where access was not subject to prior review by a court or an independent administrative authority, and where there was no requirement that the data concerned should be retained within the European Union.

107. The CJEU declared the Court of Appeal's question whether the protection afforded by Articles 7 and 8 of the Charter was wider than that guaranteed by Article 8 of the Convention inadmissible.

108. Following the handing down of the CJEU's judgment, the case was relisted before the Court of Appeal. On 31 January 2018 it granted declaratory relief in the following terms: that section 1 of DRIPA was inconsistent with EU law to the extent that it permitted access to retained data where the object pursued by access was not restricted solely to fighting serious crime; or where access was not subject to prior review by a court or independent administrative authority.

3. Ministerio Fiscal (*Case C-207/16; ECLI:EU:C:2018:788*)

109. This request for a preliminary ruling arose after Spanish police, in the course of investigating the theft of a wallet and mobile telephone, asked the investigating magistrate to grant them access to data identifying the users of telephone numbers activated with the stolen telephone during a period of twelve days prior to the theft. The investigating magistrate rejected the request on the ground, *inter alia*, that the acts giving rise to the criminal investigation did not constitute a "serious" offence. The referring court subsequently sought guidance from the CJEU on fixing the threshold of seriousness of offences above which an interference with fundamental rights, such as competent national authorities' access to personal data

retained by providers of electronic communications services, may be justified.

110. On 2 October 2018 the Grand Chamber of the CJEU ruled that Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, had to be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entailed an interference with their fundamental rights which was not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime. In particular, it indicated that:

“In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as ‘serious’.

By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting ‘criminal offences’ generally.”

111. It did not consider access to the data which were the subject of the request to be a particularly serious interference because it:

“only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.”

4. Maximillian Schrems v. Data Protection Commissioner (*Case C-362/14; ECLI:EU:C:2015:650*)

112. This request for a preliminary ruling arose from a complaint against Facebook Ireland Ltd which was made to the Irish Data Protection Commissioner by Mr. Schrems, an Austrian privacy advocate. Mr. Schrems challenged the transfer of his data by Facebook Ireland to the United States and the retention of his data on servers located in that country. The Data Protection Commissioner rejected the complaint since, in a decision of 26 July 2000, the European Commission had considered that the United States ensured an adequate level of protection of the personal data transferred (“the Safe Harbour Decision”).

113. In its ruling of 6 October 2015, the CJEU held that the existence of a Commission decision finding that a third country ensured an adequate

level of protection of the personal data transferred could not eliminate or even reduce the powers available to the national supervisory authorities under the Charter or the Data Protection Directive. Therefore, even if the Commission had adopted a decision, the national supervisory authorities had to be able to examine, with complete independence, whether the transfer of a person's data to a third country complied with the requirements laid down by the Directive.

114. However, only the CJEU could declare a decision of the Commission invalid. In this regard, it noted that the safe harbour scheme was applicable solely to the United States' undertakings which adhered to it, and United States' public authorities were not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevailed over the safe harbour scheme, so that United States' undertakings were bound to disregard, without limitation, the protective rules laid down by the scheme where they conflicted with such requirements. The safe harbour scheme therefore enabled interference by United States' public authorities with the fundamental rights of individuals, and the Commission had not, in the Safe Harbour Decision, referred either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference.

115. As to whether the level of protection in the United States was essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the CJEU found that legislation was not limited to what was strictly necessary where it authorised, on a generalised basis, storage of all the personal data of all the persons whose data were transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of their subsequent use. Therefore, under EU law legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications had to be regarded as compromising the essence of the fundamental right to respect for private life. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromised the essence of the fundamental right to effective judicial protection.

116. Finally, the Court found that the Safe Harbour Decision denied the national supervisory authorities their powers where a person called into question whether the decision was compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Commission had not had competence to restrict the national supervisory

authorities' powers in that way and, consequently, the CJEU held the Safe Harbour Decision to be invalid.

5. Data Protection Commissioner v Facebook Ireland and Maximilian Schrems *Case (C-311/18; ECLI:EU:C:2020:559)*

117. Following the judgment of the CJEU of 6 October 2015, the referring court annulled the rejection of Mr Schrems' complaint and referred that decision back to the Commissioner. In the course of the Commissioner's investigation, Facebook Ireland explained that a large part of personal data were transferred to Facebook Inc. pursuant to the standard data protection clauses set out in the annex to Commission Decision 2010/87/EU, as amended.

118. Mr Schrems reformulated his complaint, claiming, *inter alia*, that the United States' law required Facebook Inc. to make the personal data transferred to it available to certain United States' authorities, such as the National Security Agency ("the NSA") and the Federal Bureau of Investigation. Since those data were used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, Decision 2010/87/EU could not justify the transfer of those data to the United States. On this basis, he asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.

119. In a draft decision published on 24 May 2016, the Commissioner took the provisional view that the personal data of European Union citizens transferred to the United States were likely to be consulted and processed by the United States' authorities in a manner incompatible with Articles 7 and 8 of the Charter and that United States' law did not provide those citizens with legal remedies compatible with Article 47 of the Charter. The Commissioner found that the standard data protection clauses in the annex to Decision 2010/87/EU were not capable of remedying that defect, since they did not bind the United States' authorities.

120. Having considered the United States' intelligence activities under section 702 of FISA and Executive Order 12333, the High Court concluded that the United States carried out mass processing of personal data without ensuring a level of protection essentially equivalent to that guaranteed by Articles 7 and 8 of the Charter; and that European Union citizens did not have available to them the same remedies as citizens of the United States, with the consequence that United States' law did not afford European Union citizens a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter. It stayed the proceedings and referred a number of questions to the CJEU for a preliminary ruling. It asked, *inter alia*, whether European Union law applied to the transfer of data from a private company in the European Union to a private company in a third country; if so, how the level of protection in the third country should be assessed; and whether

the level of protection afforded by the United States respected the essence of the rights guaranteed by Article 47 of the Charter.

121. In a judgment of 16 July 2020 the CJEU held that the General Data Protection Regulation (“GDPR”) applied to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, those data were liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security. Moreover, the appropriate safeguards, enforceable rights and effective legal remedies required by the GDPR had to ensure that data subjects whose personal data were transferred to a third country pursuant to standard data protection clauses were afforded a level of protection essentially equivalent to that guaranteed within the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer had to take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country.

122. Furthermore, unless there was a valid Commission adequacy decision, the competent supervisory authority was required to suspend or prohibit a transfer of data to a third country if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, the standard data protection clauses adopted by the Commission were not or could not be complied with in that third country and the protection of the data transferred (as required by European Union law) could not be ensured by other means.

123. In order for the Commission to adopt an adequacy decision, it had to find, duly stating reasons, that the third country concerned ensured, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the European Union legal order. In the CJEU’s view, the Safe Harbour decision was invalid. Section 702 of the Foreign Intelligence Security Act (“FISA”) did not indicate any limitations on the power it conferred to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances, it could not ensure a level of protection essentially equivalent to that guaranteed by the Charter. Furthermore, as regards the monitoring programmes based on Executive Order 12333, it was clear that that order also did not confer rights which were enforceable against the United States’ authorities in the courts.

6. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (Case C-623/17; ECLI:EU:C:2020:790) and La Quadrature du Net and Others, French Data Network and Others and Ordre des barreaux francophones et germanophone and Others (Cases C-511/18, C-512/18 and C-520/18; ECLI:EU:C:2020:791)*

124. On 8 September 2017 the United Kingdom Investigatory Powers Tribunal (“IPT”) gave judgment in the case of *Privacy International*, which concerned the acquisition by the intelligence services of bulk communications data under section 94 of the Telecommunications Act 1984 and bulk personal data. The IPT found that, following their avowal, the regimes were compliant with Article 8 of the Convention. However, it identified the following four requirements which appeared to flow from the CJEU judgment in *Watson and Others* and which seemed to go beyond the requirements of Article 8 of the Convention: a restriction on non-targeted access to bulk data; a need for prior authorisation (save in cases of validly established emergency) before data could be accessed; provision for subsequent notification of those affected; and the retention of all data within the European Union.

125. On 30 October 2017 the IPT made a request to the CJEU for a preliminary ruling clarifying the extent to which the *Watson* requirements could apply where the bulk acquisition and automated processing techniques were necessary to protect national security. In doing so, it expressed serious concern that if the *Watson* requirements were to apply to measures taken to safeguard national security, they would frustrate them and put the national security of Member States at risk. In particular, it noted the benefits of bulk acquisition in the context of national security; the risk that the need for prior authorisation could undermine the intelligence services’ ability to tackle the threat to national security; the danger and impracticality of implementing a requirement to give notice in respect of the acquisition or use of a bulk database, especially where national security was at stake; and the impact an absolute bar on the transfer of data outside the European Union could have on Member States’ treaty obligations.

126. A public hearing took place on 9 September 2019. The *Privacy International* case was heard together with cases C-511/18 and C-512/18, *La Quadrature du Net and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*, which also concerned the application of Directive 2002/58 to activities related to national security and the combating of terrorism. Thirteen States intervened in support of the States concerned.

127. Two separate judgments were handed down on 6 October 2020. In *Privacy International* the CJEU found that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence

agencies for the purpose of safeguarding national security fell within the scope of the Directive on privacy and electronic communications. The interpretation of that Directive had to take account of the right to privacy, guaranteed by Article 7 of the Charter, the right to protection of personal data, guaranteed by Article 8, and the right to freedom of expression, guaranteed by Article 11. Limitations on the exercise of those rights had to be provided for by law, respect the essence of the rights, and be proportionate, necessary, and genuinely meet the objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Furthermore, limitations on the protection of personal data must apply only in so far as is strictly necessary; and in order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be protected effectively against the risk of abuse.

128. In the opinion of the CJEU, national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission – which affected all persons using electronic communications services – exceeded the limits of what was strictly necessary and could not be considered to be justified as required by the Directive on privacy and electronic communications read in light of the Charter.

129. However, in *La Quadrature du Net and Others* the CJEU confirmed that while the Directive on privacy and electronic communications, read in light of the Charter, precluded legislative measures which provided for the general and indiscriminate retention of traffic and location data, where a Member State was facing a serious threat to national security that proved to be genuine and present or foreseeable, it did not preclude legislative measures requiring service providers to retain, generally and indiscriminately, traffic and location data for a period limited to what was strictly necessary, but which could be extended if the threat persisted. For the purposes of combating serious crime and preventing serious threats to public security, a Member State could also provide - if it was limited in time to what was strictly necessary - for the targeted retention of traffic and location data, on the basis of objective and non-discriminatory factors according to the categories of person concerned or using a geographical criterion, or of IP addresses assigned to the source of an Internet connection. It was also open to a Member State to carry out a general and indiscriminate retention of data relating to the civil identity of users of means of electronic communication, without the retention being subject to a specific time limit.

130. Furthermore, the Directive on privacy and electronic communications, read in light of the Charter, did not preclude national rules

which required providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection of traffic and location data, and secondly, to the real-time collection of technical data concerning the location of the terminal equipment used, where it was limited to situations in which a Member State was facing a serious threat to national security that was genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review by a court or independent administrative body whose decision was binding; and where recourse to the real-time collection of traffic and location data was limited to persons in respect of whom there was a valid reason to suspect that they were involved in terrorist activities and was subject to a prior review carried out either by a court or by an independent administrative body whose decision was binding.

IV. RELEVANT COMPARATIVE LAW AND PRACTICE

A. Contracting States

1. Overview

131. At least seven Contracting States (being Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways.

132 In one additional State (Norway) a draft law is being debated: if enacted, it will also authorise bulk interception.

133. The bulk interception regime in the United Kingdom is described in detail in the Court's judgment in the case of *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13 and 2 others, 25 May 2021).

134. As regards intelligence sharing agreements, at least thirty-nine Contracting States have either concluded intelligence sharing agreements with other States, or have the possibility for such agreements. Two expressly prohibit and two expressly permit the State to ask a foreign power to intercept material on their behalf. In the remaining States, the position on this issue is not clear.

135. Finally, in most States the applicable safeguards are broadly the same as for domestic operations, with various restrictions on the use of the received data and in some cases an obligation to destroy them if they became irrelevant.

2. Judgment of the German Federal Constitutional Court of 19 May 2020 (1 BvR 2835/17)

136. In this judgment, the Constitutional Court considered whether the Federal Intelligence Service's powers to conduct strategic (or "signals")

intelligence on foreign telecommunications were in breach of the fundamental rights contained in the Basic Law (Grundgesetz).

137. The regime in question involved the interception of both content and related communications data and aimed only to monitor foreign telecommunications outside of German territory. Such surveillance could be carried out for the purpose of gaining information about topics determined by the Federal Government's mandate to be significant for the State's foreign and security policy. It could, however, also be used to target specific individuals. The admissibility and necessity of the orders to conduct such surveillance was controlled by an Independent Panel. According to the Constitutional Court's judgment, interception was followed by a multi-stage, fully automated filtering and evaluation process. For this purpose, the Federal Intelligence Service used a six-digit number of search terms which were subject to control by an internal sub-unit responsible for ensuring that the link between the search terms employed and the purpose of the data request was explained in a reasonable and comprehensive manner. After the application of the automated filtering process, intercepted material was either deleted or stored and sent for evaluation by an analyst.

138. The sharing of intercept material with foreign intelligence services was accompanied by a cooperation agreement which had to include usage restrictions and assurances to ensure that data were handled and deleted in accordance with the rule of law.

139. The Constitutional Court held that the regime in question was not compliant with the Basic Law. While it acknowledged the overriding public interest in effective foreign intelligence gathering, it nevertheless considered, *inter alia*, that the regime was not restricted to sufficiently specific purposes; that it was not structured in a way that allowed for adequate oversight and control; and that various safeguards were lacking, particularly with respect to the protection of journalists, lawyers and other persons whose communications required special confidentiality protection.

140. Regarding the sharing of intelligence obtained through foreign surveillance, the court again found the safeguards to be lacking. In particular, it was not specified with sufficient clarity when weighty interests might justify data transfers. In addition, while the court did not consider it necessary for a recipient State to have comparable rules on the processing of personal data, it nevertheless considered that data could only be transferred abroad if there was an adequate level of data protection and there was no reason to fear that the information would be used to violate fundamental principles of the rule of law. More generally, in the context of intelligence sharing, the court considered that cooperation with foreign States should not be used to undermine domestic safeguards and if the Federal Intelligence Service wished to use search terms provided to it by a foreign intelligence service it should first confirm the existence of the necessary link between the search terms and the purpose of the data request and that the resulting

data did not disclose a particular need for confidentiality (for example, because they concerned whistle-blowers or dissidents). Although the court did not exclude the possibility of the bulk transfer of data to foreign intelligence services, it found that this could not be a continuous process based on a single purpose.

141. Finally, the court found that the surveillance powers under review also lacked an extensive independent and continual oversight serving to ensure that the law was observed and compensating for the virtual absence of safeguards commonly guaranteed under the rule of law. The legislator had to provide for two different types of oversight, which had also to be reflected in the organisational framework: firstly, a body resembling a court, tasked with conducting oversight and deciding in a formal procedure providing *ex ante* or *ex post* legal protection; and secondly, an oversight that was administrative in nature and could, on its own initiative, randomly scrutinise the entire process of strategic surveillance as to its lawfulness. In the Constitutional Court's view, certain key procedural steps would, in principle, require *ex ante* authorisation by a body resembling a court, namely: the formal determination of the various surveillance measures (exemptions in cases of urgency were not ruled out); the use of search terms, insofar as these directly targeted individuals who might pose a danger and were thus of direct interest to the Federal Intelligence Service; the use of search terms that directly targeted individuals whose communications required special confidentiality protection; and sharing the data of journalists, lawyers and other professions meriting special confidentiality protection with foreign intelligence services.

B. The United States of America

142. The United States' intelligence services operate the Upstream programme pursuant to section 702 of the Foreign Intelligence Surveillance Act ("FISA").

143. The Attorney General and Director of National Intelligence make annual certifications authorising surveillance targeting non-U.S. persons reasonably believed to be located outside the U.S. They do not have to specify to the Foreign Intelligence Surveillance Court ("FISC") the particular non-U.S. persons to be targeted, and there is no requirement to demonstrate probable cause to believe that an individual targeted is an agent of a foreign power. Instead, the section 702 certifications identify categories of information to be collected, which have to meet the statutory definition of foreign intelligence information. Authorised certifications have included information concerning international terrorism, and the acquisition of weapons of mass destruction.

144. Pursuant to the authorisation, the NSA, with the compelled assistance of service providers, copies and searches streams of Internet

traffic as data flows across the Internet. Both telephone calls and Internet communications are collected. Prior to April 2017 the NSA acquired Internet transactions that were “to”, “from”, or “about” a tasked selector. A “to” or “from” communication was a communication for which the sender or a recipient was a user of a section 702 tasked selector. An “about” communication was one in which the tasked selector was referenced within the acquired Internet transaction, but the target was not necessarily a participant in the communication. Collection of “about” communications therefore involved searching the content of communications traversing the Internet. However, from April 2017 onwards the NSA have not been acquiring or collecting communications that are merely “about” a target. In addition the NSA stated that, as part of this curtailment, it would delete the vast majority of previously acquired Upstream Internet communications as soon as practicable.

145. Section 702 requires the Government to develop targeting and minimization procedures which are kept under review by the FISC.

146. Executive Order 12333, which was signed in 1981, authorises the collection, retention and dissemination of information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation. Surveillance of foreign nationals under Executive Order 12333 is not subject to domestic regulation under FISA. It is not known how much data are collected under Executive Order 12333, relative to those collected under section 702.

THE LAW

I. PRELIMINARY ISSUE: DATE OF ASSESSMENT

147. Before the Chamber the applicant sought a ruling on the Convention compatibility of the relevant Swedish legislation as it applied during three distinct periods (see paragraph 82 of the Chamber judgment). The Chamber decided to focus on the Swedish legislation as it stood at the time of its examination of the case (see paragraphs 96-98 of the Chamber judgment).

148. Before the Grand Chamber, the applicant did not reiterate its request concerning the three periods but relied in its submissions on, *inter alia*, developments from 2018 and 2019 post-dating the Chamber’s examination of the case.

149. The Government considered that, having regard to the Court’s case law according to which “the content and scope of the “case” referred to the Grand Chamber are ... delimited by the Chamber’s decision on admissibility”, the Grand Chamber’s review should be limited to the Swedish legislation as it stood at the time of the Chamber’s examination.

150. The Grand Chamber agrees with the Chamber that it cannot be the Court's task, when reviewing the relevant law *in abstracto*, as in the present case, to examine compatibility with the Convention before and after every single legislative amendment.

151. The temporal scope of the Grand Chamber's examination is therefore limited to the Swedish law and practice as it stood in May 2018, at the time of the Chamber examination.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

152. The applicant complained that the relevant legislation and practice in Sweden on bulk interception of communications, also referred to as signals intelligence, were in violation of its right to respect for private life and correspondence protected by Article 8 of the Convention. The Government contested that argument.

153. Article 8 of the Convention reads as follows:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

A. The Government's preliminary objection on victim status

1. *The Chamber judgment*

154. Applying the criteria set out in *Roman Zakharov v. Russia* ([GC], no. 47143/06, ECHR 2015), and *Kennedy v. the United Kingdom* (no. 26839/05, 18 May 2010), the Chamber considered that the contested legislation on signals intelligence instituted a system of secret surveillance that potentially affected all users and that no domestic remedy provided detailed grounds in response to a complainant who suspects that he or she has had his or her communications intercepted. In these circumstances, the Chamber considered an examination of the relevant legislation *in abstracto* to be justified and concluded that the applicant could claim to be the victim of a violation of the Convention, even though it was unable to allege that it had been subjected to a concrete measure of interception. For the same reasons the Chamber concluded that the mere existence of the contested legislation amounted in itself to an interference with the applicant's rights under Article 8.

2. The parties' submissions before the Grand Chamber

(a) The Government

155. The Government stated that the applicant did not belong to a “group of persons or entities targeted by the legislation” on signals intelligence within foreign intelligence.

156. In the Government’s view, furthermore, the contested legislation did not directly affect all users of mobile telephone services and the internet since it was restricted to foreign intelligence, and thereby foreign circumstances.

157. Referring to the six stages of signals intelligence activities as described by them (see paragraph 29 above), the Government claimed that the applicant’s telephone and internet communications were unlikely to be affected for the following reasons: the majority of purely domestic communications would not pass the hand-over points in cross-border cables; even if that happened, the selectors used to identify relevant signals are designed with great precision as regards targeted foreign phenomena and the selectors are subject to approval by the Foreign Intelligence Court; as a result of the above, the applicant’s communications are unlikely to be sifted out in the above automatic processing; any data passing through the communications bearers that has not been selected disappears without any possibility to be reproduced and examined by the FRA; even if the applicant’s data or communications reached the third stage in the bulk interception process, there will be then further refining through automatic and manual means and the risk of the applicant’s communication being retained for further scrutiny beyond that stage is virtually non-existent.

158. In the Government’s view, there is no interference with Article 8 rights until the stage when an analytical examination of selected signals is possible.

159. The Government were also of the view that Swedish law affords effective remedies for a person who suspects that he or she was subjected to signals interception measures, including the possibility to file a request with the Foreign Intelligence Inspectorate and, as a result, obtain a notification whether or not any improper data collection has taken place. In the Government’s view, the Chamber’s insistence that there should be, in addition to the above, “detailed grounds” given in response, was not based on earlier case-law and unduly expanded the relevant requirements.

160. On this basis the Government considered that the applicant might only claim to be a victim of a violation occasioned by the mere existence of impugned legislation if it was able to show that, due to its “personal” situation, it was potentially at risk of being subjected to signals intelligence measures. That was far from being so. Quite to the contrary, the applicant’s telephone and internet communications were unlikely to be intercepted and

sifted and, in any event, the risk that they would be retained for further scrutiny beyond the automatic processing stage was virtually non-existent.

161. The Government thus requested the Grand Chamber to declare the application inadmissible for lack of victim status or to find that there was no interference with the applicant's Article 8 rights.

162. As to other admissibility issues, the Government stated that they did not have objections regarding the exhaustion of domestic remedies.

(b) The applicant

163. The applicant considered that the relevant two conditions for claiming victim status in applications concerning the very existence of a legal regime for secret surveillance, as enunciated in *Roman Zakharov* (cited above), were satisfied in the present case.

164. In particular, the Signals Intelligence Act permits the interception of any communications travelling along the cables that cross the Swedish border, or that are transmitted via the airways, and therefore, according to the applicant, directly affects all users of such communication services. Even though only communications relating to foreign circumstances are allowed to be intercepted, virtually all users of communications services may engage in cross-border communications, either deliberately by contacting a foreign recipient or inadvertently through communicating via a server located abroad. Also, the Signals Intelligence Act permits interception for development purposes unrelated to foreign circumstances.

165. The applicant also submitted that there is no effective remedy at the national level for the applicant or for anyone suspecting that they may have been subject to bulk interception by the Swedish authorities. Therefore, the applicant must be able to have its case examined by the Court and can claim that the very existence of the impugned regime amounts to an interference with its Article 8 rights.

3. The Court's assessment

166. As the Court noted in *Kennedy* and *Roman Zakharov* (both cited above), in cases concerning secret measures, there are special reasons justifying the Court's departure from its general approach, according to which individuals cannot challenge before it a domestic law *in abstracto*. The principal reason is to ensure that the secrecy of surveillance measures should not result in them being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court (see *Roman Zakharov*, cited above, § 169).

167. It is now settled case-law that several criteria apply in assessing whether an applicant may claim to be the victim of a violation of his or her Convention rights allegedly occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance

measures. Those criteria were formulated as follows in *Roman Zakharov* (cited above, § 171):

“Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his communications intercepted.

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

By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.”

168. Applying those criteria to the present case, the Court agrees with the Government that the applicant does not belong to a group of persons or entities targeted by the Swedish signal intelligence legislation and measures. Indeed, the applicant has not made such a claim.

169. It must be seen, therefore, whether, as alleged by the applicant, the impugned legislation institutes a system of secret surveillance that potentially affects all persons communicating over the telephone or using the internet.

170. In this regard, it is clear that communications or communications data of any person or entity in Sweden may happen to be transmitted via intercepted communications bearers and may thus be subject to at least the initial stages of automatic processing by the FRA under the contested legislation.

171. The Government’s arguments that signals intelligence is restricted to foreign threats and circumstances and that therefore there is virtually no risk of the applicant’s communications being retained for further scrutiny beyond the automatic processing stage in bulk interception are relevant in the assessment of the intensity and proportionality of the interference with Article 8 rights, including the safeguards built into the impugned signals interception regime, but are not decisive with regard to the applicant’s

victim status under Article 34 of the Convention. Any other approach risks rendering the access to the Convention complaints' procedure conditional on proving that one's communications are of interest for agencies tasked with foreign intelligence – an almost impossible task, having regard to the secrecy inherent in foreign intelligence activities.

172. In these circumstances, the Court must have regard to the remedies available in Sweden to persons who suspect that they were subjected to measures under the Signals Intelligence Act in order to assess whether, as maintained by the applicant, the threat of surveillance can be claimed in itself to restrict free communication, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8.

173. In this regard, the Court observes that, in practice, persons affected by bulk interception activities do not receive notification. On the other hand, in reaction to a request by anyone, regardless of nationality and residence, the Foreign Intelligence Inspectorate must investigate if the person's communications have been intercepted through signals intelligence and, if so, verify whether the interception and treatment of the information have been in accordance with law. The Inspectorate has the power to decide that the signals intelligence operation shall cease or that the intelligence shall be destroyed. Any person may also seek the involvement of the Parliamentary Ombudsmen and the Chancellor of Justice in a number of circumstances.

174. The applicant alleged, however, that the only information that might be given by the Inspectorate, without any reasons for the conclusions reached and in the form of a final decision not amenable to appeal, was that there had been an unlawful action. No other remedy could result in the complainant obtaining additional information on the circumstances of a possible interception and use of his or her communications or related data or about the nature of the unlawful action, if it occurred.

175. In the context of the issue of victim status, without prejudice to the conclusions to be drawn in respect of the substantive requirements of Article 8 § 2 and Article 13 in the present case, the Court notes that the domestic remedies available in Sweden to persons who suspect that they are affected by bulk interception measures are subject to a number of limitations. In the Court's view, even if these limitations are to be considered inevitable or justified, the practical result is that the availability of remedies cannot sufficiently dispel the public's fears related to the threat of secret surveillance.

176. It follows that it is not necessary to examine whether the applicant, due to its personal situation, is potentially at risk of seeing its communications or related data intercepted and analysed.

177. On the basis of the above considerations the Court finds that an examination of the relevant legislation *in abstracto* is justified. The Government's objection that the applicant may not claim to be the victim of a violation of his or her Convention rights allegedly occasioned by the mere

existence of Swedish bulk interception legislation and activities is therefore rejected.

B. Merits

1. The Chamber judgment

178. The Chamber found that the surveillance system clearly had a basis in domestic law and was justified by national security interests. Indeed, given the present-day threats of global terrorism and serious cross-border crime, as well as the increased sophistication of communications technology, the Court held that Sweden had considerable power of discretion (“a wide margin of appreciation”) to decide on setting up such a system of bulk interception. The State’s discretion in actually operating such an interception system was narrower, however, and the Court had to be satisfied that there were adequate and effective guarantees against abuse. It assessed the minimum safeguards to avoid abuse of power, as developed in its case-law and, in particular, in *Roman Zakharov* (cited above; see paragraphs 99-115 of the Chamber judgment).

179. Overall, while the Chamber found some areas where there was scope for improvement of the system, notably the regulation of the communication of personal data to other States and international organisations and the practice of not giving public reasons following a review of individual complaints (see paragraphs 150, 173 and 177 of the Chamber judgment), it considered that the system revealed no significant shortcomings in its structure and operation. In this context, it noted that the regulatory framework had been reviewed several times with a view to enhancing protection of privacy and that it had in effect developed in such a way that it minimised the risk of interference with privacy and compensated for the lack of openness of the system (see paragraphs 180 and 181 of the Chamber judgment).

180. More specifically, the scope of the interception and the treatment of intercepted data were clearly defined in law; the duration of the measures were clearly regulated (any permit was valid for a maximum of six months and renewal required a new review); the authorisation procedure was detailed and entrusted to a judicial body, the Foreign Intelligence Court; there were several independent bodies, in particular the Foreign Intelligence Inspectorate and the Data Protection Authority, tasked with the supervision and review of the system; and, on request, the Inspectorate had to investigate individual complaints of intercepted communications, as did the Parliamentary Ombudsmen and the Chancellor of Justice (see paragraphs 116-47 and 153-78 of the Chamber judgment).

181. The Chamber therefore found that the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. The relevant legislation met the “quality

of law” requirement and the interference could be considered as being “necessary in a democratic society”. Furthermore, the structure and operation of the system were proportionate to the aim sought to be achieved. The Chamber pointed out, however, that its examination had been made *in abstracto* and did not preclude a review of the State’s liability under the Convention where, for example, the applicant has been made aware of an actual interception (see paragraphs 179-81 of the Chamber judgment).

2. *The parties’ submissions*

(a) **The applicant**

(i) *The applicant’s view on the standard to be applied*

182. According to the applicant, bulk interception regimes are inherently incompatible with the Convention. In *Klass and Others v. Germany* (6 September 1978, § 51, Series A no. 28) and *Association “21 December 1989” and Others v. Romania* (nos. 33810/07 and 18817/08, §§ 174-75, 24 May 2011), the Court had considered “exploratory” or “general surveillance” as problematic. As regards untargeted interception, solely regimes far more confined in scope than the Swedish regime had been found to be compatible with the Convention. Seeing that FRA could gain access to virtually all cable-based communications crossing the Swedish border, the amount of intimate, private and privileged data that could be surveyed under the Swedish signals intelligence regime was far greater. Therefore, the applicant considered that only targeted and smaller-scale untargeted interception regimes could fall within the State’s margin of appreciation. Any other approach risked leading to inconsistent case-law having regard to the Court’s approach to other Convention issues, such as blanket retention of fingerprints and DNA profiles, dealt with in *S. and Marper v. the United Kingdom* ([GC], nos. 30562/04 and 30566/04, § 115, ECHR 2008).

183. If the Court considered that bulk interception activities may be justified under the Convention, the applicant submitted that robust minimum safeguards were imperative. The factors outlined in *Roman Zakharov* (cited above, § 238) could serve as an initial framework, but untargeted surveillance entailed elevated privacy risks and required these standards to be adapted.

184. In particular, the main elements of the regime should be set out in sufficient detail in statute law. That would ensure that it is the representative of the people who strike the balance between the competing interests.

185. As regards prior authorisation, while it accepted that the body entrusted with this task in Sweden is a judicial one, the applicant invited the Court to move one step further in its case-law and hold that prior authorisation must always be judicial.

186. In addition, in the applicant's view, the authorising body should be capable of verifying the existence of a reasonable suspicion in relation to any person singled out or targeted. The applicant found unconvincing the Chamber's departure, in the present case and in *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13 and 2 others, 13 September 2018, from this allegedly established requirement. The use of personalised selectors to single out and collect data on an individual, albeit in the bulk interception context, should be subject to the same threshold as applied to targeted interception. Otherwise, such selectors can be used as a work-around method for targeting individuals.

187. If there are no predefined targets, on the other hand, the authorising body should be capable of verifying that personal data is used in selectors only to the extent that it is material to a narrowly specified foreign intelligence objective. The latter is necessary because the use of selectors relating to specific individuals exposes them to distinct privacy risks, including about intimate matters and opinions.

188. In the applicant's view, furthermore, the authorising judicial body should be provided with an indication of how the data will be analysed and used (for example, via pattern-based or subject-based analysis, and whether profiles of individuals will be compiled).

189. As regards supervision at the stages of carrying out the surveillance activities and after they have been terminated, the applicant accepted that the Swedish oversight bodies meet the requirement of sufficient independence from the executive.

190. However, the oversight body must be vested with sufficient powers to issue legally binding decisions, including stopping and remedying breaches and seeking the liability of those responsible for such breaches. It should have access to classified documents and its functioning should be open to public scrutiny. The supervision powers should concern both content and communications data and should be exercised at the stages when collected communications are subject to automated computer analysis, where a human analyst works on them and where information is communicated to national authorities, foreign Governments or international organisations. Storage of data at each stage should also be supervised.

191. In the applicant's view, in addition, individuals must dispose of effective remedies which may take three forms: post-fact notification of the subject of surveillance, a possibility to request information about the surveillance or the existence of a body that can examine complaints without requiring the individual to submit evidence.

192. As regards transmitting intercepted material to foreign actors, the applicant underlined that Contracting States do not have unfettered discretion as they cannot outsource data processing and analysis in such a manner as to avoid responsibility under the Convention. The applicant considered that the minimum standards must include accessible legal

provisions, clear legal conditions for sharing, including a duty to take reasonable steps to ensure that the receiving party protects the data with similar safeguards as those applicable at home and sufficient supervisory and remedial mechanisms.

(ii) The applicant's analysis of the impugned Swedish regime

193. Applying these standards to the impugned Swedish regime, the applicant stated that the general scope of application of the FRA's powers is sufficiently constrained with the exception of the wide discretion it enjoys regarding its development activities. However, the applicant expressed concern that since 1 January 2013 the Security Police and the National Operative Department of the Police Authority (the "NOA") had been empowered to issue tasking directives for signals intelligence, and that as of 1 March 2018, the Security Police might be granted direct access to the FRA's databases with analysis material. The risk of signals intelligence being used outside the scope of foreign intelligence activities must be sufficiently contained by clear legal provisions and effective supervision.

194. The applicant also alleged that while warrants under the Swedish Signals Intelligence Act have a clear expiry date, there is no requirement that a warrant must be cancelled if collection of communication under the warrant ceases to be necessary.

195. The applicant further considered that the scope of judicial review by the authorising body in Sweden, the Foreign Intelligence Court, was too narrow to be effective. In particular, the existence of a reasonable suspicion in relation to a person who is singled out is not verified and the "exceptional importance" criterion, justifying selectors relating directly to an individual, only refers to selectors employed in the automated collection of data, not to the stage when the collected data is further searched. Also, the Foreign Intelligence Court is not required to review the intended subsequent use of the collected data and, indeed, the warrant request does not specify how the data will be analysed – for example, via subject-based data mining or through compilation of profiles of individuals.

196. As regards storing, accessing, examining, using and destroying intercepted data, the applicant identified two major flaws in the Swedish system: lack of legal obligation for the FRA to keep detailed records of the interception, use and communication of data, for which it had been repeatedly criticised by the Swedish Data Protection Authority, and lack of rules specifically adapted to bulk interception as opposed to general rules on data processing. The applicant was further concerned that as of 1 March 2018 the Security Police may be granted direct access to FRA's databases with analysis material.

197. The applicant also alleged that legal persons did not enjoy adequate protection since the FRA Data Processing Act only applies to intercept material containing personal data. This allegedly resulted in a situation

where material not containing personal data may be kept forever and used for purposes incompatible with the original purpose of collection.

198. The applicant criticised the following features of the existing supervision system. First, while the Inspectorate may decide that an operation shall cease or that the collected intelligence must be destroyed if it finds incompatibility with a warrant granted by the Foreign Intelligence Court, it does not have the power to issue binding decisions where the warrant is deemed unlawful. The Inspectorate cannot grant compensation or seek the liability of those responsible for breaches. Second, neither the Data Protection Authority, nor the Chancellor of Justice or the Ombudsmen may issue legally binding decisions. The Data Protection Authority may only apply to the Administrative Court in Stockholm to have illegally processed data destroyed. Furthermore, none of the complaints that have been submitted to the Chancellor and the Ombudsmen in relation to the FRA's activities has been successful. Those bodies are not specialised in the FRA's activities and do not possess the knowledge and capacity to supervise them effectively.

199. The applicant made the following submissions as regards the remedies available under the impugned Swedish regime.

First, in its view the notification provided for under section 11(a) of the Signals Intelligence Act only concerns natural persons, not organisations, and may be disapplied if required for reasons of secrecy, which has happened invariably in practice. This remedy was therefore "theoretical and illusory". The possibility to request the FRA to inform an individual whether personal data concerning him or her had been processed was also subject to the secrecy rule and the Administrative Court that examines ensuing appeals would not have access to secret documents and would be unable to review the FRA's assessment on whether secrecy applies. This remedy too is unavailable to legal persons as the applicant.

Second, the applicant referred to powers of the IPT in the United Kingdom to hear complaints of unlawful interception without the need for the complainant to prove that they had been subject to surveillance. The IPT, an independent judicial body, had access to secret documents, could take binding decisions and award compensation. Its decisions were published. The applicant submitted that a similar remedy was lacking in Sweden.

Third, as regards the possibility under Swedish law to ask the Inspectorate to investigate whether an individual's communications have been intercepted, the applicant noted that the Inspectorate did not inform the individual concerned of its findings and only sent standardised replies that no unlawful surveillance had taken place. The applicant reiterated their view that the Inspectorate had no power to control compliance with the law and the Constitution and could not order the payment of compensation.

Fourth, the applicant considered that seeking compensation from the Chancellor of Justice was not an effective remedy because: (i) the individual bears the burden to prove that there had been unlawful surveillance; (ii) compensation without erasing the unlawfully processed data could not be regarded as an effective remedy; (iii) to date the Chancellor, who enjoys discretion as to which complaints to review, had dismissed all complaints concerning the FRA's activities; (iv) the Government had not shown the effectiveness of this remedy, seeing that it is unclear what action must be undertaken by the Chancellor upon receipt of a report from the Inspectorate informing about actions of the FRA that may give rise to a claim of damages: in particular, if the Chancellor were to provide the individual with an opportunity to claim damages, that would require advising him or her of the unlawful conduct of the FRA which could be precluded by secrecy.

Fifth, in the absence of notification or access to documents it is virtually impossible for an individual to discharge the burden of proof in a civil action for damages.

Sixth, the Ombudsmen could not order any redress and no examples of the effectiveness of this remedy have been shown.

Seventh, the procedure according to which the FRA could correct or destroy unlawfully processed personal data was dependent on the individual's knowledge that data had been processed and was ineffective due to the secrecy requirement. Also, the Administrative Court has never received applications from the Data Protection Authority seeking the erasure of unlawfully processed data.

Finally, the possibility to seek prosecution was also dependent on the individual knowing of relevant wrongdoing and thus ineffective.

200. On the issue of transfers of intercepted data to foreign third parties, the applicant submitted that the deficiencies in the Swedish legal regime and practice were glaring. The legal limitations on such transfers consisted of nothing more than a vague and broadly defined obligation to act in the national interest. There was no requirement that possible harm to the individual is to be taken into account or that the recipient is to be required to protect the data with similar safeguards as those applicable in Sweden.

201. The applicant disagreed with the finding of the Chamber that the above shortcomings were counterbalanced by the supervisory mechanisms of the Swedish system. It considered that this supervision was inadequate and in any event did not cover the transfer of intercepted data to foreign parties. The FRA was merely required to inform the Inspectorate of the principles governing its cooperation with foreign parties, identify the countries or international organisations to which data was transferred and provide general details of operations. As the Inspectorate monitors the FRA's activities for compliance with existing legal requirements and the law allows excessive discretion to the FRA in this area, even the most stringent policing by the Inspectorate could do little to provide safeguards

against abuse. In the applicant's view, the arrangements described above cannot constitute a practice compatible with the Convention as they allow to simply outsource otherwise unlawful activities without appropriate limits safeguarding fundamental rights.

(b) The Government

202. The Government submitted that the purpose of signals intelligence was to obtain information and identify phenomena of relevance for foreign intelligence. Foreign intelligence was essential for Sweden's national security and also relevant with regard to Sweden's positive obligations under the Convention to protect the lives and safety of the public.

203. In the Government's view, owing to the fact that the Court's case-law setting out minimum safeguards for secret surveillance measures concerns, with the exception of the present case and *Big Brother Watch*, criminal investigations, some of the minimum safeguards required by the Court presuppose a link to a certain individual or to a certain place. This is very different from signals intelligence, which cannot be used to investigate criminal offences and one of the duties of the Foreign Intelligence Court is to ensure that it is not so used. Signals intelligence as part of foreign intelligence may in many cases target specific individuals' communications but the individuals are most often not of interest *per se*: they are only carriers of information.

204. It was necessary, therefore, to adapt the relevant requirements, including by reformulating some of the criteria set out in the Court's case-law as follows: introducing the criterion "the circumstances in which the measures may be used" instead of "the nature of the offences" and "categories of persons targeted". Also, account must be taken of the fact that national security threats are by their nature variable and difficult to define in advance.

205. The Government strongly disagreed with the applicant who had claimed, on the basis of *Roman Zakharov* (cited above) and *Szabó and Vissy v. Hungary* (no. 37138/14, 12 January 2016), that the existence of a reasonable suspicion was required at least when selectors linked to a specific individual were used. In the Government's view no such requirement could be deducted from the above-cited case-law. The Government supported the Chamber's reasoning in paragraph 317 in *Big Brother Watch*, where the Court held that the requirements of "reasonable suspicion" and "subsequent notification" are incompatible with bulk interception regimes.

206. The Government further asserted that bulk interception in Sweden was regulated by a comprehensive legal regime that was based on published legal provisions and provided for significant safeguards, including independent supervision, covering both surveillance activities related to communications data and to the content of communications. The law clearly

delimited the scope of the surveillance activities, the mandate given to the competent authorities in this regard and the manner of its exercise.

207. As regards the FRA's development activities, the Government emphasised that they are rigorously regulated and subject to all substantive and procedural requirements applicable to signals intelligence in general. In development activities, which are crucial to permit the FRA to adjust its tools, systems and methods to an ever-changing signals environment and technical developments, it is the flow of traffic and the systems through which information is transmitted that are of interest. To maintain the FRA's capabilities, it would be far too restrictive if development activities were only allowed for the eight purposes that circumscribe signals intelligence.

208. There was, furthermore, a prior authorisation procedure before the Foreign Intelligence Court, whose president is a permanent judge and the other members are appointed by the Government on four-year terms. In the exceptional cases of urgency when the FRA may itself grant a signals intelligence permit, that court must be immediately notified and it may modify or revoke the permit, with the consequence that collected data must be destroyed. If the permit granted by the FRA, not by the court, contains access to certain communications bearers, such access can only be realised by the Swedish Foreign Intelligence Inspectorate which will have the possibility to estimate the relevant legal aspects.

209. The Foreign Intelligence Court holds public hearings except when required by secrecy considerations. The Government submitted that the latter limitation on transparency was justified and was compensated by safeguards, such as the presence of a privacy protection representative at the court's private hearings. The representative defends the public interest, is given full access to case documents and can make statements. He or she is a permanent judge or a former permanent judge or a member of the Swedish Bar Association.

210. The Government emphasised that the FRA must seek a permit in respect of each mission and must specify the assignment, the bearers to which access is sought and the selectors or at least the categories of selectors to be used. The court examines not only the formal lawfulness but also the proportionality to the expected interference. The permit must specify all parameters, including the conditions needed to limit such interference.

211. As regards safeguards on the duration of the interception, Swedish law limited it to six months, subject to extension following full review by the Foreign Intelligence Court. Also, interception is discontinued if a tasking directive is revoked or expires, if interception is not in accordance with the permit and if it is no longer needed.

212. Adequate safeguards also exist in respect of the procedures for storing, accessing, examining, using and destroying intercepted data. These safeguards include limiting processing to what is adequate and relevant to

its purpose, vetting of staff and their duty of confidentiality and sanctions in case of mismanagement of data. Also, intelligence must be destroyed immediately in a number of circumstances, including, *inter alia*, where it concerns constitutionally protected media sources or legal professional privilege in relations between a criminal suspect and his lawyer. Moreover, if the intercepted communications prove to be entirely domestic, the intercepted data must also be destroyed.

213. As regards the conditions for communicating the intercepted data to other parties, the FRA has a regulated obligation to report to the Swedish authorities concerned but ensures that personal data is only reported if it is of relevance for the purposes for which foreign intelligence may be conducted. Compliance with this requirement is monitored by the Foreign Intelligence Inspectorate.

214. The Government emphasised that despite the provision allowing the FRA to give direct access to its completed intelligence reports to the Government Offices, the Armed Forces, the Security Police and three other bodies, no decisions permitting such access have yet been taken by the FRA. The Government clarified in addition that, since 1 March 2018, under section 15 of the FRA Personal Data Protection Act, the Security Police and the Armed Forces may be granted direct access to data that constitutes the analysis results in a data compilation for analyses, so as to allow these two authorities to be able to make strategic assessments of terrorist threats. This changes nothing with regard to the prohibition to use signals intelligence within foreign intelligence for the purposes of investigating criminal offences.

215. Finally, with regard to communication of personal data to other States and to international organisations, the Government disagreed with the Chamber which had found shortcomings in the relevant legal regime (see paragraph 150 of the Chamber judgment). They submitted, *inter alia*, that the FRA must report to the Ministry of Defence before it establishes and maintains cooperation with other states and international organisations and inform the ministry about important issues that occur in the process of such cooperation. Furthermore, the FRA must inform the Swedish Foreign Intelligence Inspectorate of the principles that apply to its relevant cooperation and provide details of the countries and organisations with which such cooperation takes place. When cooperation is established, the FRA must inform the Inspectorate of the scope of the cooperation and, where deemed warranted, of the results, experience and continued direction of the cooperation.

216. The Government also pointed to the fact that in international cooperation data is exclusively communicated to parties that are themselves engaged in foreign intelligence, which meant that it is in the recipient's interest to protect the data received. The trust between the parties is based on a mutual interest in maintaining the security of the data. Also, the FRA's

general guidelines stipulate that international cooperation is conditional on the receiving State respecting Swedish legislation. Foreign partners receive information and training on the relevant content of Swedish legislation. As the Inspectorate has a clear mandate to control the FRA's international cooperation, any change to its internal guidelines would not go unnoticed. There are therefore clear safeguards against circumventing Swedish law.

217. In the Government's view, Sweden's system of supervision on signals intelligence offered important safeguards. The Foreign Intelligence Inspectorate is independent, has access to all relevant documents, examines the selectors used and has the power to decide that data collection must cease or the data collected be destroyed if the terms of the relevant permit have not been complied with. The Inspectorate also ensures that the FRA is only provided access to communications bearers insofar as such access is covered by a permit. The Inspectorate submits annual public reports and is subject to audit by the National Audit Office and supervision by the Parliamentary Ombudsmen and the Chancellor of Justice. As regards personal data, the Swedish Data Protection Authority has general supervisory functions. In the Government's view, this kind of supervision by independent non-judicial bodies is adequate and in conformity with the Court's case-law.

218. The Government submitted that between 2009 and 2018 the Inspectorate had conducted 113 audits of the FRA resulting in 18 opinions. At least seventeen of these audits served, *inter alia*, to control that the FRA was using selectors in a way compatible with the permit issued by the Foreign Intelligence Court and at least nine audits included issues of data destruction. A number of audits also concerned the FRA's handling of personal data. Only very few observations or opinions ensued from the audits. During the same time period, the Inspectorate carried out 141 controls at the request of an individual on whether his or her communications had been the subject of unlawful signals intelligence. None of those showed improper signals collection. There were also several thematic reviews of the FRA's activities, such as on compliance with the limits imposed by the permits.

219. The Government also submitted that there are several remedies by which an individual may initiate an examination of the lawfulness of measures taken during the operation of the signals intelligence system. These include a request to the Inspectorate which may result in notification whether anything improper had taken place, a request to the FRA on whether personal data concerning him or her has been processed, applications to the Parliamentary Ombudsmen, the Chancellor of Justice and the Data Protection Authority, an action for damages and reporting a matter for prosecution. Some of these remedies are not dependent on prior notification being made to an individual. While systematic notification was impossible, it is significant that the FRA is obliged to inform a natural

person if selectors directly related to him or her have been used, except where secrecy applies.

220. The Government also stated that no distinction is made in Swedish law on bulk interception between content and communications data, all safeguards applying equally to both. In practice, using communications data to discover unknown threats requires putting together various pieces of such data to establish a picture from which conclusions can be drawn. This requires that the selectors used for intercepting communications data are less specific than those used for the content of communications and that data is available for examination by an analyst over a period of time. No other differences exist.

221. In conclusion, the Government submitted that the impugned regime on signals intelligence within foreign intelligence reveals no significant shortcomings in its structure and operation. The risk of interference with privacy is minimised and sufficient guarantees against arbitrariness are in place. The regime as a whole is lawful and proportionate to the legitimate aim of protecting national security.

3. Third intervening parties

(a) The Government of the Republic of Estonia

222. The Estonian Government considered that the criteria for the assessment of the Convention compatibility of secret surveillance regimes, as developed in the Court's case-law, needed adaptation to reflect the specific nature of bulk interception of communications as a foreign intelligence activity. The differences between such an activity and surveillance in the criminal investigation context must be taken into account. Foreign intelligence aims at detecting threats to national security and is therefore broader in its scope. Also, it is a long-term activity that requires a higher level of secrecy over a very long period of time.

223. On this basis, the Estonian Government, referring to the criteria for assessment used in *Roman Zakharov* (cited above, § 231), agreed with the Chamber that the "nature of the offences" and "reasonable suspicion" criteria were not appropriate and stated that, instead of the "categories of people" criterion, domestic law should indicate "the fields in which bulk interception of cross-border communications may be used to gather intelligence". As to notification of affected persons, in the view of the intervening Estonian Government no such obligation should be imposed because of the importance of secrecy in foreign intelligence.

(b) The Government of the French Republic

224. The French Government, emphasising the importance of bulk interception activities for the identification of unknown threats, considered that the criteria for assessing their Convention compatibility, as developed

in *Weber and Saravia v. Germany* ((dec.), no. 54934/00, ECHR 2006-XI) and *Roman Zakharov* (cited above), were relevant in the present case. However, in their view, there should be no “reasonable suspicion” requirement, having regard to the specific nature of bulk interception operations, which are different from the secret surveillance of a specific individual.

225. The French Government further considered that States enjoy a wide margin of appreciation in operating bulk interception regimes and that the assessment whether the applicable guarantees against abuse were sufficient must always be made *in concreto*, having regard to the relevant legislation seen as a whole. The Chamber in the present case had done exactly that, noting that despite the fact that some improvements were desirable, the Swedish system as a whole did not disclose significant shortcomings. However, in the case of *Big Brother Watch and Others* (cited above), the Chamber had applied a stricter scrutiny and unjustifiably found violations of Articles 8 and 10 of the Convention. The French Government advocated against the latter approach. In particular, they considered that a bulk interception regime that did not include judicial pre-authorisation was compatible with Article 8 as long as there was a mechanism for *a posteriori* supervision by an independent body.

226. The French Government also expressed the view, supported by references to case-law, that the interception and processing of communications data interfered with privacy rights in a less significant manner than the interception and processing of the content of communications and that, therefore, should not be subject to the same guarantees for the protection of the right to private life.

227. As regards intelligence sharing, the French Government stressed the importance of secrecy and the fact that the procedures and guarantees applied can vary from one State to another. They further elaborated on several relevant criteria, in particular, in the context of receiving and using intercepted data from foreign partners.

(c) The Government of the Kingdom of the Netherlands

228. The Government of the Kingdom of the Netherlands submitted that bulk interception was necessary to identify hitherto unknown threats to national security. In order to protect national security, intelligence services needed the tools to investigate emerging threats in a timely and effective manner. For this they needed the powers necessary to enable them to detect and/or prevent not only terrorist activities (such as planning of attacks, recruitment, propaganda and funding), but also intrusive State or non-State actors’ cyber activities aimed at disrupting democracy (for example, by influencing national elections or obstructing investigations by national and international organisations). An example of this was the attempted hacking of the investigation of the use of chemical weapons in Syria by the

Organisation for the Prohibition of Chemical Weapons in The Hague. Moreover, the increasing dependency of vital sectors on digital infrastructures meant that such sectors, including water management, energy, telecoms, transport, logistics, harbours and airports, were increasingly vulnerable to cyber-attacks. The consequences of disruption in such sectors would have a deep impact on society, far beyond the substantial monetary damage.

229. A complicating factor in all of this was the development of new means of digital communication and the exponential increase of data that was transmitted and stored globally. In many instances the nature and origin of a particular threat was unknown and the use of targeted interception was not feasible. However, while bulk interception was not as tightly defined as targeted interception, it was never completely untargeted. Rather, it was applied for specific aims.

230. In the intervening Government's view, there was no need for additional or updated minimum requirement; the minimum safeguards; those previously identified by the Court were sufficiently robust and "future proof". The additional requirements proposed by the applicant – in particular, the requirement to demonstrate "reasonable suspicion" – would unacceptably reduce the effectiveness of the intelligence services without providing any meaningful additional protection of individuals' fundamental rights.

231. Furthermore, according to the intervening Government, it was still relevant to distinguish between content and communications data, as the content of communications was likely to be more sensitive than communications data. The intervening Government also agreed with the Chamber that it was wrong automatically to assume that bulk interception constituted a greater intrusion into the private life of an individual than targeted interception, since once targeted interception takes place it was likely that all, or nearly all, of the intercepted communications would be analysed. This was not true of bulk interception, where restrictions on the examination and use of data determined the intrusiveness of the interception on the individuals' fundamental rights.

232. Finally, the intervening Government submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception in view of the high degree of uncertainty regarding the source of a threat. *Ex post* oversight provided sufficient safeguards.

(d) The Government of the Kingdom of Norway

233. The Norwegian Government submitted that, with regard to the decision of States to introduce and operate some form of bulk interception regime for national security purposes, the margin of appreciation had to be wide. This was because intelligence services had to keep pace with the rapid

advances in information and communications technology. Hostile actors changed their devices and digital identities at a pace which made it difficult to track them over time. It was also difficult to discover and counteract hostile cyber operations in a timely manner without tools capable of discovering anomalies and relevant signatures. It was therefore without doubt that modern capacities like bulk interception were needed in order to find unknown threats operating in the digital domain and to enable the services to discover and follow relevant intelligence threats.

234. As a consequence, the Court's oversight should be based on an overall assessment of whether the procedural safeguards against abuse which are in place are sufficient and adequate. It should therefore avoid enumerated and absolute requirements. It should also not apply criteria that would undermine indirectly the wide margin of appreciation afforded to States in deciding to operate a bulk interception regime for national security reasons. A "reasonable suspicion" or "subsequent notification" requirement would have this effect.

235. Finally, the Norwegian Government encouraged the Court to refrain from importing concepts and criteria from the CJEU. First of all, at the relevant time nineteen Council of Europe Contracting States were not members of the European Union. Secondly, while the Convention and the Charter of Fundamental Rights had many features in common, there were also differences, most notably Article 8 of the Charter which contained a right to the protection of personal data. The CJEU also formulated "proportionality" differently, using a "strict necessity" method which did not compare to that used by the Court.

4. The Court's assessment

(a) Preliminary remarks

236. The present complaint concerns the bulk interception of cross-border communications by the intelligence services. While it is not the first time the Court has considered this kind of surveillance (see *Weber and Saravia* and *Liberty and Others*, both cited above), in the course of the proceedings it has become apparent that the assessment of any such regime faces specific difficulties. In the current, increasingly digital, age the vast majority of communications take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance which is not targeted directly at individuals therefore has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State. Safeguards are therefore pivotal and yet elusive. Unlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, bulk interception is also – perhaps even predominantly – used for

foreign intelligence gathering and the identification of new threats from both known and unknown actors. When operating in this realm, Contracting States have a legitimate need for secrecy which means that little if any information about the operation of the scheme will be in the public domain, and such information as is available may be couched in terminology which is obscure and which may vary significantly from one State to the next.

237. While technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, global terrorism, drug trafficking, human trafficking and the sexual exploitation of children. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected. Access to such technology also permits hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes through the use of cyberattacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there. Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate.

(b) The existence of an interference

238. The Government considered that there was no interference with the applicant's Article 8 rights since it did not belong to a group of persons or entities targeted by the relevant legislation and in view of the fact that it was highly unlikely that the applicant's communications would be subject to analytical examination, there allegedly being no interference with Article 8 rights at the preceding stages of bulk interception of communications as it functioned in Sweden.

239. The Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses. Bulk interception regimes may not all follow exactly the same model, and the different stages of the process will not necessarily be discrete or followed in strict chronological order. Nevertheless, subject to the aforementioned caveats, the Court considers that the stages of the bulk interception process which fall to be considered can be described as follows:

- (a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);

- (b) the application of specific selectors to the retained communications/related communications data;
- (c) the examination of selected communications/related communications data by analysts; and
- (d) the subsequent retention of data and use of the “final product”, including the sharing of data with third parties.

240. At what the Court has taken to be the first stage, electronic communications (or “packets” of electronic communications) will be intercepted in bulk by the intelligence services. These communications will belong to a large number of individuals, many of whom will be of no interest whatsoever to the intelligence services. Some communications of a type unlikely to be of intelligence interest may be filtered out at this stage.

241. The initial searching, which is mostly automated, takes place at what the Court has taken to be the second stage, when different types of selectors, including “strong selectors” (such as an email address) and/or complex queries are applied to the retained packets of communications and related communications data. This may be the stage where the process begins to target individuals through the use of strong selectors.

242. At what the Court has taken to be the third stage, intercept material is examined for the first time by an analyst.

243. What the Court has taken to be the final stage is when the intercept material is actually used by the intelligence services. This may involve the creation of an intelligence report, the sharing of the material with other intelligence services within the intercepting State or even the transmission of material to foreign intelligence services.

244. The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals’ Article 8 rights will increase as the bulk interception process progresses. In this regard, the Court has clearly stated that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116), and that the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned (see *S. and Marper*, cited above, § 103). The fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, can have no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II and *S. and Marper*, cited above, §§ 67 and 75). Finally, at the end of the process, where information about a particular person will be analysed or the content of the communications is being examined by an analyst, the need for safeguards will be at its highest. This approach of the

Court is in line with the finding of the Venice Commission, which in its report on the Democratic Oversight of Signals Intelligence Agencies considered that in bulk interception the main interference with privacy occurred when stored personal data were processed and/or accessed by the agencies (see paragraphs 86-91 above).

245. Thus, the degree of interference with privacy rights will increase as the process moves through the different stages. In examining whether this increasing interference was justified, the Court will carry out its assessment of the relevant Swedish regime on the basis of this understanding of the nature of the interference.

(c) Whether the interference was justified

(i) General principles relating to secret measures of surveillance, including the interception of communications

246. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227; see also *Kennedy*, cited above, § 130). The wording "in accordance with the law" requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis – see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V, § 52; *S. and Marper*, cited above, § 95; and *Kennedy*, cited above, § 151).

247. The meaning of "foreseeability" in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone v. the United Kingdom*, 2 August 1984, § 67, Series A no. 82; *Leander*, cited above, § 51; *Huvig v. France*, 24 April 1990, § 29, Series A no. 176-B;

Valenzuela Contreras v. Spain, 30 July 1998, § 46, Reports of Judgments and Decisions 1998-V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

248. In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the “necessity” test has been complied with and it is therefore appropriate for the Court to address jointly the “in accordance with the law” and “necessity” requirements. The “quality of law” in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when “necessary in a democratic society”, in particular by providing for adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov*, cited above, § 236; and *Kennedy*, cited above, § 155).

249. In this regard it should be reiterated that in its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: (1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (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 intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum safeguards also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see *Roman Zakharov*, cited above, § 238).

250. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two

stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see *Roman Zakharov*, cited above, § 233; see also *Klass and Others*, cited above, §§ 55 and 56).

251. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others v.*, cited above, § 57; and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

252. As to the question whether an interference was “necessary in a democratic society” in pursuit of a legitimate aim, the Court has recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106).

253. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are 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. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the

“interference” to what is “necessary in a democratic society” (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106; and *Kennedy*, cited above, §§ 153 and 154).

(ii) *Whether there is a need to develop the case-law*

254. In *Weber and Saravia* and *kingdom and Others* (cited above) the Court accepted that bulk interception regimes did not *per se* fall outside the States’ margin of appreciation. In view of the proliferation of threats that States currently face from networks of international actors, using the Internet both for communication and as a tool, and the existence of sophisticated technology which would enable these actors to avoid detection, the Court considers that the decision to operate a bulk interception regime in order to identify threats to national security or against essential national interests is one which continues to fall within this margin.

255. In both *Weber and Saravia* and *Liberty and Others* (cited above) the Court applied the above-mentioned six minimum safeguards developed in its case-law on targeted interception. However, while the bulk interception regimes considered in those cases were on their face similar to that in issue in the present case, both cases are now more than ten years old, and in the intervening years technological developments have significantly changed the way in which people communicate. Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago. The scope of the surveillance activity considered in those cases would therefore have been much narrower.

256. This is equally so with related communications data. It appears that greater volumes of communications data are currently available on an individual relative to content, since every piece of content is surrounded by multiple pieces of communications data. While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.

257. More importantly, however, in *Weber and Saravia* and *Liberty and Others* (both cited above), the Court did not expressly address the fact that it

was dealing with surveillance of a different nature and scale from that considered in previous cases. Nonetheless, targeted interception and bulk interception are different in a number of important respects.

258. To begin with, bulk interception is generally directed at international communications (that is, communications physically travelling across State borders), and while the interception and even examination of communications of persons within the surveilling State might not be excluded, in many cases the stated purpose of bulk interception is to monitor the communications of persons outside the State's territorial jurisdiction, which could not be monitored by other forms of surveillance. For example, the German system aims only to monitor foreign telecommunications outside of German territory (see paragraph 137 above).

259. Moreover, as already noted, the purposes for which bulk interception may be employed would appear to be different. In so far as the Court has considered targeted interception, it has, for the most part, been employed by respondent States for the purposes of investigating crime. However, while bulk interception may be used to investigate certain serious crimes, Council of Europe member States operating a bulk interception regime appear to use it for the purposes of foreign intelligence gathering, the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism (see paragraphs 131-146 above).

260. While bulk interception is not necessarily used to target specified individuals, it evidently can be – and is – used for this purpose. However, when this is the case, the targeted individuals' devices are not monitored. Rather, individuals are “targeted” by the application of strong selectors (such as their email addresses) to the communications intercepted in bulk by the intelligence services. Only those “packets” of the targeted individuals' communications which were travelling across the bearers selected by the intelligence services will have been intercepted in this way, and only those intercepted communications which matched either a strong selector or complex query could be examined by an analyst.

261. As with any interception regime, there is of course considerable potential for bulk interception to be abused in a manner adversely affecting the right of individuals to respect for private life. While Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present. The Court has already identified those safeguards which should feature in a Convention-compliant targeted interception regime. While those principles provide a useful framework for this exercise, they will have to be adapted to reflect the specific features of a bulk interception regime and, in particular, the

increasing degrees of intrusion into the Article 8 rights of individuals as the operation moves through the stages identified in paragraph 239 above.

(iii) The approach to be followed in bulk interception cases

262. It is clear that the first two of the six “minimum safeguards” which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power (that is, the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted: see paragraph 249 above), are not readily applicable to a bulk interception regime. Similarly, the requirement of “reasonable suspicion”, which can be found in the Court’s case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual’s communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments — that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk interception.

263. In its case-law on targeted interception, the Court has had regard to the arrangements for supervising and reviewing the interception regime (see *Roman Zakharov*, cited above, §§ 233-34). In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

264. Therefore, in order to minimise the risk of the bulk interception being abused, the Court considers that the process must be subject to “end-to-end safeguards”, meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the bulk operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review. In the Court’s view, these are fundamental safeguards which will be the cornerstone of any

Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 86 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).

265. Turning first to authorisation, the Grand Chamber considers that while judicial authorisation is an “important safeguard against arbitrariness” it is not a “necessary requirement”. Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive.

266. Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

267. The use of selectors – and strong selectors in particular – is one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence services. However, the Court notes that the intervening Government of the Netherlands have submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception (see paragraphs 228-232 above). In the United Kingdom, the IPT found that the inclusion of the selectors in the authorisation would “unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic” (see *Big Brother Watch and Others*, cited above, § 49).

268. Taking into account the characteristics of bulk interception (see paragraphs 258 and 259 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used.

269. Moreover, enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles.

270. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the “interference” to what is “necessary in a democratic society” (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106; and *Kennedy*, cited above, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process.

271. Finally, an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. In the targeted interception context, the Court has repeatedly found the subsequent notification of surveillance measures to be a relevant factor in assessing the effectiveness of remedies before the courts and hence the existence of effective safeguards against the abuse of surveillance powers. However, it has acknowledged that notification is not necessary if the system of domestic remedies permits any person who suspects that his or her communications are being or have been intercepted to apply to the courts; in other words, where the courts’ jurisdiction does not depend on notification to the interception subject that there has been an interception of his or her communications (see *Roman Zakharov*, cited above, § 234; and *Kennedy*, cited above, § 167).

272. The Court considers that a remedy which does not depend on notification to the interception subject could also be an effective remedy in the context of bulk interception; in fact, depending on the circumstances it may even offer better guarantees of a proper procedure than a system based on notification. Regardless of whether material was acquired through targeted or bulk interception, the existence of a national security exception could deprive a notification requirement of any real practical effect. The likelihood of a notification requirement having little or no practical effect will be more acute in the bulk interception context, since such surveillance may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State’s territorial jurisdiction. Therefore, even if the identity of a target is known, the authorities may not be aware of his or her location.

273. The powers and procedural guarantees an authority possesses are relevant in determining whether a remedy is effective. Therefore, in the absence of a notification requirement it is imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, insofar as possible, an adversarial process. The decisions of such authority shall be reasoned and legally binding with regard, *inter alia*, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material (see, *mutatis mutandis*, *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 120, ECHR 2006-VII and also *Leander*, cited above, §§ 81-83 where the lack of power to render a legally binding decision constituted a main weakness in the control offered).

274. In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to “end-to-end safeguards” (see paragraph 264 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhev*, cited above, § 92).

275. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 256 above), the Court would need to take account of a wider range of criteria than the six *Weber* safeguards. More specifically, in addressing jointly “in accordance with the law” and “necessity” as is the established approach in this area (see *Roman Zakharov*, cited above, § 236; and *Kennedy*, cited above, § 155), the Court will examine whether the domestic legal framework clearly defined:

1. The grounds on which bulk interception may be authorised;
2. The circumstances in which an individual’s communications may be intercepted;
3. The procedure to be followed for granting authorisation;
4. The procedures to be followed for selecting, examining and using intercept material;
5. The precautions to be taken when communicating the material to other parties;
6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;

8. The procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

276. Despite being one of the six *Weber* criteria, to date the Court has not yet provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties. However, it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Consequently, the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control.

277. For the reasons identified at paragraph 256 above, the Court is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content. It therefore considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content.

278. That being said, while the interception of related communications data will normally be authorised at the same time the interception of content is authorised, once obtained they may be treated differently by the intelligence services. In view of the different character of related communications data and the different ways in which they are used by the intelligence services, as long as the aforementioned safeguards are in place, the Court is of the opinion that the legal provisions governing their treatment may not necessarily have to be identical in every respect to those governing the treatment of content.

(iv) The Court's assessment of the case at hand

(1) Preliminary remarks

279. As noted by the Chamber, it has not been disputed by the parties that the Swedish signals intelligence activities have a basis in domestic law (see paragraph 111 of the Chamber judgment). It is further undisputed that the impugned signals intelligence regime pursues legitimate aims in the interest of national security by supporting Swedish foreign, defence and security policy and identifying external threats to the country. Therefore, following the approach outlined above, it remains to be considered whether the domestic law was accessible and contained adequate and effective safeguards and guarantees to meet the requirements of “foreseeability” and “necessity in a democratic society”.

280. Bulk interception of electronic signals within foreign intelligence in Sweden is regulated in several pieces of legislation, the main ones being the Foreign Intelligence Act and the associated Ordinance, the Signals Intelligence Act and Ordinance, the Foreign Intelligence Court Act and the FRA Personal Data Processing Act and Ordinance. Additional relevant provisions on, in particular, some aspects of the functioning of the applicable supervision mechanisms and remedies are to be found in the Foreign Intelligence Inspectorate Instructions Ordinance, the Parliamentary Ombudsmen Instructions Act and the Chancellor of Justice Supervision Act (see paragraphs 14-74 above).

281. It has not been disputed that all these provisions are publicly available. The Court would accept, therefore, that the domestic law was adequately “accessible”.

282. Turning next to the question whether the law contained adequate and effective safeguards and guarantees to meet the requirements of “foreseeability” and “necessity in a democratic society”, the Court will address in subsections (β) – (ι) each of the eight requirements set out in paragraph 275 above.

283. In the present case it will do so simultaneously with respect to the interception of the contents of electronic communications and related communications data. This approach is justified by the fact, undisputed between the parties, that under the Swedish signals intelligence regime, the same legal provisions, procedures and safeguards concerning the interception, retention, examining, use and storing of electronic signals apply without distinction both to communications data and to the content of communications. Under the Swedish regime no particular separate issue arises, therefore, with regard to the use of communications data in bulk interception operations.

(2) The grounds on which bulk interception may be authorised

284. As noted by the Chamber, according to the Signals Intelligence Act signals intelligence may be conducted only to monitor:

1. external military threats to the country;
2. conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations;
3. strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests;
4. the development and proliferation of weapons of mass destruction, military equipment and other similar specified products;
5. serious external threats to society's infrastructure;
6. foreign conflicts with consequences for international security;
7. foreign intelligence operations against Swedish interests; and
8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy (see paragraph 22 above).

285. The preparatory works to the Signal Intelligence Act contain further elaboration of the meaning of these eight purposes (see paragraph 23 above). In the Court's view, the level of detail and the terms used circumscribe the area in which bulk interception may be used with sufficient clarity, having regard, in particular, to the fact that the impugned regime aims at uncovering unknown foreign threats whose nature may vary and evolve with time.

286. The Court observes that while section 4 of the Foreign Intelligence Act excludes the conduct of signals intelligence within foreign intelligence to solve tasks in the area of law enforcement or crime prevention, one of the eight purposes listed above concerns "serious cross-border crime" such as, according to the preparatory works, "drug or human trafficking of such severity that it may threaten significant national interests" (see paragraph 23 above).

287. The preparatory works clarify that the aim in this regard is to survey terrorism or other cross-border crime from the perspective of Sweden's foreign and security policy, not to combat criminal activity operatively (*ibid*). It is undisputed that information obtained through the impugned regime of signals intelligence cannot be used in criminal proceedings. As explained by the Government, tasking directives for signals intelligence may not be issued to investigate criminal offences and when the FRA reports intelligence to other agencies it stipulates that the intelligence may not be used in criminal investigations. In the light of the above, the Court does not share the concerns expressed by the applicant regarding the fact that since 1 March 2018 certain police departments may issue tasking directives and that the Security Police might be granted access to the FRA's

analysis material (see above paragraphs 193 *in fine* and 196 *in fine*). It finds convincing the Government's clarification that access may only be granted to "data that constitutes the analysis results" so as to allow strategic assessments and that the prohibition on using signals intelligence within foreign intelligence for the purposes of investigating criminal offences fully applies (see paragraph 214 above).

288. In sum, the grounds upon which bulk interception can be authorised in Sweden are clearly circumscribed so as to permit the necessary control at the authorisation and operation stage and *ex post facto* supervision.

- (3) The circumstances in which an individual's communications may be intercepted

289. In a bulk interception regime the circumstances in which communications might be intercepted will be very broad, as it is the communications bearers that are targeted rather than the devices from which the communications are sent, or the senders or recipients of the communications. The circumstances in which communications may be examined will be narrower, but compared to targeted interception this category will still be relatively wide, since bulk interception may be used for a more varied range of purposes, and communications may be selected for examination by reference to factors other than the identity of the sender or recipient.

290. As regards interception, signals intelligence conducted on fibre optic cables may only concern communications crossing the Swedish border. Also, and regardless of whether the source is airborne or cable-based, communications between a sender and a receiver in Sweden may not be intercepted (see paragraph 25 above). The Government have admitted, however, that separating "domestic" from "foreign" traffic is not always possible in the initial interception stages, as confirmed in the 2011 report of the Signals Intelligence Committee (see paragraphs 77-80 above; see also the reports of the Data Protection Authority, paragraphs 75-76 above).

291. It is true that the FRA may also intercept signals as part of its development activities, which may lead to data not relevant for the regular foreign intelligence being intercepted. It appears from the report of the Signals Intelligence Committee (see paragraphs 77-80 above), that signals intercepted as part of the FRA's development activities can be used, including by being "read" and stored, for technological development purposes regardless of whether they fall within the categories defined under the eight foreign intelligence purposes.

292. The Court observes, however, that signals intercepted in the context of the FRA's development activities do not interest the authorities for the data they might contain but only for the possibility they afford to analyse the systems and routes through which information is transmitted. In the Court's view, the respondent Government's explanation about the need for

such an arrangement (see paragraph 207 above) is satisfactory. The examples given (the need to monitor the traffic between certain countries in order to identify bearers with relevant traffic; the need to identify trends such as new types of signals and signals protection) appear convincing: the authorities must be able to react to the evolution in technology and communication practices and, for that reason, may need to monitor very large segments of the international signals traffic. The degree of interference with individuals' Article 8 rights engendered by such activities appears to be of a very low intensity having regard to the fact that the data thereby obtained is not in a form destined to generate intelligence.

293. In addition, it is undisputed that any information that may happen to emerge from signals intercepted for technological development purposes cannot be used as intelligence information unless such use is in conformity with the eight purposes and the applicable tasking directives (see paragraph 79 above). Moreover, development activities can be undertaken only under a permit issued by the Foreign Intelligence Court and are supervised by the Inspectorate, including for compliance with the law and the tasking directives approved by the Foreign Intelligence Court. In these circumstances the Court is satisfied that the legal framework within which the FRA's development activities are conducted contains safeguards capable of preventing attempts to circumvent the legal restrictions related to the grounds for which signals intelligence may be used.

294. In view of the above the Court can accept that the legal provisions on bulk interception in Sweden set out with sufficient clarity the circumstances in which communications may be intercepted.

(4) The procedure to be followed for granting authorisation

295. Under Swedish law, every signals intelligence mission to be conducted by the FRA must be authorised in advance by the Foreign Intelligence Court. Where this procedure might cause delay or other inconveniences of essential importance for one of the specified purposes of the signals intelligence, the FRA may itself grant a permit and notify the Foreign Intelligence Court immediately, which triggers the permit's rapid review by that court. The court has the power to modify or revoke it if necessary (see paragraphs 30-33 above).

296. There is no doubt that the Foreign Intelligence Court meets the requirement of independence from the executive. In particular, its president and vice-presidents are permanent judges and, while all members are appointed by the Government, they have legally defined four-year terms of office. Also, it is undisputed that neither the Government or Parliament nor other authorities may interfere with the court's decision-making, which is legally binding.

297. As noted by the Chamber, for reasons of secrecy the Foreign Intelligence Court has never held a public hearing and all its decisions are

confidential. However, Swedish law provides for the mandatory presence of a privacy protection representative at that court's sessions, except in urgent cases. The representative, who is a judge, a former judge or an attorney, acts independently and in the public interest but not in the interest of any affected private individual. He or she has access to all the case documents and may make statements (see paragraph 34 above). In the Court's view, having regard to the imperative need for secrecy, in particular at the stages of initial authorisation and conducting signals intelligence, the arrangement described above contains relevant safeguards against arbitrariness and must be accepted as an inevitable limitation on the authorisation procedure's transparency.

298. The Court further observes that when applying for a permit the FRA must specify the need for the intelligence sought, the communications bearers to which access is needed and the selectors – or at least the categories of selectors – that will be used. This should lead to examination whether the mission is compatible with applicable legislation, including the eight purposes for which signals intelligence may be undertaken, and whether the intelligence collection is proportional to the resultant interference with private life (see paragraphs 30-33 above).

299. Importantly, section 3 of the Signals Intelligence Act requires that the selectors must be formulated in such a way that the interference with personal integrity is limited as far as possible (see paragraph 26 above), which implies necessity and proportionality analysis. Compliance with this requirement at the authorisation phase is within the competence of the Foreign Intelligence Court. That court's decision, taken in proceedings with the participation of a privacy protection representative, is binding. This is an important safeguard built into the Swedish bulk interception system.

300. The Court further observes that Swedish law provides for a form of special prior authorisation of strong selectors in that the Foreign Intelligence Court verifies whether, as required by section 3 of the Signals Intelligence Act, the use of selectors directly related to a specific natural person is of "exceptional importance" for the intelligence activities. The interpretation of section 3 of the Signals Intelligence Act in the practice of the Foreign Intelligence Court has not been explained to the Court, nor how section 3 interacts with section 5 of the same Act, which indicates that the judicial authorisation may at least in some cases concern "categories of selectors" rather than individual selectors. If such a case would occur, namely individual selectors not being approved by the Foreign Intelligence Court, the question would arise whether a process of prior internal authorisation providing for separate and objective verification is in place (see paragraph 269 above). However, having regard to the independence of the Foreign Intelligence Court and the applicable procedural guarantees in proceedings before it, the "exceptional importance" standard at the authorisation stage is

capable of providing relevant enhanced protection against the arbitrary use of selectors linked to identified individuals.

301. The Swedish system of authorisation has its inherent limits. For example, it may be difficult for the Foreign Intelligence Court to appreciate the proportionality aspect where only categories of selectors are specified in the FRA's request for a permit, or where the indicated selectors are several thousand in number or are expressed as technical combinations of numbers or letters.

302. However, for the purposes of the Court's analysis, at this stage the relevant point is that the Swedish authorisation system offers a judicial *ex ante* review of permit requests which is comprehensive, in the sense that the aim of the mission and the bearers and categories of selectors to be used are subject to control, and is sufficiently detailed in respect of secret bulk signals intelligence as part of foreign intelligence. Such a review offers a significant safeguard against, notably, the launch of abusive or clearly disproportionate bulk interception operations. Importantly, it also sets the framework within which a concrete operation must unfold and the limits whose observance then becomes the object of the applicable supervision and *ex post facto* control mechanisms.

- (5) The procedures to be followed for selecting, examining and using intercept material

303. It transpires from the material in the Court's possession that in Sweden the interception of cable-based electronic signals is automated and the interception of such signals over the airways may be either automated or manual. Automated interception over the airways is a process that is identical to the process of interception of signals passing through cross-border cables.

304. As regards the use of non-automated interception and searches of electronic signals over the airways, the Swedish Government clarified before the Grand Chamber that it is primarily used for near real-time reporting of foreign military activities and is done by an operator who listens in real time to military radio transmissions on selected radio frequencies or looks at a screen where the energy from a signal in electronic form is visualised and then records relevant parts for analysing and reporting. The applicant did not comment in reply.

305. Even assuming that the interception of foreign military radio frequencies may affect Article 8 rights in rare cases, the Court notes that this aspect of the Swedish signals intelligence regime is covered by the same procedures and safeguards as applicable to interception and use of cable-based communications.

306. Turning to the procedure for examination of the intercepted material, the Court notes that, as explained by the respondent Government, the FRA processes the data through automated and manual means, using,

among other techniques, cryptanalysis, structuring and language translation. Thereafter, the processed information is analysed by an analyst in order to identify intelligence therein. The next step consists in the elaboration of a report which is disseminated to selected recipients of foreign intelligence (see paragraphs 18 and 29 above).

307. In the Court's view, it is significant that at the examination stage the FRA is under an obligation to discard intercepted domestic communications immediately once identified (see paragraph 38 above).

308. Despite the fact that the distinction between domestic and foreign communications may not be waterproof and the prohibition to intercept the former apparently cannot prevent it from happening in the automatic stage of capturing signals, the exclusion of domestic traffic from the scope of signals intelligence must be seen as a significant limitation on the authorities' discretion and as a safeguard against abuse. The limitation in question sets the framework within which the authorities are allowed to operate and provides the existing pre-authorisation, supervision and control mechanisms with an important criterion related to the operation's lawfulness and the protection of the rights of individuals. In particular, it is clear that the choice of communications bearers and categories of selectors – which is subject to control by the Foreign Intelligence Court (see paragraph 30 above) – must be in conformity with the above-mentioned exclusion of domestic communications.

309. As already noted above (see paragraph 300), the practice of the Foreign Intelligence Court regarding the pre-authorisation of selectors or categories of selectors directly linked to identifiable individuals has not been presented to the Court. The Court notes, however, the Government's position that logs and records are systematically kept by the FRA throughout the process, from the collection of data to the final reporting, communicating to other parties and destruction. All searches made by analysts are recorded. When the search is made in a data compilation containing personal data the record includes the selectors used, the time, the name of the analyst and the justification for the search, including the detailed tasking directive which is the reason for the search. In addition to the logs, records are kept of decisions taken in the course of the signals intelligence process.

310. The applicant did not dispute the above but considered that (i) it had not been shown that logs were sufficiently detailed and (ii) the FRA's record-keeping practices, not being prescribed by law, were at the mercy of internal procedures and discretion.

311. The Court considers that the obligation to keep logs and detailed record of each step in bulk interception operations, including all selectors used, must be set out in domestic law. The fact that in Sweden it appears in internal instructions only is undoubtedly a shortcoming. However, having regard, in particular, to the existence of oversight mechanisms covering all

aspects of the FRA's activities, there is no reason to consider that detailed logs and records are not kept in practice or that the FRA could proceed to changing its internal instructions arbitrarily and removing its obligation in that regard. While it is true that in 2010 and 2016 the Swedish Data Protection Authority criticised an aspect of the FRA's practices of keeping logs, this only concerned the manner in which the FRA monitored logs used to detect unwarranted use of personal data (see paragraph 76 above). Furthermore, the Government clarified that since 1 January 2018 logs which were previously kept by separate "system owners" within the FRA are being sent to a central function, thus improving their monitoring. This change had been reported to the Swedish Data Protection Authority, which had not requested further action and had closed the file.

312. Swedish law affords specific protection of personal data, including data that may reveal aspects of natural persons' private life or communications. In the context of signals intelligence, the FRA Personal Data Processing Act imposes on the FRA the obligation to ensure that personal data is collected only for the authorised purposes expressly determined through tasking directives and within the limits of the permit issued by the Foreign Intelligence Court. As noted by the Chamber, the personal data treated also has to be adequate and relevant in relation to the purpose of the treatment. No more personal data than what is necessary for that purpose may be processed. All reasonable efforts have to be made to correct, block and obliterate personal data which is incorrect or incomplete in relation to the purpose (see paragraph 40 above). The FRA staff treating personal data are security cleared, subject to confidentiality and under an obligation to handle the personal data in a safe manner. Also, they could face criminal sanctions if tasks relating to the treatment of personal data are mismanaged (see paragraph 42 above).

313. The applicant criticised the fact that the safeguards mentioned in the preceding paragraph only apply to intercepted material containing "information that is directly or indirectly related to a natural living person". The applicant deduced from this fact that legal persons were left unprotected.

314. The Court observes, however, that there is nothing to suggest that the protection guaranteed by the FRA Personal Data Processing Act and the FRA Personal Data Processing Ordinance does not apply to the content of communications exchanged by legal persons such as the applicant whenever those include "information that is directly or indirectly related to a natural living person". Furthermore, it must be noted that most legal requirements and safeguards provided for in the above-mentioned legislation would normally be of value to natural persons only. For example, the Act in question prohibits processing of personal data solely because of what is known of a person's race or ethnicity, political, religious or philosophical views, membership of a union, health or sexual life. It provides for a special

requirement limiting the keeping of material containing personal data and for sanctions for mismanagement of personal data. It guarantees specific monitoring of personal data treatment and sets out the powers of the Data Protection Authority in this regard. In other words, the Act in question adds another layer of protection, tailored to the specificities of personal data, to the already existing safeguards that are applicable to information concerning natural and legal persons alike.

315. This approach, which takes into account the special sensitivity of personal data, does not seem to be problematic and does not mean that the communications of legal persons are left unprotected by safeguards. Contrary to the applicant's claim, there is nothing in the relevant legislation suggesting that intercept material not containing personal data can be used for purposes incompatible with the original purpose of the interception, as approved by the Foreign Intelligence Court.

316. In sum, the Court is satisfied that the legislation on selecting, examining and using intercepted data provides adequate safeguards against abuse that may affect Article 8 rights.

- (6) The precautions to be taken when communicating the material to other parties

317. As regards communication of data from the FRA to other Swedish Government bodies, the Court observes that the very purpose of signals intelligence is to obtain information that is useful for the mission of relevant sectors of Government. The circle of domestic authorities that may be given such information in Sweden is narrow and includes above all the Security Police and the Armed Forces. The FRA may grant these bodies direct access to data that constitutes the results of analysis in a data compilation, to enable them to make assessments of terrorist threats at strategic level. This is done, in particular, in the framework of a tripartite working group of analysts from the FRA, the Security Police and the Armed Forces, called the National Centre for Assessment of Terrorist Threats. The Court considers that the above regime is clearly circumscribed and does not appear to generate a particular risk of abuse.

318. The Court further notes that the Chamber expressed concerns as regards the Swedish arrangements on communicating data to foreign Governments or international organisations, pointing to three issues: (a) that the legislation does not require consideration of possible harm to the individual concerned when making a decision about sharing; (b) that there is no provision requiring the recipient State or organisation to protect the data with the same or similar safeguards as those applicable under Swedish law and; (c) that the possibility to communicate data when necessary for "international defence and security cooperation" opens up for a rather wide scope of discretion. The Chamber nevertheless considered that the

supervisory mechanisms sufficiently counterbalanced these regulatory shortcomings (see paragraph 150 of the Chamber judgment).

319. Before the Grand Chamber the Government essentially disputed that there were areas of concern, emphasising that international cooperation was limited to exchanges with trusted foreign partners and was monitored by the Inspectorate, whereas the applicant considered that the discretion granted to the FRA was too broad and that the existing supervisory mechanisms did not counterbalance the identified shortcomings, there being no legal requirements in respect of which compliance could be supervised (see the parties' positions in more detail in paragraphs 200, 201, 215 and 216 above).

320. The Court points out at the outset that in the present case it is not dealing with a concrete occurrence of, for example, the disclosure or use, by a foreign Government or organisation, of personal data transmitted to them by the Swedish authorities. Indeed, no examples about such disclosures or use have been submitted to the Court. Nonetheless, insofar as the possibility of transmitting intelligence to foreign parties is part of the Swedish bulk interception regime and activities whose very existence can be seen as interfering with Article 8 rights, the Court, having regard to the applicant's complaints, must review the Swedish intelligence transmission regime and its functioning for their compliance with the requirements of quality of the law and necessity in a democratic society. The applicant's complaints relate solely to the sending of intelligence to foreign parties and do not concern the receipt of foreign intelligence and its use by the Swedish authorities.

321. It is undisputed that Contracting States may need to transmit to foreign services intelligence obtained through bulk interception of communications for a variety of reasons, including warning foreign Governments about threats, soliciting their help in identifying and dealing with threats or enabling international organisations to act in exercise of their mandate. International cooperation is crucial for the effectiveness of the authorities' efforts to detect and thwart potential threats to Contracting States' national security.

322. The Court observes that the possibility for the FRA to share intelligence it has obtained with foreign partners is provided for in Swedish law, which also sets out the relevant general purpose (see paragraphs 49 and 74 above). It is to be observed, however, that the level of generality of the terms used cannot but lead to the conclusion that the FRA may send intelligence abroad whenever this is considered to be in the national interest.

323. Having regard to the unpredictability of situations that may warrant cooperation with foreign intelligence partners, it is understandable that the precise scope of intelligence sharing cannot be circumscribed in law through, for example, exhaustive and detailed lists of such situations or the types of intelligence or content that can be transmitted. The applicable legal regulation and practice must operate, however, in a manner capable of

limiting the risk of abuse and disproportionate interference with Article 8 rights.

324. In this regard the Court notes, first, that in so far as the intelligence transmitted to foreign services is in the form of information obtained by the FRA through its bulk interception activities, it is necessarily the product of legally regulated procedures to which all relevant safeguards apply. This includes the procedural guarantees, such as the authorisation by the Foreign Intelligence Court and the supervision by the Inspectorate (see paragraphs 295-302 above and 345-353 below), and the substantive limitations, such as those regarding the grounds on which interception of signals can be ordered, the searching, in particular through selectors identifying an individual, and all further examination (see paragraphs 284-288 and 303-316 above). As already seen, the above mentioned procedures involve an assessment of necessity and proportionality with regard to, in particular, Article 8 Convention rights. Therefore, the safeguards internally applicable in Sweden in the process of obtaining the intelligence that may later be transmitted to a foreign partner also limit, at least to a certain extent, the risk of adverse consequences that may ensue after the transmission has taken place.

325. The Court also notes that the supervision mechanisms provided for under the Personal Data Processing Act, specifically tailored to the protection of personal data, apply to all activities of the FRA (see paragraphs 56 above).

326. In the Court's view, despite the above considerations, the absence, in the relevant signals intelligence legislation, of an express legal requirement for the FRA to assess the necessity and proportionality of intelligence sharing for its possible impact on Article 8 rights is a substantial shortcoming of the Swedish regime of bulk interception activities. It appears that, as a result of this state of the law, the FRA is not obliged to take any action even in situations when, for example, information seriously compromising privacy rights is present in material to be transmitted abroad without its transmission being of any significant intelligence value. Furthermore, despite the fact that the Swedish authorities obviously lose control over the shared material once it has been sent out, no legally binding obligation is imposed on the FRA to analyse and determine whether the foreign recipient of intelligence offers an acceptable minimum level of safeguards (see paragraph 276 above).

327. The Government's answer to these concerns was essentially that intelligence cooperation with foreign services inevitably functions on the basis of a shared interest in preserving the secrecy of information and that this practical reality limited the risks of abuse.

328. The Court finds the above-mentioned approach insufficient as a safeguard. The Government have not identified any obstacles against setting out clearly in domestic law an obligation for the FRA or another relevant

body to balance the necessity of transmitting intelligence abroad against the need to protect the right to respect for private life. By comparison, the Court notes that, for example, the relevant regime in the United Kingdom includes an obligation to take reasonable steps to ensure that the foreign authorities would maintain the necessary procedures to safeguard the intercepted material and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary (see paragraph 7.5 of the United Kingdom Interception of Communications Code of Practice, quoted in *Big Brother Watch and Others*, cited above, § 96).

329. It is true that in 2014 the Inspectorate undertook a general review of the FRA's cooperation with other States and, between 2009 and 2017, repeatedly inspected other relevant aspects of its activities, including the treatment of personal data and the communication of its reports (see paragraph 53 above). However, since the Inspectorate's role is to exercise control for lawfulness, in the absence of an express legal obligation for the FRA to consider privacy concerns or seek at least some safeguards in this regard from foreign partners before sending them intelligence, it is not unreasonable to consider, as the applicant did, that the Inspectorate does not monitor possible risks or disproportionate consequences of intelligence sharing on Article 8 Convention rights. The respondent Government have failed to convince the Court that this is done in practice on the basis of, for example, constitutional or other general fundamental rights provisions. It follows that, unlike the Chamber, the Grand Chamber cannot accept that the shortcomings in the regulatory framework are sufficiently counterbalanced by the supervisory elements of the Swedish regime.

330. In sum, the absence of a requirement in the Signals Intelligence Act or other relevant legislation that consideration be given to the privacy interests of the individual concerned when making a decision about intelligence sharing is a significant shortcoming of the Swedish regime, to be taken into account in the Court's assessment of its compatibility with Article 8 of the Convention.

- (7) The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed

331. The duration of bulk interception operations is, of course, a matter for the domestic authorities to decide. There must, however, be adequate safeguards, such as a clear indication in domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled (see *Roman Zakharov*, cited above, § 250).

332. Under section 5(a) of the Signals Intelligence Act a permit may be granted for a maximum of six months. This period may be extended, for six months at a time, following a new full examination of the relevant conditions for the granting of a permit by the Foreign Intelligence Court.

Therefore, as noted by the Chamber, Swedish law gives a clear indication of the period after which a permit will expire and of the conditions under which it may be renewed.

333. As also noted by the Chamber, however, there is no provision obliging the FRA, the authorities mandated to issue detailed tasking directives or the Foreign Intelligence Court to cancel a signals intelligence mission if the conditions for it have ceased to exist or the measures themselves are no longer necessary.

334. Before the Grand Chamber, the applicant considered that the lack of provision for the cancellation of permits when no longer needed opened the door to excessive and inappropriate surveillance for several months until the warrant eventually expired on its own. In the applicant's view, this shortcoming was very significant, given the sheer volume of information that could be obtained through bulk interception in that time. The Government stated that an interception operation would be discontinued if it was no longer needed, if a tasking directive was revoked or if it was not in accordance with the permit.

335. The Court is of the view that an express provision on discontinuation of bulk interception when no longer needed would have been clearer than the existing arrangement in Sweden according to which, apparently, permits may or may not be cancelled when circumstances warranting such a cancellation come to light in the period before the expiry of their six months' validity.

336. The significance of this shortcoming should, however, not be overestimated, in the Court's view, for two main reasons. First, Swedish law provides for relevant mechanisms, such as the possibility for the requesting authority to revoke a tasking directive and for supervision by the Inspectorate, both of which can lead to the cancellation of a bulk interception mission when the conditions for it have ceased to exist or it is no longer needed. Second, by the nature of things, in the context of signals intelligence within foreign intelligence the implementation of a legal requirement to cancel a permit when no longer needed must in all likelihood be heavily dependent on internal operative assessments involving secrecy. Therefore, in the specific context of bulk interception for foreign intelligence purposes, the existence of supervision mechanisms with access to all internal information must generally be seen as providing similar legislative safeguards against abuse related to the duration of interception operations.

337. For the reasons set out above, the Court finds that Swedish law satisfies the requirements concerning duration of bulk interception of communications.

338. The Chamber made the following findings concerning the circumstances in which intercept data must be erased and destroyed, at paragraphs 145 and 146 of its judgment:

“145. Contrary to the applicant’s claim, there are several provisions regulating the situations when intercepted data has to be destroyed. For example, intelligence must be destroyed immediately if it 1) concerns a specific natural person and has been determined to lack importance for the purpose of the signals intelligence, 2) is protected by constitutional provisions of secrecy for the protection of anonymous authors or media sources, 3) contains information shared between a criminal suspect and his or her counsel and is thus protected by attorney-client privilege, or 4) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information ... Moreover, if communications have been intercepted between a sender and receiver both in Sweden, despite the ban on the interception of such communications, they must be destroyed as soon as their domestic nature has become evident ... Also, where a temporary permit granted by the FRA has been revoked by the Foreign Intelligence Court, all intelligence collected on the basis of that permit must be immediately destroyed ...

146. Although the FRA may maintain databases for raw material containing personal data up to one year, it has to be kept in mind that raw material is unprocessed information. That is, it has yet to be subjected to manual treatment. The Court accepts that it is necessary for the FRA to store raw material before it can be manually processed. At the same time, the Court stresses the importance of deleting such data as soon as it is evident that it lacks pertinence for a signals intelligence mission.”

339. The Grand Chamber endorses this analysis in principle but also considers it important to point to the fact that it has insufficient information about certain aspects of the manner in which the rules on destruction of intercept material are applied in practice.

340. Certainly, the Inspectorate’s supervision powers include the monitoring of the FRA’s practice on destroying intercept material and this aspect of its activities has already been the subject of inspections (see paragraph 53 above). This is an important safeguard for the proper application of the existing rules.

341. However, before the Grand Chamber the applicant pointed to the fact that the limits on the storing of intercept material and the requirements mentioned by the Chamber about destroying it did not apply to material which does not contain personal data. The Government did not address this issue specifically.

342. In the Court’s view, while there is clear justification for special requirements regarding the destruction of material containing personal data, there must also be a general legal rule governing the destruction of other material obtained through bulk interception of communications, where keeping it may affect, for example, the right of respect for correspondence under Article 8, including concerning legal persons as the applicant. As a very minimum, as also stressed by the Chamber, there should be a legal requirement to delete intercepted data that has lost pertinence for signals intelligence purposes. The Government have not shown that the Swedish regulatory framework covers this aspect. However, while observing that there is only a narrow set of circumstances in which it could happen that none of the specific rules on destruction of intercept material noted in the

preceding paragraphs would apply, the Court notes this point as a procedural shortcoming in the regulatory framework.

343. Finally, the Court does not have sufficient information as to the manner in which the necessity to keep or destroy material containing personal data is assessed in practice and as to whether unprocessed intercept material is always stored for the maximum period of one year or the necessity of continued storage is regularly reviewed, as it should be. This makes it difficult to arrive at comprehensive conclusions covering all aspects of the storage and deletion of intercept material. In the context of its analysis on the *ex post facto* review in the Swedish bulk interception system, the Court will return to the question what conclusions could be drawn from the fact that it has insufficient information on the above point and other aspects of the functioning of the Swedish system.

344. In sum, for the purposes of the present stage of the analysis, while the Court noted in the preceding paragraph a procedural shortcoming that needs to be addressed, it considers that, as a whole, the circumstances in which the intercept material has to be destroyed are clear under Swedish law.

(8) Supervision

345. Under Swedish law the task of overseeing foreign intelligence activities in general and signals intelligence in particular is entrusted mainly to the Foreign Intelligence Inspectorate. Further supervisory functions, albeit with lesser powers, are exercised by the Data Protection Authority.

346. Noting that the Inspectorate's board is presided over by permanent judges or former judges and that its members, appointed for terms of at least four years by the Government, are selected from candidates proposed by the party groups in the Parliament, the Court is satisfied that the Inspectorate's role is that of an independent control mechanism.

347. The Inspectorate has wide-ranging powers covering the operation of signal intelligence activities from beginning to end. In particular, it is tasked with granting the FRA access to communications bearers after verifying that the requested access corresponds to the permit issued by the Foreign Intelligence Court (Chapter 6, section 19a of the Electronic Communications Act). The Inspectorate reviews all other aspects of the FRA's activities, including the interception, analysis, use and destruction of material. Importantly, it can scrutinise the selectors used (section 10 of the Signals Intelligence Act) and enjoys access to all relevant documents of the FRA (see paragraphs 50-53 above).

348. It appears therefore that the Inspectorate has the powers and tools necessary to assess not only compliance with the formal requirements of Swedish law but also to examine aspects of the proportionality of the interference with individual rights that may be occasioned by signals intelligence activities. It is noteworthy in this regard that its inspections

included numerous detailed examinations of, in particular, the selectors used (see paragraph 53 above).

349. The applicant pointed to the fact that some of the acts issued by the Inspectorate are in the form of opinions and recommendations, rather than legally binding decisions, and apparently considered that this weakened substantially the real impact of the Inspectorate's work.

350. The Court notes that under section 10 of the Signals Intelligence Act the Inspectorate, when it finds evidence of improper signals collection, has the power to decide, with legally binding effect, that the collection must cease or that recordings or notes of collected data must be destroyed. On certain other issues, such as potential civil liability of the State with respect to a person or organisation or where there is an indication that a criminal offence may have been committed, the Inspectorate has a duty to report to the competent authorities with which the power to take legally binding decisions lies. The Court considers the above arrangement to be satisfactory. While it is true that there appears to be no legal possibility under Swedish law for the enforcement of the Inspectorate's recommendations when it seeks the evolution or correction of practices by the FRA, the Court observes that, according to the conclusions of the National Audit Office which audited the Inspectorate in 2015, the FRA had routines in place for handling the Inspectorate's opinions, the latter's suggestions were dealt with in a serious manner and, when called for, gave rise to reforms. The action decided by the Inspectorate had been taken, with the exception of one case when the FRA had referred the matter to the Government (see paragraph 54 above).

351. Furthermore, the information available to the Court concerning the inspections conducted by the Inspectorate confirms that not only in theory but also in practice it actively reviews FRA's actions both on a general systematic basis and also by themes. In particular, over a period of eight years the Inspectorate has undertaken 102 inspections, including detailed examinations of the selectors used, the destruction of intelligence, the communication of reports, cooperation with other States and international organisations, the processing of personal data and the overall compliance with the legislation, directives and permits relevant to the signals intelligence activities. These resulted in several opinions and suggestions to the FRA and one opinion submitted to the Government. The effect of the Inspectorate's activity is illustrated by the fact that, for example, when it suggested in 2011 some amendments to the FRA's internal rules concerning destruction of data, these were introduced the same year (see paragraph 53 above).

352. Finally, the Inspectorate issues annual reports which are made available to the public and its activities have been the object of audits by the National Audit Office (see paragraphs 53 and 54 above).

353. In these circumstances, there is no reason to doubt that Swedish law and practice secure an effective supervision on signal intelligence activities in Sweden. In the Court's view, the Inspectorate's role, coupled with the judicial pre-authorisation procedure before the Foreign Intelligence Court, form together a functioning safeguard against abuse at the crucial stages of the signals intelligence process – before and during the process of interception, analysis, use and destruction of the information obtained.

(9) Ex post facto review

354. It appears undisputed that, due to secrecy, no use has ever been made in practice of the theoretical possibility under the Signals Intelligence Act to notify natural persons when selectors directly related to them have been employed (see paragraphs 58, 59, 75 *in fine* and 80 above).

355. In the Court's view, it is clear that notifying affected individuals in the context of the Swedish system of signals intelligence as part of foreign intelligence, if at all technically possible, might have far-reaching consequences that are difficult to foresee in advance. As already noted (see paragraph 272 above) a remedy which does not depend on notification to the interception subject could be an effective remedy in the context of bulk interception. The Court therefore accepts the respondent State's approach in this regard as being legitimate. However, the absence of a functioning notification mechanism should be counterbalanced by the effectiveness of the remedies that must be available to individuals who suspect that their communications may have been intercepted and analysed.

356. The Court notes in this regard that the Signals Intelligence Act provides for *ex post facto* review on the initiative of individuals or legal persons without them having to demonstrate that they may have been affected by a bulk interception operation. In reaction to a request by anyone, regardless of nationality and residence, the Foreign Intelligence Inspectorate must investigate if the person's communications have been intercepted through signals intelligence and, if so, verify whether the interception and treatment of the information have been in accordance with the law. As already noted (see paragraph 350 above), the Inspectorate has the power to decide that the signals intelligence operation shall cease or that the intelligence shall be destroyed.

357. The applicant pointed out that there is no possibility for an individual to be informed of whether his or her communications have actually been intercepted or, generally, to be given reasoned decisions. Under the relevant domestic law the Inspectorate informs the complainant only that an investigation has been carried out (see paragraph 61 above).

358. It transpires from the material available to the Court (see, in particular, paragraphs 61 and 203 above) that the Inspectorate regularly examines the requests submitted to it by individuals.

359. However, while it is true that the Inspectorate is an independent body, the Court observes that, having regard to that body's duty to supervise and monitor the FRA's activities, which includes taking or authorising operational decisions such as those concerning access to the signal carriers, use of selectors, analysis, use and destruction of intercept material (see paragraphs 50-53 above), the Inspectorate's additional role of *ex post facto* review on request from individuals may lead to situations where it will have to assess its own activities in supervising bulk interception by the FRA. In the conditions of secrecy, which legitimately characterise the relevant procedures, and failing a legal obligation for the Inspectorate to provide reasons to the individual concerned, there may be doubts as to whether the Inspectorate's examination of individual complaints in such situations affords adequate guarantees of objectivity and thoroughness. It cannot be excluded that the dual role of the Inspectorate may generate conflicts of interest and, therefore, the temptation to overlook an omission or misconduct in order to avoid criticism or other consequences.

360. The Court does not disregard in this respect the fact that the Inspectorate is itself subject to audits (paragraph 54 above), which could in principle be seen as a relevant safeguard. It notes, however, that the Government have not provided any information demonstrating that the audits conducted so far covered the Inspectorate's investigations undertaken at the requests of individuals seeking information as to whether their communications had been intercepted by the FRA. It appears that there is no legal obligation for the National Audit Office – which is responsible for auditing a significant number of administrative bodies in various sectors – to conduct such specific audits and to do so regularly. In these circumstances and having regard to the structural issue noted in the preceding paragraph, the Court is not convinced that the potential possibility of the National Audit Office examining the Inspectorate's handling of individuals' complaints is sufficient.

361. Furthermore, in the Court's view, a system of *ex post facto* review that does not produce reasoned decisions in response to complaints submitted by individuals, or at least decisions that contain reasons accessible to security-cleared special counsel, is too dependent on the initiative and perseverance of appointed officials operating away from the public eye. With regard to the Swedish system, the Court notes that no details are communicated to the complainant as to the content and outcome of the investigation conducted by the Inspectorate and, hence, the Inspectorate seems to be afforded wide discretion. A reasoned decision has the undeniable advantage of providing publicly available guidance on the interpretation of the applicable legal rules, the limits to be observed and the manner in which the public interest and individual rights are to be balanced in the specific context of bulk interception of communications. As noted by the Court in *Kennedy* (cited above, § 167), the publication of such legal

rulings enhanced the level of scrutiny in this area. These observations lead the Court to consider that the above-mentioned features of the Swedish system do not offer a sufficient basis for public confidence that abuses, if they occur, will be unveiled and remedied.

362. It is true that individuals can turn to the Parliamentary Ombudsmen and the Chancellor of Justice, who can scrutinise the authorities' actions for, *inter alia*, lawfulness and possible encroachment upon fundamental rights and freedoms. The Chancellor and the Ombudsmen have the power to initiate criminal or disciplinary proceedings (see paragraphs **Error! Reference source not found.**-68 above). While these are relevant complaint mechanisms, the Court notes that they do not seem to have been used frequently in the context of bulk interception of communications (see above, paragraph **Error! Reference source not found.** *in fine*). In any event, it is of the view that a legal procedure before an independent body, which in so far as possible offers an adversarial process resulting in reasoned and legally binding decisions, is an essential element of an effective *ex post facto* review. However, these conditions were met neither by the Chancellor nor the Ombudsmen.

363. Finally, the Court agrees with the applicant that the remedy available in the United Kingdom before the IPT (see *Big Brother Watch and Others*, cited above, §§ 413-15), illustrates that it is possible to reconcile legitimate security concerns and the need to ensure a reliable *ex post facto* control of bulk interception activities.

364. In sum, the Inspectorate's dual role and the absence of a possibility for members of the public to obtain reasoned decisions in some form in response to inquiries or complaints regarding bulk interception of communications, elements that are not in line with the requirements of an effective *ex post facto* review, must be seen as a shortcoming of the Swedish regime, to be taken into account in the Court's assessment of its compatibility with Article 8 of the Convention. In the Court's view, the above-mentioned shortcoming is particularly relevant having regard to the fact that the Court has insufficient information about the practice of the Foreign Intelligence Court on judicial pre-authorisation of strong selectors or categories of selectors (see paragraph 300 above) and on the manner in which the legal requirements on destruction of intercept material are applied in practice (see paragraph 343 above). This undoubtedly exacerbates the uncertainty for the individuals concerned as to whether arbitrariness or abuse concerning them might have occurred.

(10) Conclusion

365. The Court is in no doubt that bulk interception is of vital importance to Contracting States in identifying threats to their national security. This has been recognised, in particular, by the Venice Commission (see paragraph 86 above). It appears that, in present-day conditions, no

alternative or combination of alternatives would be sufficient to substitute for the bulk interception power.

366. The Court further reiterates that it is not its role to prescribe an ideal model for signals intelligence but rather to review for Convention compliance the existing legal and practical arrangements, which vary conceptually and functionally from one Contracting Party to another. In this exercise, the Swedish signals intelligence model and its safeguards against abuse must be seen as one whole.

367. The review of the Swedish bulk interception system in the present case has revealed that it is based on detailed legal rules, is clearly delimited in scope and provides for safeguards. The grounds upon which bulk interception can be authorised in Sweden are clearly circumscribed, the circumstances in which communications might be intercepted and examined are set out with sufficient clarity, its duration is legally regulated and controlled and the procedures for selecting, examining and using intercepted material are accompanied by adequate safeguards against abuse. The same protections apply equally to the content of intercepted communications and communications data.

368. Crucially, the judicial pre-authorisation procedure as it exists in Sweden and the supervision exercised by an independent body in Sweden serve in principle to ensure the application of the domestic legal requirements and the Convention standards in practice and to limit the risk of disproportionate consequences affecting Article 8 rights. Notably, regard must be had to the fact that in Sweden the limits to be observed in each bulk interception mission, as well as its lawfulness and proportionality in general, are the subject matter of judicial pre-authorisation proceedings before the Foreign Intelligence Court, which sits in the presence of a privacy protection representative defending the public interest.

369. The Court noted three shortcomings in the Swedish bulk interception regime: the absence of a clear rule on destroying intercepted material which does not contain personal data (see paragraph 342 above); the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration is given to the privacy interests of individuals (see paragraphs 326-330 above); and the absence of an effective *ex post facto* review (see paragraphs 359-364 above).

370. As regards the first of these shortcomings, its potential for causing adverse consequences on Article 8 rights is limited by the fact that Swedish law provides for clear rules on the destruction of intercept material in a number of circumstances and, above all, when it contains personal data.

371. However, the Court considers that the second shortcoming may potentially lead to very significant adverse consequences for affected individuals or organisations. As noted, the above-mentioned shortcoming may allow information seriously compromising privacy rights or the right to

respect for correspondence to be transmitted abroad mechanically, even if its intelligence value is very low. Such transmission may therefore generate clearly disproportionate risks for Article 8 Convention rights. Furthermore, no legally binding obligation is imposed on the FRA to analyse and determine whether the foreign recipient of intelligence offers an acceptable minimum level of safeguards.

372. Finally, the Inspectorate's dual role and the absence of a possibility for members of the public to obtain reasoned decisions in some form in response to inquiries or complaints regarding bulk interception of communications weakens the *ex post facto* control mechanism to an extent that generates risks for the observance of the affected individuals' fundamental rights. Moreover, the lack of an effective review at the final stage of interception cannot be reconciled with the Court's view that the degree of interference with individuals' Article 8 rights increases as the process advances (see paragraphs 239 and 245 above) and falls short of the requirement of "end-to-end" safeguards (see paragraph 264 above).

373. The Court is satisfied that the main features of the Swedish bulk interception regime meet the Convention requirements on quality of the law and considers that the operation of this regime at the time of the Chamber examination was therefore in most aspects kept within the limits of what is "necessary in a democratic society". It finds, however, that the shortcomings mentioned in the preceding paragraphs are not sufficiently compensated by the existing safeguards and that, therefore, the Swedish bulk interception regime oversteps the margin of appreciation left to the authorities of the respondent State in that regard. The Court reiterates that there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for private life (see paragraph 261 above). Therefore, having regard to rule of law principle, which is expressly mentioned in the Preamble to the Convention and is inherent in the object and purpose of Article 8 (see *Roman Zakharov*, cited above, § 228), the Court considers that the Swedish bulk interception regime, when viewed as a whole, did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse.

(d) Conclusion on Article 8

374. Having regard to the above conclusion concerning the lawfulness and justification of the impugned bulk interception regime, the Court finds that in the present case there has been a violation of Article 8 of the Convention.

III. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

375. The applicant complained that the remedies available under the Swedish bulk interception regime were insufficient and did not meet the requirements of Article 13 of the Convention. That provision reads as follows:

“Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.”

376. The Chamber found that no separate issue arose under that provision (see paragraph 184 of the Chamber judgment).

377. The Grand Chamber adopts the same conclusion, having regard to its finding above that there has been a violation of Article 8.

IV. APPLICATION OF ARTICLE 41 OF THE CONVENTION

378. Article 41 of the Convention provides:

“If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.”

A. Damage

379. The applicant stated that a finding of a violation would constitute sufficient redress. The Government agreed.

380. The Court accordingly makes no award under this head.

B. Costs and expenses

381. The applicant claimed 544,734 Swedish crowns (“SEK”) for 217 hours of legal work in the Chamber proceedings and 190 hours of legal work in the Grand Chamber proceedings (407 hours in total) at hourly rates ranging from SEK 1,302 to SEK 1,380.

382. The applicant also claimed travel and accommodation expenses for the attendance of its three representatives at the hearing before the Grand Chamber on 10 July 2019. These expenses amounted to SEK 8,669 for flight tickets and SEK 8,231 for hotel accommodation (SEK 16,900 in total). The applicant submitted copies of the relevant invoices.

383. The total amount claimed by the applicant was thus SEK 561,634 (the equivalent of approximately EUR 52,625).

384. The Government stated that they did not object to the claims made by the applicant but considered that if only one of the Convention Articles

covered by the complaint is found to be violated the reimbursement should be reduced accordingly.

385. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in the Court's possession and the above criteria and noting, in addition, that a violation of the Convention was found in respect of the applicant's main complaint, the complaint under Article 8, the Court considers it reasonable to award EUR 52,625 to cover costs and expenses under all heads.

C. Default interest

386. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT

1. *Rejects*, unanimously, the respondent Government's preliminary objection regarding the applicant's victim status.
2. *Holds*, by fifteen votes to two, that there has been a violation of Article 8 of the Convention;
3. *Holds*, unanimously, that it is not necessary to examine separately the complaint under Article 13 of the Convention;
4. *Holds*, unanimously,
 - (a) that the respondent State is to pay the applicant, with respect to costs and expenses, within three months EUR 52,625, plus any tax that may be chargeable to the applicant, to be converted into the currency of the respondent State at the rate applicable at the date of settlement;
 - (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points.

CENTRUM FÖR RÄTTVISA v. SWEDEN JUDGMENT

Done in English and in French, and delivered at a hearing on 25 May 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

{signature_p_1}

{signature_p_2}

Søren Prebensen
Deputy to the Registrar

Robert Spano
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

- (a) joint concurring opinion of Judges Lemmens, Vehabović and Bošnjak;
- (b) concurring opinion of Judge Pinto de Albuquerque;
- (c) joint declaration of vote of Judges Kjølbro and Wennerström.

R.S.O.
S.C.P.

JOINT CONCURRING OPINION OF JUDGES LEMMENS,
VEHABOVIĆ AND BOŠNJAK

In this case, we voted with the majority on all counts of the operative part. As in the connected case of *Big Brother Watch and Others v. the United Kingdom* (applications nos. 58170/13, 62322/14 and 24969/15) we consider that the judgment should go considerably further in upholding the importance of the protection of private life and correspondence, in particular by introducing stricter minimum safeguards, but also by applying those safeguards more rigorously to the impugned bulk interception regime. The arguments advanced in our concurring opinion in that case are largely applicable in this case too. In order to avoid unnecessary repetition, we refer the reader to that separate opinion. In so far as certain passages are not pertinent to the present case due to differences in the regulatory frameworks of the two bulk interception regimes, the reader should simply disregard them as irrelevant.

CONCURRING OPINION OF JUDGE PINTO DE ALBUQUERQUE

1. I voted with the majority, but for very different reasons. The Swedish legal framework of bulk interception is problematic in many aspects which the majority either disregarded or downplayed. The domestic practice is even worse. In fact, the domestic practice is highly opaque, even more so than in the United Kingdom. Yet the European Court of Human Rights (the Court) chose to adjudicate the case without being cognisant of important features of this practice, such as the actual practice regarding the keeping of logs and detailed records of each step in the bulk interception operations. Astonishingly, the Government was dispensed from the burden of presenting evidence of what they pleaded, because the Court simply assumed the veracity of the Government's pleadings¹. Even more baffling is the fact that the Court did not even have access to the relevant case-law of the competent domestic court in the field of bulk interception, ignoring for instance the actual interpretation of section 3 of the Signals Intelligence Act by the Foreign Intelligence Court (FIC)². Just as in the *Big Brother Watch and Others v. the United Kingdom* case (applications nos. 58170/13, 62322/14 and 24960/15), the Court's biased methodology, coupled with vague language, has led to a defective regime of safeguards in the present case³.

Legal purposes of bulk interception

2. The lack of foreseeability with regard to the legal purposes of bulk interception, as set out in the Signals Intelligence Act, stands out as the first major flaw of the Swedish regime. The purpose related to external military threats to the country may include "not only imminent threats, such as threats of invasion, but also phenomena that may in the long term develop into security threats"⁴. This is a highly undefined purpose, in terms both of its temporal and its spatial dimensions, allowing for profiling of foreigners, minorities and legitimate businesses that may be considered as long-term potential threats.

¹ See paragraph 311 of this judgment: "there is no reason to consider that detailed logs and records are not kept in practice or that the FRA could proceed to changing its internal instructions arbitrarily and removing its obligation in that regard".

² See paragraph 300 of this judgment: "The interpretation of section 3 of the Signals Intelligence Act in the practice of the Foreign Intelligence Court has not been explained to the Court". I will return to this point below.

³ For a critique of the Court's *pro autoritate* regime of bulk interception, I refer to my opinion in the *Big Brother Watch and Others* case.

⁴ See paragraph 23 of this judgment.

3. The purpose related to strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests, including “drug or human trafficking of such severity that it may threaten significant national interests”⁵, does not delimit serious cross-border crime sufficiently. The concept of serious crime as it exists in international law encompasses offences punishable with imprisonment for a term of four or more years⁶. Hence, to be foreseeable, the concept of serious offences that may trigger bulk interception must be linked either to a list of specific serious offences or, generally, to offences punishable by four or more years’ imprisonment. That is not the case in Sweden.

4. The purpose related to the development and proliferation of weapons of mass destruction, military equipment and other similar specified products may include, “among other things, activities relevant to Sweden’s commitments in regard to non-proliferation and export control, even in cases where the activity does not constitute a crime or contravenes international conventions”⁷. According to information officially provided by the Government,⁸ “similar specified products” includes munitions and military and civil dual-use products and even technical assistance, as provided for in Law no, 1064 (2000) on control of products with dual uses and technical assistance. However, the monitored activities (“among other things”) are not sufficiently defined. Is economic and trade espionage for the benefit of the Swedish arms, aerospace, electronics, petrochemical and other manufacturing industry included in this purpose?

5. The purpose related to serious external threats to societal infrastructure “includes, among other things, serious IT-related threats emanating from abroad. That the threats should be of a serious nature means that they, for example, should be directed towards vital societal systems for energy and water supply, communication or monetary services.”⁹ Neither the types of threats (“among other things”) nor the societal infrastructure systems that may be threatened (“for example”) are sufficiently delimited. Does this purpose mean, for example, that a general strike in a neighbouring country that might ultimately disturb and derail the Swedish energy or petroleum distribution system may justify surveillance of the trade unions involved in the strike, and of their members? What if the supposed “threat” is directed against the Swedish public transportation and sports systems?

⁵ Ibid.

⁶ Article 2 (b) of the UN Convention against Transnational Organized Crime defines “serious crime” as conduct punishable by a maximum deprivation of liberty of at least four years or by a more serious penalty. The Explanatory Report on Recommendation Rec(2005)10 of the Committee of Ministers of the Council of Europe follows that approach (see its paragraph 20).

⁷ See paragraph 23 of this judgment.

⁸ <https://www.loc.gov/law/help/foreign-intelligence-gathering/sweden.php#Signal>

⁹ See paragraph 23 of this judgment.

Does the massive movement of foreign football fans for a football championship in Sweden justify monitoring all football fans from the countries involved in the championship?

6. The purpose related to actions or intentions of a foreign power that are of substantial importance for the Swedish foreign, security or defence policy is very broadly phrased. It is clarified that “it is not sufficient that the phenomenon is of general interest but that the intelligence should have a direct impact on Swedish actions or positions in various foreign, security or defence policy matters”¹⁰, but this clarification is insufficient, since it does not delimit the threshold of materiality and the specific subject matters at stake. It is also worrying that even the “intentions” of a foreign power may justify the launching of a surveillance campaign, which opens the door for monitoring of “alien” philosophical and religious *Weltanschauungen*. Monitoring of the “causes”¹¹ of ethnic, religious and political conflicts, which is included in the purpose related to foreign conflicts with consequences for international security, feeds into this same updated Orwellian policy of thought control¹².

7. The purpose related to “development activities”¹³ is a true legal black hole, which has allowed for the interception and analysis of communications which do not fall within the eight foreign-intelligence purposes¹⁴. This is a blank cheque for monitoring “large segments of the international signals traffic”¹⁵. The Government’s argument that these data do not generate any intelligence reports but are vital in order to monitor the “ever-changing signals environment, technical developments and signals protection”¹⁶ is tantamount to saying that all internet communication should be scrutinised so that the FRA can keep pace with the ever-changing internet environment, technical developments and internet protection. This is evidently absurd, but in practical terms it is what the Government is claiming. The purposeless (that is, beyond the eight purposes of the law)

¹⁰ Ibid.

¹¹ Ibid.

¹² Likewise, the United Nations Human Rights Committee (HRC) Concluding observations on the seventh report of Sweden, 28 April 2016, CCPR/C/SWE/CO/7, § 36, expressed concern about “the limited degree of transparency with regard to the scope of surveillance powers and the safeguards on their application”. I would point out that the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 22 February 2016, A/HRC/31/65, § 43, was of the opinion that “effective strategies should not be based on pre- or mis-conceptions about the groups that are most susceptible to radicalisation or violent extremism, but should be developed in reliance on evidence to ensure a proper understanding of the national and local issues that impact on the radicalisation process.”

¹³ See paragraph 24 of this judgment.

¹⁴ As concluded by the report of the Signals Intelligence Committee (in paragraph 79 of this judgment).

¹⁵ See paragraph 292 of this judgment.

¹⁶ The Government’s pleadings during the Grand Chamber hearing on 10 July 2019.

gathering of such an unlimited amount of data represents *per se* a disproportionate interference with Articles 8 and 10 of the European Convention on Human Rights (the Convention).

8. Finally, it is also a matter of concern that the ever-increasing powers of law-enforcement agencies (such as the Security Policy and the National Operative Department of the Police Authority) to commission signals intelligence and access collected data or intelligence reports endangers the finality principle underlying the Swedish bulk interception regime, that is, that data must be collected and processed for one or more legal purposes, and may not be used in a way inconsistent with that or those purposes, namely they may not be used for law-enforcement purposes in ongoing criminal proceedings. As a matter of fact, the FII itself warned recently that law-enforcement agencies would not be able to keep information received from the FRA separate from their law-enforcement activities¹⁷.

Authorisation of bulk interception

9. Swedish law entrusts the authorisation of bulk surveillance to a court. But the FIC is not an ordinary court. Herein lies the second major shortcoming in the Swedish system. The FIC’s composition consists of one president, one or two vice-presidents and two to six lay members, mainly former politicians¹⁸, all of whom are appointed by the Government for a four-year mandate. Their appointment is renewable, which strengthens their political bond to the Government. Even the privacy protection representative, who is supposed to act in the public interest, but not in the interest of any affected individual, is a Government appointee, with a renewable mandate. Furthermore, his or her intervention can be dispensed with. If the matter is so urgent that a delay would seriously jeopardize the purpose of the application, a meeting may be held, and a decision taken, without a privacy protection representative having been present or otherwise given an opportunity to comment. The highly politicised status of the FIC’s members is consonant with the fact that it has never held a public hearing and its decisions are final and confidential¹⁹. In view of these characteristics the FIC is more akin to a political body than to a truly independent judicial authority²⁰.

¹⁷ See the reference to the FII’s position in the applicant’s observations before the Grand Chamber of 3 May 2019, p. 24, not disputed by the Government.

¹⁸ See the Venice Commission Report on the democratic oversight of signals intelligence agencies, 2015, p. 33.

¹⁹ It is beyond my understanding that the majority reproach the FII (which is not a court) for not delivering public decisions but are ready to accept that the FIC (which is a court) does not deliver public decisions (compare and contrast paragraphs 297 and 372 of this judgment).

²⁰ The Venice Commission considered it a “hybrid body” (Venice Commission Report, cited above, p. 33). That is why the HRC asked the Swedish State to ensure that “effective

10. The FIC’s oversight encompasses assessment of the specific “bearers” (signal carriers) to which the FRA will have access, as well as the “selectors” (search terms) and the categories of selectors that will be used for the automatic collection of data, and the duration of the surveillance permit. But there is no requirement that the permit must be cancelled if the collection of the communication ceases to be necessary²¹ or that intercepted material which does not contain personal data must be destroyed within a certain period²². Nor is there any requirement that the FIC verify the existence of reasonable suspicion in relation to any person targeted. It is true that strong selectors directly relating to a specific person may be used if this is of “exceptional importance” for the intelligence activities²³, but this restriction only applies to the automated collection of data, not to the selectors used to search the bulk collected data. This means that the law allows for a large degree of discretion in the collection and search of communications and related communications data by the FRA, especially when the FIC’s permit refers to categories of selectors²⁴. The problem of a lack of specificity with regard to the selectors seems to be even more serious regarding the selectors used for related communications data²⁵.

11. Furthermore, there is no evidence that the FIC can and does assess the need to protect privileged communications, including situations where

and independent oversight mechanisms over intelligence-sharing of personal data are put in place” (United Nations Human Rights Committee Concluding observations, cited above, § 37). This is not an isolated case in Europe. The European Union’s Fundamental Rights Agency (FRA of the EU) identified the following shortcomings in the EU states: “the findings also identified limits to full independence, with some oversight bodies remaining strongly dependent on the executive: the law does not grant them binding decision-making powers, they have limited staff and budget, or their offices are located in government buildings.” (FRA, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, volume II: Field perspectives and legal updates, 2017, p. 11).

²¹ The majority neglect the importance of this flaw, confusing the “existence of supervision mechanisms” with the provision of a specific substantive guarantee that mandates the cessation of unnecessary interception measures (see paragraph 336 of this judgment).

²² The majority consider the rules pertaining to the destruction of intercepted material containing personal data sufficiently clear “as a whole”, ignoring the regulatory omission regarding material which does not contain personal data (see paragraph 344 of this judgment).

²³ I find it puzzling that the majority are willing to accept that the “exceptional importance standard” for the authorisation of strong selectors is “capable of providing relevant enhanced protection” when they have no clue about how the FIC applies this standard (see paragraph 300 of this judgment). This amounts to a blank cheque for the FIC and to the Government.

²⁴ The majority rightly acknowledge this, admitting that “it may be difficult” to appreciate the proportionality aspect when only categories of selectors are specified in the FRA’s request for a permit (see paragraph 301 of this judgment). That is precisely why bulk interception based on categories of selectors should not be admissible (see my separate opinion in *Big Brother Watch and Others*, cited above).

²⁵ As concluded by the report of the Signals Intelligence Committee (see paragraph 78 of this judgment) and acknowledged by the Government (see paragraph 220 of this judgment).

there is a reasonable probability that such communications will be intercepted as a by-catch of the requested interception. Privileged communications, such as those related to media sources and attorney-client privilege, are protected only to the extent that they ought to be destroyed if they have been intercepted. The fact that not even communications in a religious context of confession or individual counselling are protected, since they may be intercepted and exceptionally examined, is quite disturbing.

Supervision of the implementation of the interception permit

12. The FIC does not oversee the implementation of the bulk interception permit, nor even the intended subsequent use of the intercepted communication, this task being assigned to the Foreign Intelligence Inspectorate (FII). As with the FIC, the composition of the FII's board is dependent on the Government. The Government appoints its members for a renewable four-year mandate, the president and the vice-president being or having been permanent judges and the other four lay members chosen from among former politicians proposed by party groups represented in Parliament²⁶. The FII works part-time²⁷, assisted by a "small secretariat"²⁸.

13. The FII does not have powers to determine, by means of a legally binding decision, whether the FIC's permit is lawful, nor to order a rectification of the FRA's practices or a reform of its internal rules, nor to grant compensation, but it can decide that an operation should cease or that the intercepted material should be destroyed if it did not comply with the relevant permit. The FII cannot take any legally binding decisions relating to breaches of the Convention, the Swedish Constitution or the FRA Personal Data Processing Act. Instead, it may report the matter to the Data Protection Authority.

14. The Data Protection Authority has a general supervisory function in respect of the protection of personal data. In the exercise of its function, it has access to personal data processed by the FRA and the relevant documentation as well as to the facilities where they are kept. The Data Protection Authority cannot itself take any legally binding decisions with respect to the FRA and is under no obligation to take any action upon receiving a report from the FII. If it chooses to act, all that the Data Protection Authority can do is to communicate its views to the FRA, or to apply to the Administrative Court for the destruction of illegally processed personal data, but to date it has never used this power²⁹.

²⁶ The Venice Commission considered the FII a "hybrid body", just as it did regarding the FIC (Venice Commission report, cited above, p. 33).

²⁷ As the Government admitted in the Grand Chamber hearing on 10 July 2019.

²⁸ As described by the Venice Commission report, cited above, p. 33.

²⁹ See paragraph 57 of this judgment.

15. Lastly, in terms of internal oversight, the Privacy Protection Council of the FRA, which is tasked with monitoring the measures taken to protect personal integrity, is also composed of members appointed by the Government. This body appears to be toothless, as evidenced by the fact that the Data Protection Authority unsuccessfully reproached the FRA in 2010 and 2016 for failing to monitor adequately logs used to detect unwarranted use of personal data³⁰. The alleged introduction in 2018 of a central function for monitoring and following up logs, invoked by the Government, does not suffice. In fact, there is no legal obligation on the FRA to keep logs and detailed records of each step in bulk interception operations, including interception, subsequent use and communication of data. This means that any record-keeping practice, if it exists, essentially depends on internal procedures and discretion.

Remedies

16. The lack of truly independent authorisation for and supervision of the implementation of bulk interception measures is aggravated by the purely virtual character of the remedies available to the intercept subject³¹. The law provides for notification of bulk interception to the intercept subject, when selectors directly related to an individual have been used and secrecy reasons do not prevail. The guarantee pertains only to natural persons, not to legal persons such as the applicant. In any event, this law remains a dead letter³².

17. In addition, at the request of a natural or legal person, the FII may investigate whether the interception and treatment of intercept material have been in accordance with the law, and it has done so. Astonishingly, in all 132 cases investigated by the FII it never once found in favour of the applicant party³³. The simple reason for this is that the FII is *iudex in causa*

³⁰ See paragraph 76 of this judgment.

³¹ The FRA of the EU has emphasised that the effectiveness of remedies depends on the capacity to issue legally binding decisions, which at a minimum should include the power to order termination of the surveillance, destruction of unlawfully collected data and payment of the appropriate compensation (FRA, Surveillance by intelligence services, cited above, p. 114).

³² See paragraphs 60 and 80 of this judgment. In fact, the HRC asked the Swedish State to ensure “that affected persons have proper access to effective remedies in cases of abuse.” (United Nations Human Rights Committee Concluding observations, cited above, § 37).

³³ See paragraph 61 of this judgment. In § 218 of this judgment, reference is made to 141 controls at the request of individuals, none of which ever showed “improper signals collection”. It is not clear what the majority seek to demonstrate in this regard. On the one hand they admit that decisions may be notified to a “security-cleared special counsel” but on the other hand they require that the decision be “publicly available” and criticise the “absence of a possibility for members of the public to obtain reasoned decisions in some form in response to inquiries” (compare and contrast paragraphs 361 and 372 of this judgment).

sua, in that it is asked to review its own overseeing conduct, without even having to inform the complainant of its findings or provide any reasons for its decisions³⁴. The FII’s working methods are not far from the dark tenebrous process described by Franz Kafka.

18. Furthermore, individuals can make requests to the FRA for disclosure and correction in regard to processed personal data, and the FRA’s decisions to disclose information may be appealed against to the Administrative Court. Yet domestic rules on secrecy may hamper the individual’s access to that information³⁵, not to mention the Administrative Court’s *de facto* powers to review the FRA’s own secrecy assessment. This “Catch 22” situation is evidenced by the fact that this possibility has never been used³⁶. In any event, this legal avenue is not available to legal persons such as the applicant.

19. Finally, neither the Parliamentary Ombudsmen nor the Chancellor of Justice provide any effective scrutiny, since they are not entitled to produce legally binding decisions to cease any interception activities or to destroy any intercepted material. As a matter of fact, neither of them has ever found it necessary to act within their remit, for example by triggering criminal or disciplinary proceedings against FRA officials³⁷ or, in the case of the Chancellor, by awarding compensation.

Transfer of intercept data to foreign intelligence services

20. Regarding the transfer of intercept material to foreign third parties, the sole guarantee provided by law is that it should be in the national interest. There is no requirement to consider privacy rights or to guarantee that the receiving State has similar safeguards to those applicable in Sweden. Where the remit of the intercepting authority is framed in such broad terms in the legislation, and oversight is limited to checking if the authority remains within its statutory remit, the oversight is of very limited use³⁸.

³⁴ This has nothing to do with the European Union standard as stated in FRA of the EU, Surveillance by intelligence services, cited above, p. 14: “EU Member States should ensure that judicial and non-judicial bodies with remedial powers have the powers and competences to effectively assess and decide on individuals’ complaints related to surveillance... In particular, the remedial body should have access to the premises of intelligence services and the data collected; be given the power to issue binding decisions; and inform complainants on the outcome of its investigations. The individual should be able to appeal the body’s decision.”

³⁵ As the chamber itself admitted (see § 175 of the Chamber judgment).

³⁶ See paragraph 64 of this judgment.

³⁷ See paragraphs 66-8 of this judgment.

³⁸ Swedish law is very far from the universal standard described by the United Nations Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, 17 May 2010 (A/HRC/14/46): “Practice 31. Intelligence-

21. The Government's argument that international cooperation is conditional on the receiving State respecting Swedish legislation is not evidenced in any national legislation. In fact, the Government only refers to the "FRA's general guidelines"³⁹. As a matter of law, the FRA is only required to inform the FII of the principles governing its foreign intelligence cooperation and to which countries or organisations it transfers data and to provide general information on the operations. Since no oversight body is vested with powers to exercise actual control over whether or not foreign intelligence cooperation is being used to circumvent national law, and the recipient States protect the data with the same or similar safeguards as those under Swedish law, the FII's monitoring of the FRA's international cooperation activities, invoked by the Government, is irrelevant⁴⁰.

22. The Government's position is even less acceptable because it is inconsistent with Sweden's international obligations, not only in view of its obligations *vis-a-vis* the European Union⁴¹, but also the Council of Europe. In addition to the Convention, Article 2 of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS no. 181), which Sweden has ratified, states that parties must ensure an adequate level of protection for personal data transfers to third countries, and that derogations are admitted only when there are legitimate prevailing interests. The Explanatory Report to this Additional Protocol adds that exceptions must be interpreted restrictively, "so that the exception does not become the rule" (§ 31). This is precisely what is happening in Sweden.

sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence." See also Practices 32-35.

³⁹ See paragraph 216 of this judgment.

⁴⁰ See also the United Nations Human Rights Committee Concluding observations, cited above, § 36, where the Committee raised specific concerns with regard to "the lack of sufficient safeguards against arbitrary interference with the right to privacy in relation to the sharing of data with other intelligence agencies."

⁴¹ FRA of the EU, Surveillance by intelligence services, cited above, p. 13: "EU Member States should define rules on how international intelligence sharing takes place. These rules should be subject to review by oversight bodies, which should assess whether the processes for transferring and receiving intelligence respect fundamental rights and include adequate safeguards... EU Member States should ensure that legal frameworks regulating intelligence cooperation clearly define the extent of oversight bodies' competences in the area of intelligence services cooperation."

Conclusion

23. In sum, the Swedish oversight bodies either do not meet the requirement of sufficient independence or provide effective scrutiny, or both. With its concealed procedure and unappealable and secret decisions, the FIC is not a court administering justice in the name of the Swedish people and accountable to it. It is a secretive commission of political appointees which produces a restricted diktat that cannot be appealed against. It serves one sole purpose: to whitewash the FRA's choices, which in reality means, the Government's own surveillance policy choices, giving the Swedish people the deceitful impression that there is a court in Stockholm taking care of privacy rights.

24. The FII is no better. When asked to investigate whether interception and processing of communications have taken place in accordance with the law, it decides *in causa sua*, without even being under an obligation to inform the complainant of its findings or to provide reasons for its decisions. The complainant is treated as a subject, deprived of privacy rights, in the hands of the Kafkian all-mighty State, not as a person empowered with rights before and against the State.

25. The Swedish full-take approach to the international exchange of intercept data between intelligence services is more dangerous to civil rights and democratic government than a targeted one.

26. Instead of the proliferation of oversight bodies with virtual powers, it would be wiser to have a fully-fledged independent court of law, composed of senior judges, with the power to provide effective, end-to-end control of the interception process, that is, to authorise and supervise on a regular basis the implementation of suspicion-based, targeted bulk interception measures and to stop unlawful collection and retention of the intercepted data, with the necessary access to classified documents pertaining to the exercise of their function⁴².

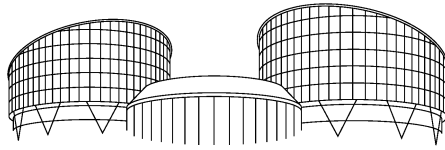
27. Arguments about the impracticality of the above-mentioned standard ought to be dismissed outright: the issue at stake is not a matter of practical effectiveness but of the rule of law. It is the law that sets the boundaries of effective public service, not the other way around. But that can only be discerned when, like Caspar David Friedrich's Wanderer, one rises above the sea of fog enveloping the Government's discourse.

⁴² See my separate opinion in *Big Brother Watch and Others v. the United Kingdom*, where the requirements for a Convention-compatible bulk interception regime are discussed.

JOINT DECLARATION OF VOTE OF JUDGES KJØLBRO
AND WENNERSTRÖM

1. We voted for finding no violation of Article 8 of the Convention and, therefore, we distance ourselves from the Court's reasoning and findings concerning intelligence sharing (see §§ 317-330) and *ex post facto* control (see §§ 354-364).

2. Having regard to the nature of the issue decided by the Court, the importance of the Court's judgment, the large majority for finding a violation of Article 8 of the Convention and also having regard to the reasoning in the unanimous Chamber judgment, we will refrain from elaborating on our legal arguments in this case and will limit ourselves to this declaration of vote.



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF CENTRUM FÖR RÄTTVISA v. SWEDEN

(Application no. 35252/08)

JUDGMENT

STRASBOURG

19 June 2018

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Centrum för Rättvisa v. Sweden,

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Branko Lubarda, *President*,

Helena Jäderblom,

Helen Keller,

Pere Pastor Vilanova,

Alena Poláčková,

Georgios A. Serghides,

Jolien Schukking, *judges*,

and Stephen Phillips, *Section Registrar*,

Having deliberated in private on 29 May 2018,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 35252/08) against the Kingdom of Sweden lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by Centrum för Rättvisa on 14 July 2008.

2. The Swedish Government (“the Government”) were represented by their Agent, Mr A. Rönquist, Ministry for Foreign Affairs.

3. The applicant alleged that Swedish legislation and practice in the field of signals intelligence have violated and continue to violate its rights under Article 8 of the Convention. It also complained that it has had no effective domestic remedy through which to challenge this violation.

4. On 1 November 2011 (admissibility) and 14 October 2014 (admissibility and merits) the application was communicated to the Government.

5. On 14 October 2014 the International Commission of Jurists, Norwegian Section, was granted leave to submit written comments, under Rule 44 § 3 of the Rules of the Court.

THE FACTS

I. INTRODUCTION

6. The applicant, Centrum för Rättvisa, is a Swedish foundation which was established in 2002 and which has its seat in Stockholm. A not-for-profit organisation, its stated objective is to represent clients, in

litigation against the State and otherwise, who claim that their rights and freedoms under the Convention and under Swedish law have been violated. It also conducts education and research and participates in the general debate on issues concerning individuals' rights and freedoms. The applicant communicates on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax and asserts that a large part of that communication is particularly sensitive from a privacy perspective. Due to the nature of its function as a non-governmental organisation scrutinising the activities of State actors, it believes that there is a risk that its communication through mobile telephones and mobile broadband has been or will be intercepted and examined by way of signals intelligence. The applicant has not brought any domestic proceedings, contending that there is no effective remedy for its Convention complaints.

7. Signals intelligence can be defined as intercepting, processing, analysing and reporting intelligence from electronic signals. These signals may be processed to text, images and sound. The intelligence collected through these procedures may concern both the content of a communication and its associated communications data (the data describing, for instance, how, when and between which addresses the electronic communication is conducted). The intelligence may be intercepted over the airways – usually from radio links and satellites – and from cables. Whether a signal is transmitted over the airways or through cables is controlled by the communications service providers. A great majority of the traffic relevant for signals intelligence is cable-based. The term “signal carriers” refers to the medium used for transmitting one or more signals. Unless indicated in the following, the regulation of Swedish signals intelligence does not distinguish between the content of communications and their communications data or between airborne and cable-based traffic.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. Generally on signals intelligence

8. Foreign intelligence is, according to the Foreign Intelligence Act (*Lagen om försvarsunderrättelseverksamhet*; 2000:130), conducted in support of Swedish foreign, defence and security policy, and in order to identify external threats to the country. The activities should also assist in Sweden's participation in international security cooperation. Intelligence under the Act may only be conducted in relation to foreign circumstances (section 1(1)). The Government determines the direction of the activities; it also decides which authorities may issue more detailed directives and which authority is to conduct the intelligence activities (section 1(2) and 1(3)). The Government issues general tasking directives annually. Foreign intelligence may not be conducted for the purpose of solving tasks in the area of law

enforcement or crime prevention, which come under the mandate of the Police Authority, the Security Police and other authorities and which are regulated by different legislation. However, authorities that conduct foreign intelligence may support authorities dealing with law enforcement or crime prevention (section 4). Examples of such support are cryptanalysis and technical help on information security (preparatory works to amended legislation on foreign intelligence, prop. 2006/07:63, p. 136).

9. The collection of electronic signals is one form of foreign intelligence. It is regulated by the Signals Intelligence Act (*Lagen om signalspaning i försvarsunderrättelseverksamhet*; 2008:717), which entered into force on 1 January 2009. Several amendments were made to the Act on 1 December 2009, 1 January 2013, 1 January 2015 and 15 July 2016. Supplementary provisions are found in the Signals Intelligence Ordinance (*Förordningen om signalspaning i försvarsunderrättelseverksamhet*; 2008:923). The legislation authorises the National Defence Radio Establishment (*Försvarets radioanstalt*; henceforth “the FRA”) to conduct signals intelligence (section 2 of the Ordinance compared to section 1 of the Act). During signals intelligence all cable-based cross-border communications are transferred to certain points of collection. No information is stored at these points and a limited amount of data traffic is transferred to the FRA by signals carriers (parliamentary committee report SOU 2016:45, p. 107) The FRA may conduct signals intelligence within the area of foreign intelligence only as a result of a detailed tasking directive issued by the Government, the Government Offices, the Armed Forces and, as from January 2013, the Security Police and the National Operative Department of the Police Authority (*Nationella operativa avdelningen i Polismyndigheten*; hereafter “NOA”) (sections 1(1) and 4(1) of the Act) in accordance with the issuer’s precise intelligence requirements. However, the direction of the FRA’s “development activities” (see further paragraph 14 below) may be determined solely by the Government (section 4(2)). A detailed tasking directive determines the direction of the intelligence activities and may concern a certain phenomenon or situation, but it may not solely target a specific natural person (section 4(3)).

10. The mandate of the Security Police and the NOA to issue detailed tasking directives aims to improve these authorities’ ability to obtain data about foreign circumstances at a strategic level concerning international terrorism and other serious international crime that may threaten essential national interests. At the time of introduction of the new rules, the Government stated in the preparatory works (prop. 2011/12:179, p. 19) that the mandate is in accordance with the prohibition on conducting signals intelligence for the purpose of solving tasks in the area of law enforcement or crime prevention.

11. According to the Foreign Intelligence Ordinance (*Förordningen om försvarsunderrättelseverksamhet*; 2000:131), a detailed tasking directive

shall include information about 1) the issuing authority, 2) the part of the Government's annual tasking directive it concerns, 3) the phenomenon or situation intended to be covered, and 4) the need for intelligence on that phenomenon or situation (section 2a).

B. Scope of application of signals intelligence

12. The purposes for which electronic signals may be collected as part of foreign intelligence are specified in the Signals Intelligence Act which provides that signals intelligence may be conducted only to survey 1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society's infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy (section 1(2)).

13. These eight purposes are further elaborated upon in the preparatory works to the legislation (prop. 2008/09:201, pp. 108-109):

“The purposes for which permits to conduct signals intelligence may be granted are listed in eight points. The first point concerns external military threats to the country. Military threats include not only imminent threats, such as threats of invasion, but also phenomena that may in the long term develop into security threats. Consequently, the wording covers the surveying of military capabilities and capacities in our vicinity.

The second point comprises both surveying necessary to provide an adequate basis for a decision whether to participate in international peacekeeping or humanitarian missions and surveying performed during ongoing missions concerning threats to Swedish personnel or other Swedish interests.

The third point refers to strategic surveying of international terrorism or other serious cross-border crime, such as drug or human trafficking of such severity that it may threaten significant national interests. The task of signals intelligence in relation to such activities is to survey them from a foreign and security policy perspective; the intelligence needed to combat the criminal activity operatively is primarily the responsibility of the police.

The fourth point addresses the need to use signals intelligence to follow, among other things, activities relevant to Sweden's commitments in regard to non-proliferation and export control, even in cases where the activity does not constitute a crime or contravenes international conventions.

The fifth point includes, among other things, serious IT-related threats emanating from abroad. That the threats should be of a serious nature means that they, for

example, should be directed towards vital societal systems for energy and water supply, communication or monetary services.

The sixth point refers to the surveying of such conflicts between and in other countries that may have consequences for international security. It may concern regular acts of war between states but also internal or cross-border conflicts between different ethnic, religious or political groups. The surveying of the conflicts includes examining their causes and consequences.

The seventh point signifies that intelligence activities conducted against Swedish interests can be surveyed through signals intelligence.

The eighth point provides the opportunity to conduct signals intelligence against foreign powers and their representatives in order to survey their intentions or actions that are of substantial importance to Swedish foreign, security or defence policy. Such activities may relate only to those who represent a foreign power. Through the condition “substantial importance” it is emphasised that it is not sufficient that the phenomenon is of general interest but that the intelligence should have a direct impact on Swedish actions or positions in various foreign, security or defence policy matters. ...”

14. The FRA may collect electronic signals also in order to monitor changes in the international signals environment, technical advances and signals protection and to develop the technology needed for signals intelligence (section 1(3)). This is regarded as “development activities” and, according to the relevant preparatory works (prop. 2006/07:63, p. 72), they do not generate any intelligence reports. However, the FRA may share experiences gained on technological issues with other authorities. Development activities usually do not focus on communications between individuals, though information on individuals’ identities may be intercepted.

15. Signals intelligence conducted on cables may only concern signals crossing the Swedish border in cables owned by a communications service provider (section 2). Communications between a sender and receiver within Sweden may not be intercepted, regardless of whether the source is airborne or cable-based. If such signals cannot be separated at the point of collection, the recording of or notes about them shall be destroyed as soon as it becomes clear that such signals have been collected (section 2a).

16. Interception of cable-based signals is automated and must only concern signals that have been identified through the use of search terms. Such terms are also used to identify signals over the airways, if the procedure is automated. The search terms must be formulated in such a way that the interference with personal integrity is limited as far as possible. Terms directly relating to a specific natural person may only be used if this is of exceptional importance for the intelligence activities (section 3).

17. After the signals have been intercepted they are processed, which means that they are, for example, subjected to cryptanalysis or translation. Then the information is analysed and reported to the authority that gave the FRA the mission to collect the intelligence in question.

C. Authorisation of signals intelligence

18. For all signals intelligence, including the development activities, the FRA must apply for a permit to the Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*). The application shall contain the mission request that the FRA has received, with information on the relevant detailed tasking directive and the need for the intelligence sought. Also, the signal carriers to which the FRA requires access have to be specified, along with the search terms or categories of search terms that will be used. Finally, the application must state the duration for which the permit is requested (section 4a).

19. A permit may only be granted if the mission is in accordance with the provisions of the Foreign Intelligence Act and the Signals Intelligence Act, if the purpose of the interception of signals cannot be met in a less interfering manner, if the mission can be expected to yield information whose value is clearly greater than the possible interference with personal integrity, if the search terms or categories of search terms are in accordance with the Signals Intelligence Act and if the application does not concern solely a specific natural person (section 5).

20. If granted, the permit shall specify the mission for which signals intelligence may be conducted, the signal carriers to which the FRA will have access, the search terms or categories of search terms that may be used, the duration of the permit and other conditions necessary to limit the interference with personal integrity (section 5a).

21. The FRA itself may decide to grant a permit, if the application for a permit from the Foreign Intelligence Court might cause delay or other inconveniences of essential importance for one of the specified purposes of the signals intelligence. If the FRA grants a permit, it has to report to the court immediately and the court shall without delay decide in the matter. The court may revoke or amend the permit (section 5b).

22. The composition of the Foreign Intelligence Court and its activities are regulated by the Foreign Intelligence Court Act (*Lagen om Försvarsunderrättelsedomstol*; 2009:966). The court consists of one president, one or two vice-presidents and two to six other members. The president is a permanent judge, nominated by the Judges Proposals Board (*Domarnämnden*) and appointed by the Government. The vice-presidents, who must be legally trained and have previous experience as judges, and the other members, who are required to have special expertise of relevance for the court's work, are appointed by the Government on four-year terms. The applications for signals intelligence permits are discussed during hearings, which may be held behind closed doors, if it is clear that information classified as secret would be exposed as a result of a public hearing. During the court's examination, the FRA as well as a privacy protection representative (*integritesskyddsombud*) are present. The representative, who

does not represent any particular person but the interests of individuals in general, monitors integrity issues and has access to the case file and may make statements. Privacy protection representatives are appointed by the Government for a period of four years and must be or have been permanent judges or attorneys. The court may hold a hearing and decide on an application without the presence of a representative only if the case is of such urgency that a delay would severely compromise the purpose of the application. The court's decisions are final.

D. The duration of signals intelligence

23. A permit may be granted for a specific period of time, maximum six months. An extension may, after a renewed examination, be granted for six months at a time (Signals Intelligence Act, section 5a).

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

24. The Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten* (SIUN); see further paragraphs 36-40 below) oversees access to the signal carriers. Communications service providers are obliged to transfer cable-based signals crossing the Swedish borders to "collaboration points" agreed upon with the Inspectorate. The Inspectorate, in turn, provides the FRA with access to signal carriers in so far as such access is covered by a signals intelligence permit and, in so doing, implements the permits issued by the Foreign Intelligence Court (Chapter 6, section 19a of the Electronic Communications Act (*Lagen om elektronisk kommunikation*; 2003:389)). The Council on Legislation (*Lagrådet*), the body giving opinions on request by the Government or a Parliamentary committee on certain draft bills, has expressed the view that an interference with private life and correspondence presents itself already at this point, because of the State obtaining access to the telecommunications (prop. 2006/07:63, p. 172).

25. According to the Signals Intelligence Act, intercepted data must be destroyed immediately by the FRA if it 1) concerns a specific natural person and lacks importance for the signals intelligence, 2) is protected by constitutional provisions on secrecy for the protection of anonymous authors and media sources, 3) contains information shared between a suspect and his or her legal counsel and is thus protected by attorney-client privilege, or 4) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information (section 7).

26. If communications have been intercepted between a sender and receiver who are both in Sweden, despite the prohibition on such

interception, they shall be destroyed as soon as the domestic nature of the communications has become evident (section 2a).

27. If a permit urgently granted by the FRA (see paragraph 21 above) is revoked or amended by the Foreign Intelligence Court, all intelligence collected which is thereby no longer authorised must be immediately destroyed (section 5b(3)).

28. The FRA Personal Data Processing Act (*Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:259) contains provisions on the treatment of personal data within the area of signals intelligence. The Act entered into force on 1 July 2007, with amendments made on 30 June 2009 and 15 February 2010. The purpose of the Act is to protect against violations of personal integrity (Chapter 1, section 2). The FRA shall ensure, *inter alia*, that personal data is collected only for certain expressly stated and justified purposes. Such purpose is either determined by the direction of the foreign intelligence activities through a detailed tasking directive or by what is necessary in order to follow changes in the signals environment, technical advances and signals protection. Also, the personal data treated has to be adequate and relevant in relation to the purpose of the treatment. No more personal data than what is necessary for that purpose may be processed. All reasonable efforts have to be made to correct, block and obliterate personal data that is incorrect or incomplete (Chapter 1, sections 6, 8 and 9).

29. Personal data may not be processed solely because of what is known of a person's race or ethnicity, political, religious or philosophical views, membership in a union, health or sexual life. If, however, personal data is treated for a different reason, this type of information may be used if it is absolutely necessary for the treatment. Information about a person's physical appearance must always be formulated in an objective way with respect for human dignity. Intelligence searches may only use the mentioned personal indicators as search terms if this is absolutely necessary for the purpose of the search (Chapter 1, section 11).

30. Personnel at the FRA who process personal data go through an official security clearance procedure and are subject to confidentiality in regard to data to which secrecy applies. They could face criminal sanctions if tasks relating to the processing of personal data are mismanaged (Chapter 6, section 2).

31. Personal data that has been subjected to automated processing shall be destroyed as soon as it is no longer needed (Chapter 6, section 1).

32. Further provisions on the treatment of personal data are laid down in the FRA Personal Data Processing Ordinance (*Förordningen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:261). It provides, *inter alia*, that the FRA may keep databases for raw material containing personal data. Raw material is unprocessed information which has been

collected through automated treatment. Personal data in such databases shall be destroyed within one year from when it was collected (section 2).

F. Conditions for communicating the intercepted data to other parties

33. The intelligence collected shall be reported to the authorities concerned, as determined under the Foreign Intelligence Act (Signals Intelligence Act, section 8; see paragraphs 8-9 above).

34. The Government Offices, the Armed Forces, the Security Police, the NOA, the Inspectorate of Strategic Products (*Inspektionen för strategiska produkter*), the Defence Material Administration (*Försvarets materialverk*), the Defence Research Agency (*Totalförsvarets forskningsinstitut*), the Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*) and the Swedish Customs (*Tullverket*) may have direct access to completed intelligence reports to the extent the FRA so decides (section 9 of the FRA Personal Data Processing Ordinance). However, to date, no decisions permitting direct access have been taken by the FRA.

35. Personal data may be communicated to other states or international organisations only if not prevented by secrecy and if necessary for the FRA to perform its activities within international defence and security cooperation. The Government may adopt rules or decide in a specific case to allow such communication of personal data also in other cases when necessary for the activities of the FRA (Chapter 1, section 17 of the FRA Personal Data Processing Act). The FRA may disclose personal data to a foreign authority or an international organisation if it is beneficial for the Swedish government (*statsledningen*) or Sweden's comprehensive defence strategy (*totalförsvaret*); information so communicated must not harm Swedish interests (section 7 of the FRA Personal Data Processing Ordinance).

G. Supervision of the implementation of signals intelligence

36. The Foreign Intelligence Act (section 5) and the Signals Intelligence Act (section 10) prescribe that an authority is to oversee the foreign intelligence activities in Sweden and verify that the FRA's activities are in compliance with the provisions of the Signals Intelligence Act. The supervisory authority – the Foreign Intelligence Inspectorate – is, among other things, tasked with monitoring the implementation of the Foreign Intelligence Act and the associated Ordinance and reviewing whether foreign intelligence activities are performed in compliance with the applicable directives (section 4 of the Foreign Intelligence Inspectorate Instructions Ordinance (*Förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*; 2009:969)). It shall also

review compliance with the Signals Intelligence Act by examining in particular the search terms used, the destruction of intelligence and the communication of reports; if an inspection reveals that a particular intelligence collection is incompatible with a permit, the Inspectorate may decide that the operation shall cease or that the intelligence shall be destroyed (section 10 of the Signals Intelligence Act). The FRA shall report to the Inspectorate the search terms which directly relate to a specific natural person (section 3 of the Signals Intelligence Ordinance).

37. The Foreign Intelligence Inspectorate is led by a board whose members are appointed by the Government on terms of at least four years. The president and the vice-president shall be or have been permanent judges. Other members are selected from candidates proposed by the party groups in the Parliament (section 10 (3) of the Signals Intelligence Act).

38. Any opinions or suggestions for measures arising from the Inspectorate's inspections shall be forwarded to the FRA, and if necessary also to the Government. The Inspectorate also submits annual reports on its inspections to the Government (section 5 of the Foreign Intelligence Inspectorate Instructions Ordinance), which are made available to the public. Furthermore, if the Inspectorate notices potential crimes, it shall report the matter to the Prosecution Authority (*Åklagarmyndigheten*), and, if deficiencies are discovered that may incur liability for damages for the State, a report shall be submitted to the Chancellor of Justice (*Justitiekanslern*). A report may also be submitted to the Data Protection Authority (*Datainspektionen*), which is the supervisory authority on the treatment of personal data by the FRA (section 15).

39. From the establishment of the Inspectorate in 2009 until and including 2017, the latest year covered by its annual reports, no inspections have revealed reasons to cease an intelligence collection or to destroy the results. During the same period, the Inspectorate submitted several opinions and suggestions to the FRA and one to the Government. In the annual reports, brief descriptions have been given of the 102 inspections undertaken at the FRA; they have included numerous detailed examinations of the search terms used, the destruction of intelligence, the communication of reports, the treatment of personal data and the overall compliance with the legislation, directives and permits relevant to the signals intelligence activities. For instance, an inspection in 2014 concerned a general review of the FRA's cooperation with other states and international organisations in intelligence matters. It did not give rise to any opinion or suggestion to the FRA. In 2017 the Inspectorate carried out a detailed inspection of the treatment by the FRA of personal data. The inspection concerned treatment of sensitive personal data in connection with strategic circumstances with regard to international terrorism and other serious cross-border crime threatening significant national interests. The inspection did not give rise to any opinion or suggestion. However, during that year, one opinion was

submitted to the Government following an inspection of whether the FRA's intelligence activities were carried out within the direction given. During the years 2009-2017 the Inspectorate found reason to make a report to another authority – the Data Protection Authority – on one occasion, concerning the interpretation of a legal provision. In its annual reports, the Inspectorate has noted that it has been given access to all the information necessary for its inspections.

40. The supervisory activities of the Foreign Intelligence Inspectorate have been audited by the National Audit Office (*Riksrevisionen*), an authority under Parliament. In a report published in 2015 the Office noted that the FRA had routines in place for handling the Inspectorate's opinions and that the supervision helped develop the activities of the FRA. Suggestions were dealt with in a serious manner and, when called for, gave rise to reforms. At the same time the Office criticised the Inspectorate's lack of documentation of inspections and that there were no clearly specified goals for the inspections.

41. Within the FRA there is a Privacy Protection Council tasked with continuously monitoring measures taken to ensure protection of personal integrity. The members are appointed by the Government. The Council shall report its observations to the FRA management or, if the Council finds reasons for it, to the Inspectorate (section 11 of the Signals Intelligence Act).

42. Further provisions on supervision are found in the FRA Personal Data Processing Act. The FRA shall appoint one or several data protection officers and report the appointment to the Data Protection Authority (Chapter 4, section 1). The data protection officer is tasked with independently monitoring that the FRA treats personal data in a legal and correct manner and point out any deficiencies. If deficiencies are suspected and no correction is made, a report shall be submitted to the Data Protection Authority (Chapter 4, section 2).

43. The Data Protection Authority, which is an authority under the Government, has on request access to the personal data that is processed by the FRA and documentation on the treatment of personal data along with the security measures taken in this regard as well as access to the facilities where personal data is processed (Chapter 5, section 2). If the Authority finds that personal data is or could be processed illegally, it shall try to remedy the situation by communicating its observations to the FRA (Chapter 5, section 3). It may also apply to the Administrative Court (*förvaltningsrätten*) in Stockholm to have illegally processed personal data destroyed (Chapter 5, section 4).

H. Notification of secret surveillance measures

44. If search terms directly related to a specific natural person have been used, he or she is to be notified by the FRA, according to the Signals Intelligence Act. The notification shall contain information on the date and purpose of the measures. Such notification shall be given as soon as it can be done without detriment to the foreign intelligence activities, but no later than one month after the signals intelligence mission has been concluded (section 11a).

45. However, the notification may be delayed if secrecy so demands, in particular defence secrecy or secrecy for the protection of international relations. If, due to secrecy, no notification has been given within a year from the conclusion of the mission, the person does not have to be notified. Furthermore, a notification shall not be given if the measures solely concern the conditions of a foreign power or the relationship between foreign powers (section 11b).

I. Remedies

46. The Signals Intelligence Act provides that the Foreign Intelligence Inspectorate, at the request of an individual, must investigate if his or her communications have been intercepted through signals intelligence and, if so, verify whether the interception and treatment of the information have been in accordance with law. The Inspectorate shall notify the individual that such an investigation has been carried out (section 10a). A request can be made by legal and natural persons regardless of nationality and residence. During the period 2010-2017, 132 requests were handled and no unlawfulness was established. In 2017, ten such requests were processed; in 2016 the number was 14. The Inspectorate's decision following a request is final.

47. Under the FRA Personal Data Processing Act, the FRA is also required to provide information upon request. Once per calendar year, an individual may demand information on whether personal data concerning him or her is being or has been processed. If so, the FRA must specify what information on the individual is concerned, from where it was collected, the purpose of the treatment and to which recipients or categories of recipients the personal data is or was reported. The information is normally to be given within one month from the request (Chapter 2, section 1). However, this right to information does not apply if disclosure is prevented by secrecy (Chapter 2, section 3).

48. Following a request from the individual who has had personal data registered, the FRA shall promptly correct, block or destroy such data that has not been processed in accordance with law. The FRA shall also notify any third party who has received the data, if the individual so requests or if

substantial harm or inconvenience could be avoided through a notification. No such notification has to be given if it is impossible or would involve a disproportionate effort (Chapter 2, section 4).

49. The FRA's decisions on disclosure and corrective measures in regard to personal data may be appealed against to the Administrative Court in Stockholm (Chapter 6, section 3).

50. The State is liable for damages following a violation of personal integrity caused by treatment of personal data not in accordance with the FRA Personal Data Processing Act (Chapter 2, section 5). A request for damages shall be submitted to the Chancellor of Justice.

51. In addition to the above remedies, laid down in the legislation relating to signals intelligence, Swedish law provides for a number of other means of scrutiny and complaints mechanisms. The Parliamentary Ombudsmen (*Justititeombudsmannen*) supervise the application of laws and regulations in public activities; courts and authorities are obliged to provide information and opinions at the request of the Ombudsmen (Chapter 13, section 6 of the Instrument of Government – *Regeringsformen*), including access to minutes and other documents. The Ombudsmen shall ensure, in particular, that the courts and authorities observe the provisions of the Instrument of Government on objectivity and impartiality and that citizens' fundamental rights and freedoms are not encroached upon in public activities (section 3 of the Parliamentary Ombudsmen Instructions Act – *Lagen med instruktion för Riksdagens ombudsmän*; 1986:765). The supervision, under which the Foreign Intelligence Court and the FRA come, is conducted by means of examining complaints from the public and through inspections and other investigations (section 5). The examination is concluded by a decision in which, although not legally binding, the opinion of the Ombudsman is given as to whether the court or authority has contravened the law or otherwise taken a wrongful or inappropriate action; the Ombudsman may also initiate criminal or disciplinary proceedings against a public official who has committed a criminal offence or neglected his or her duty in disregarding the obligations of the office (section 6).

52. With a mandate similar to the Parliamentary Ombudsmen, the Chancellor of Justice scrutinises whether officials in public administration comply with laws and regulations and otherwise fulfil their obligations (section 1 of the Chancellor of Justice Supervision Act – *Lagen om justitiekanslerns tillsyn*; 1975:1339). The Chancellor does so by examining individual complaints or conducting inspections and other investigations, which could be directed at, for instance, the Foreign Intelligence Court and the FRA. At the request of the Chancellor, courts and authorities are obliged to provide information and opinions as well as access to minutes and other documents (sections 9 and 10). The decisions of the Chancellor of Justice are similar in nature to the decisions of the Parliamentary Ombudsmen, including their lack of legally binding power. By tradition, however, the

opinions of the Chancellor and the Ombudsmen command great respect in Swedish society and are usually followed (see *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 118, ECHR 2006-VII). The Chancellor has the same power as the Ombudsmen to initiate criminal or disciplinary proceedings (sections 5 and 6).

53. The Chancellor of Justice is also authorised to determine complaints and claims for damages directed against the State, including compensation claims for alleged violations of the Convention. The Supreme Court and the Chancellor of Justice have developed precedents in recent years, affirming that it is a general principle of law that compensation for Convention violations can be ordered without direct support in Swedish statute to the extent that Sweden has a duty to provide redress to victims of Convention violations through a right to compensation for damages (see *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, §§ 58-62 and 67, 20 December 2016, with further references). On 1 April 2018, through the enactment of a new provision – Chapter 3, section 4 – of the Tort Liability Act (*Skadeståndslagen*; 1972:207), the right to compensation for violations of the Convention was codified.

54. In addition to its above-mentioned supervisory functions under the Foreign Intelligence Inspectorate Instructions Ordinance and the FRA Personal Data Processing Act (see paragraphs 38, 42 and 43 above), the Data Protection Authority is generally entrusted with protecting individuals against violations of their personal integrity through the processing of personal data, under the Act with Supplementary Provisions to the EU General Data Protection Regulation (*Lagen med kompletterande bestämmelser till EU:s dataskyddsförordning*) which entered into force on 25 May 2018, the same day as the new EU regulation it supplements (paragraph 81 below). In regard to the signals intelligence conducted by the FRA – which falls outside the competence of the EU and is thus not regulated by Community law – the Personal Data Act (*Personuppgiftslagen*; 1998:204) continues to apply, although it is otherwise replaced by the new EU Regulation and the supplementary act. It gives the Data Protection Authority the same general supervisory task. In performing this task, the Authority may receive and examine individual complaints.

J. Secrecy at the FRA

55. The Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslagen*; 2009:400) contains a specific provision on the FRA's signals intelligence activities. Secrecy applies to information on an individual's personal or economic circumstances, unless it is evident that the information can be disclosed without the individual concerned or any other person closely related to him or her being harmed. The presumption is for secrecy (Chapter 38, section 4).

56. According to the Act, secrecy also generally applies to foreign intelligence activities in regard to information concerning another State, international organisation, authority, citizen or legal person in another State, if it can be presumed that a disclosure will interfere with Sweden's international relations or otherwise harm the country (Chapter 15, section 1).

57. Secrecy further applies to information on activities related to the defence of the country or the planning of such activities or to information that is otherwise related to the country's comprehensive defence strategy, if it can be presumed that a disclosure will harm the country's defence or otherwise endanger national security (Chapter 15, section 2).

58. Information which is protected by secrecy under the Public Access to Information and Secrecy Act may not be disclosed to a foreign authority or an international organisation unless 1) such disclosure is permitted by an express legal provision (cf. section 7 of the FRA Personal Data Processing Ordinance, paragraph 34 above), or 2) the information in an analogous situation may be communicated to a Swedish authority and the disclosing authority finds it evident that the communication of the information to the foreign authority or the international organisation is consistent with Swedish interests (Chapter 8, section 3 of the Act).

K. The reports of the Data Protection Authority

59. On 12 February 2009 the Government ordered the Data Protection Authority to examine the handling of personal data at the FRA from an integrity perspective. In its report, published on 6 December 2010, the Authority stated that its conclusions were overall positive. Issues relating to the processing of personal data and to personal integrity were given serious consideration by the FRA and a considerable amount of time and resources were spent on creating routines and educating its personnel in order to minimise the risk of unwarranted interferences with personal integrity. Moreover, no evidence had been found which indicated that the FRA was handling personal data for purposes not authorised by the legislation in force (see paragraphs 12-14 and 28 above). However, the Authority noted, *inter alia*, that there was a need to improve the methods for separating domestic and cross-border communications. Even if the FRA had implemented mechanisms in that area, there was no guarantee that domestic communications were never intercepted, and, although the occasions had been very few, such communications had in fact been intercepted. The Authority further noted that the procedure for notification to individuals (paragraphs 44-45 above) had never been used by the FRA, due to secrecy.

60. A second report was issued by the Authority on 24 October 2016. Again, the Authority found no evidence that personal data had been collected for other purposes than those stipulated for the signals intelligence

activities. It also noted that the FRA continuously reviewed whether data intercepted was still needed for those purposes. A similar review was made concerning the carriers from which the FRA obtained intelligence. Moreover, there was nothing to indicate that the provisions on destruction of personal data had been disregarded (see paragraphs 25-27 above). However, the FRA was criticised for not adequately monitoring logs used to detect unwarranted use of personal data, a shortcoming that had been pointed out already in 2010.

L. The report of the Signals Intelligence Committee

61. On 12 February 2009 the Government also decided to appoint a committee predominantly composed of members of parliament, the Signals Intelligence Committee (*Signalspaningskommittén*), with the task of monitoring the signals intelligence conducted at the FRA in order to examine the implications for personal integrity. The report was presented on 11 February 2011 (*Uppföljning av signalspaningslagen*; SOU 2011:13). The Committee's examination had its main focus on signals intelligence conducted over the airways as such activities on cable-based traffic had not yet commenced on a larger scale.

62. The Committee concluded that concerns of personal integrity were taken seriously by the FRA and formed an integral part of the development of its procedures. It noted, however, that there were practical difficulties in separating domestic cable-based communications from those crossing the Swedish border. Any domestic communications that were not separated at the automated stage were instead separated manually at the processing or analysing stage. The Committee further observed that the search terms used for communications data were less specific than those used for interception of the content of a communication and that, consequently, a larger number of individuals could have such data stored by the FRA.

63. Another finding in the report was that the FRA's development activities (see paragraph 14 above) could lead to non-relevant communications being intercepted and possibly read or listened to by FRA personnel. However, the Committee noted that the development activities were directly essential for the FRA's ability to conduct signals intelligence. Moreover, information obtained through the development activities could be used in the regular intelligence activities only if such use conformed with the purposes established by law and the relevant tasking directives issued for the signals intelligence.

64. Like the Data Protection Authority (see paragraph 59 above), the Committee pointed out that, in reality, the obligation of the FRA to notify individuals that had been directly and personally subjected to secret surveillance measures was very limited due to secrecy; it concluded therefore that this obligation served no purpose as a guarantee for legal

certainty or against integrity interferences. The Committee found, however, that, in particular, the authorisation procedure before the Foreign Intelligence Court, in deciding on permits to conduct signals intelligence measures (paragraphs 18-22), and the supervisory functions performed by the Foreign Intelligence Inspectorate (paragraphs 24 and 36-40) and the Privacy Protection Council (paragraph 41) provided important protection for individuals' personal integrity. It noted, in this respect, that, although the Privacy Protection Council formed part of the FRA, it acted in an independent manner.

III. RELEVANT INTERNATIONAL AND EUROPEAN LAW

A. United Nations

65. Resolution no. 68/167, on The Right to Privacy in the Digital Age, adopted by the General Assembly on 18 December 2013, reads as follows:

“The General Assembly,

...

4. *Calls upon* all States:

...

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ...”

B. Council of Europe

1. *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its Additional Protocol*

66. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (CETS No. 108) was ratified by Sweden on 29 September 1982. It sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides, in so far as relevant, as follows:

Preamble

“The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:”

Article 1 – Object and purpose

“The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (“data protection”).”

Article 8 – Additional safeguards for the data subject

“Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.”

Article 9 – Exceptions and restrictions

“1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

...”

Article 10 – Sanctions and remedies

“Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.”

67. The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181), ratified by Sweden on the latter date, provides as follows:

Article 1 – Supervisory authorities

“1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

...”

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

“1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of:

– specific interests of the data subject, or

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.”

2. *Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services*

68. Recommendation No. R (95) 4 of the Committee of Ministers on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, adopted on 7 February 1995, reads, *inter alia*, as follows:

“2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

- a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;
- b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

- a. the exercise of the data subject’s rights of access and rectification;
- b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;
- c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference.”

3. *Report of the Venice Commission*

69. In December 2015 the European Commission for Democracy through Law – “the Venice Commission” – published its “Report on the Democratic Oversight of Signals Intelligence Agencies”. The Commission noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data was accessed and/or processed by the agencies. For this reason, the computer analysis

(usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

70. According to the report, the two most significant safeguards were the authorisation process (of collection and access) and the oversight process. It was clear from the Court's case-law that the latter must be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the court's conditions was problematic.

71. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention. In this regard, a general complaints procedure to an independent oversight body could compensate for non-notification.

72. The report also considered internal controls to be a "primary safeguard". In this regard, recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

73. The report also considered the position of journalists. It accepted that they were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. It acknowledged, however, that the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

74. Finally, the report briefly considered the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

C. European Union

1. *Charter of Fundamental Rights of the European Union*

75. Articles 7, 8 and 11 of the Charter provide as follows:

Article 7 – Respect for private and family life

“Everyone has the right to respect for his or her private and family life, home and communications.”

Article 8 – Protection of personal data

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

Article 11 – Freedom of expression and information

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.”

2. *EU directives relating to protection and processing of personal data*

76. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. As the activities of member States regarding public safety, defence and State security fall outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

77. The Privacy and Electronic Communications Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), adopted on 12 July 2002, states, in recitals 2 and 11:

“(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the

State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.”

The Directive further provides, *inter alia*, the following:

Article 1 – Scope and aim

“1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.”

Article 15 – Application of certain provisions of Directive 95/46/EC

“1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.”

78. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) was adopted. It provided, *inter alia*, as follows:

Article 1 - Subject matter and scope

“1. This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.”

Article 3 – Obligation to retain data

“1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

...”

3. Case-law of the Court of Justice of the European Union (CJEU) on data protection

79. In *Digital Rights Ireland v Minister for Communications & Others*, (cases C-293/12 and C-594/12, judgment of 8 April 2014), the CJEU declared invalid Directive 2006/24/EC. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation on providers of publicly available electronic communications services or of public communications networks to retain those data and the access of the national authorities to the data constituted an interference with the right to respect for private life and communications and the right to protection of personal data guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights. While the interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security, it failed to satisfy the requirement of proportionality. The protection of the fundamental right to respect for private life required, according to the court’s settled case-law, that derogations and limitations in relation to the protection of personal data could apply only in so far as was strictly necessary. The directive covered, however, in a generalised manner, all persons and all means of electronic communication as well as all communications data without any differentiation, limitation or exception being made in the light of the

objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population, even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring to serious crime, as defined by each member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the rights in Articles 7 and 8 of the Charter, without having laid down clear and precise rules governing the extent of the interference and ensuring that it was actually limited to what was strictly necessary. Moreover, the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

80. In joined cases *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* (cases C-203/15 and C-698/15, judgment of 21 December 2016), the CJEU (Grand Chamber) dealt, firstly, with the issue of a provider of electronic communications services having refused to retain data under Swedish legislation that had given effect to the now invalid Directive 2006/24/EC. The CJEU stated, *inter alia*, the following:

“107. National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing

minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary. ...

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

112. Having regard to all of the foregoing, ... Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.”

The CJEU also examined a question by the Court of Appeal (England & Wales) (Civil Division) as to whether, in the *Digital Rights* judgment, the Court had interpreted Article 7 or 8 of the Charter in such a way as to expand the scope conferred on Article 8 of the Convention by the European Court of Human Rights. The CJEU stated:

“127. As a preliminary point, it should be recalled that, whilst, as Article 6(3) [of the Treaty on European Union] confirms, fundamental rights recognised by the [Convention] constitute general principles of EU law, the [Convention] does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law

128. Accordingly, the interpretation of Directive 2002/58, which is at issue in this case, must be undertaken solely in the light of the fundamental rights guaranteed by the Charter

129. Further, it must be borne in mind that the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the [Convention], ‘without thereby adversely affecting the autonomy of Union law and ... that of the Court of Justice of the European Union’ (judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84,

paragraph 47). In particular, as expressly stated in the second sentence of Article 52(3) of the Charter, the first sentence of Article 52(3) does not preclude Union law from providing protection that is more extensive than the [Convention]. It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the [Convention].

130. However, in accordance with the Court's settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law

131. In this case, in view of the considerations set out, in particular, in paragraphs 128 and 129 of the present judgment, the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter, which is the matter in dispute in the proceedings in Case C-698/15.

132. Accordingly, it does not appear that an answer to the second question in Case C-698/15 can provide any interpretation of points of EU law that is required for the resolution, in the light of that law, of that dispute.

133. It follows that the second question in Case C-698/15 is inadmissible.”

The CJEU ruled as follows:

“1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

3. The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible.”

4. The General Data Protection Regulation

81. On 25 May 2018 the General Data Protection Regulation (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and repealing Directive 95/46/EC) entered into force. Like the Directive it replaced, the Regulation does not apply to State activities concerning public safety, defence and State security (Article 2(2)).

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

82. The applicant complained that that Swedish state practice and legislation concerning signals intelligence had violated and continued to violate its right to respect for private life and correspondence. The complaint concerned three time periods: from 2002 to 1 January 2009, from 1 January 2009 to 1 December 2009 and from 1 December 2009 onwards. The applicant invoked Article 8 of the Convention, which reads as follows:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

A. Admissibility

83. The Government questioned whether the applicant had exhausted all domestic remedies available and left it for the Court to determine the exhaustion issue. They further submitted that the applicant could not claim to be a victim of the alleged violation of Article 8. With regard to private life, the Government disputed that such a right was afforded to legal persons. In any event, they argued that the complaint was manifestly ill-founded.

84. In regard to the Government’s first objection, the Court notes, as explained below (see paragraphs 171-177), that there is, in practice, no remedy which provides detailed grounds in its response to a complainant who suspects that he or she has had his communications intercepted. Furthermore, the Government have not pointed to any individual effective remedy that would have to be exhausted for the purposes of Article 35. The Court therefore finds that the applicant was not required to bring any domestic proceedings and accordingly rejects the objection concerning the exhaustion of domestic remedies.

85. As regards private life, the Court has previously held that it may be open to doubt whether a legal person can have a private life within the

meaning of Article 8. However, it can be said that its mail and other communications are covered by the notion of “correspondence” which applies equally to communications originating from private and business premises. Moreover, applicants who are legal persons may fear that they are subjected to secret surveillance and it has accordingly been accepted that they may claim to be victims (see *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 60, 28 June 2007, with further references). It is therefore appropriate to examine the complaint under the right to respect for the applicant’s correspondence.

86. Considering that the Government’s objection on victim status is closely linked to the substance of the applicant’s complaint, it must be joined to the merits.

87. The Court further notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The applicant’s victim status and the existence of an interference

(a) The parties’ submissions

88. The Government submitted that the applicant could not claim to be a victim of a violation of the Convention by the mere existence of legislation concerning signals intelligence. The aggregate of control mechanisms, supervisory elements and remedies available constituted sufficient safeguards against abuse of the FRA’s competence to conduct signals intelligence. Furthermore, the possibility that the applicant had been subject to signals intelligence was virtually non-existent.

89. The applicant disagreed with the Government and remarked, with reference to the case of *Kennedy v. the United Kingdom* (no. 26839/05, 18 May 2010), that its victim status was based on the risk of secret surveillance measures having been applied.

(b) The Court’s assessment

90. In the *Roman Zakharov v. Russia* judgment ([GC], no. 47143/06, § 171, ECHR 2015), which concerned covert interception of mobile telephone communications, the Court, adopting the *Kennedy* approach, clarified the conditions under which an applicant can claim to be a victim of a violation of Article 8 without having to prove that secret surveillance measures have in fact been applied to him or her specifically. Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or

legislation permitting such measures, if the following conditions are satisfied.

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

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

93. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he or she is able to show that, due to the specific personal situation, he or she is potentially at risk of being subjected to such measures.

94. The Court considers that the contested legislation on signals intelligence institutes a system of secret surveillance that potentially affects all users of, for example, mobile telephone services and the internet, without their being notified about the surveillance. Also, as concluded above (see paragraph 84), no domestic remedy provides detailed grounds in response to a complainant who suspects that he or she has had his communications intercepted. In these circumstances, the Court considers an examination of the relevant legislation *in abstracto* to be justified.

95. The applicant is therefore entitled to claim to be the victim of a violation of the Convention, even though it is unable to allege that it has been subjected to a concrete measure of interception. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of the applicant's rights under Article 8. The Court therefore dismisses the Government's objection concerning the applicant's lack of victim status.

2. *The temporal scope of the Court's examination*

96. As already mentioned, the applicant has complained about three different time periods, arguing that each period is characterised by a different legal regime.

97. In other cases where the law has been reviewed *in abstracto* and amendments have been made to the legislation while the application was pending, the Court has limited itself to reviewing Convention compliance of the law in force at the time of its examination (see, for example, *Association for European Integration and Human Rights and Ekimdzhiiev*, cited above; *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009; and *Roman Zakharov*, cited above).

98. As stated above, the Court's task is not to examine measures that have "directly affected" the applicant, but to review the relevant Swedish law and practice *in abstracto*. The Swedish legislation has been amended on many occasions since the application was lodged with the Court, also since the start of the third time period on 1 December 2009. It cannot be the task of the Court, when reviewing the law *in abstracto*, to examine compatibility with the Convention before and after every single legislative amendment. The review will therefore focus on the Swedish legislation as it stands at the time of the present examination.

3. *The justification of the interference*

(a) **General principles**

99. The Court reiterates that any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim. The following general principles have been collated in *Roman Zakharov* (see §§ 228-236 of that judgment and the further references listed therein).

100. The wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects (*Roman Zakharov*, § 228).

101. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of telephone communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance cannot mean that an individual should be able to foresee when the authorities are likely to intercept communications so that he or she can adapt his or her conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risk of arbitrariness is evident. It is therefore essential to have

clear, detailed rules on interception of telephone communications, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances and conditions which give public authorities the power to resort to such measures (*Roman Zakharov*, § 229).

102. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (*Roman Zakharov*, § 230).

103. In its case-law on secret measures of surveillance in criminal investigations, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: a description of the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of the measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (*Roman Zakharov*, § 231).

104. As to the question whether an interference has been “necessary in a democratic society” in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant’s rights under Article 8, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are 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. It has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the

“interference” to what is “necessary in a democratic society” (*Roman Zakharov*, § 232).

105. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual’s knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control normally offering the best guarantees of independence, impartiality and a proper procedure (*Roman Zakharov*, § 233).

106. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to a remedy by the individual concerned unless he or she is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, that any person who suspects that his or her communications are being or have been intercepted can apply to an appropriate body, so that the latter’s jurisdiction does not depend on a notification having been given to the subject who has had communications intercepted (*Roman Zakharov*, § 234).

107. Having found an interference of the applicant’s rights under Article 8 § 1, in examining the justification for the interference under Article 8 § 2, the Court needs to determine whether the contested legislation itself is in conformity with the Convention (*Roman Zakharov*, § 235). In cases where the legislation permitting secret surveillance is contested, the matter of the lawfulness of the interference is closely related to the question whether the “necessity” requirement has been complied with and it is therefore appropriate to address these two issues jointly. The “quality of law” in this sense implies that the domestic law must not only be accessible and foreseeable in its application, but must also ensure that secret surveillance measures are applied only when “necessary in a democratic

society”, in particular by providing for adequate and effective safeguards and guarantees against abuse (*Roman Zakharov*, § 236).

(b) Existing case-law on the bulk interception of communications

108. The Court has considered the Convention compatibility of regimes which expressly permit the bulk interception of communications on two occasions: first in *Weber and Saravia v. Germany* ((dec.), no. 54934/00, ECHR 2006-XI), and then in *Liberty and Others v. the United Kingdom* (no. 58243/00, 1 July 2008).

109. In *Weber and Saravia* the applicants complained about the process of strategic monitoring under the amended G10 Act, which authorised the monitoring of international wireless telecommunications. Signals emitted from foreign countries were monitored by interception sites situated on German soil with the aid of certain catchwords which were listed in the monitoring order. Only communications containing these catchwords were recorded and used. Having particular regard to the six “minimum safeguards” (see paragraph 103 above), the Court considered that there existed adequate and effective guarantees against abuses of the State’s strategic monitoring powers. It therefore declared the applicants’ Article 8 complaints to be manifestly ill-founded.

110. In *Liberty and Others* the Court was considering the regime under the Interception of Communications Act 1985 which allowed the executive to intercept communications passing between the United Kingdom and an external receiver. At the time of issuing an interception warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. On the face of the 1985 Act, external communications sent to or from an address in the United Kingdom could only be included in the certificate if the Secretary of State considered it necessary for the prevention or detection of acts of terrorism. Otherwise, the legislation provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered that this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom’s economy. The Court held that the domestic law at the relevant time did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.

(c) Application of these principles to the facts of the case

111. It has not been disputed by the parties that the Swedish signals intelligence, in its present structure, has a basis in domestic law.

Furthermore, the Court considers it clear that the measures permitted by Swedish law pursue legitimate aims in the interest of national security by supporting Swedish foreign, defence and security policy and identifying external threats to the country. It therefore remains to be ascertained whether the domestic law is accessible and contains adequate and effective safeguards and guarantees to be considered “foreseeable” and “necessary in a democratic society”.

112. The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106). In *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States’ margin of appreciation.

113. Nevertheless, it is evident from the Court’s case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities’ discretion to intercept cannot be discerned from the relevant legislation (see, for example, *Klass and Others v. Germany*, 6 September 1978, Series A no. 28; *Kennedy*, cited above; *Roman Zakharov*, cited above, and *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016). Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard, the Court has identified six minimum safeguards that both bulk interception and other interception regimes must incorporate in order to be sufficiently foreseeable to minimise the risk of abuses of power (see paragraph 103 above).

114. Accordingly, adapting these minimum safeguards where necessary to reflect the operation of a bulk interception regime dealing exclusively with national security issues, the following assessment of the interference established (see paragraph 95 above) will address, in turn, the accessibility of the domestic law, the scope and duration of signals intelligence, the authorisation of the measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted

data, the arrangements for supervising the implementation of the measures, any notification mechanisms and the remedies provided for by national law.

(i) Accessibility of domestic law

115. The Court finds that all legal provisions relevant to signals intelligence have been officially published and are accessible to the public, a fact that has not been questioned by the applicant.

(ii) Scope of application of signals intelligence

(α) The parties' submissions

116. The applicant submitted that, whereas the conduct against which signals intelligence could be directed had clear affinities to various criminal offences, for instance crimes against the security of the nation, the same could not be said for the FRA's development activities. The latter activities allegedly permitted bulk collection of data, including large amounts of communications data, without regard to the requirement that interception be ordered only in regard to certain specific offences. The applicant further emphasised that, since 1 January 2013, the Security Police and the NOA have been given a mandate to issue more detailed tasking directives for signals intelligence. Since the general tasks of these two authorities were crime prevention and investigation there was a risk that signals intelligence was being conducted outside the scope of foreign intelligence activities.

117. The Government submitted that the FRA's development activities were as rigorously regulated – and subject to supervision to the same extent – as signals intelligence in general. The Government also opposed the claim that signals intelligence could be used to investigate crimes, as the law did not permit such use of signals intelligence.

(β) The Court's assessment

118. The Court reiterates that the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures (see paragraph 103 above).

119. The requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. At the same time, it must be emphasised that in matters affecting fundamental rights it would be contrary to the rule of law for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and

the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 247, with further references).

120. The Signals Intelligence Act stipulates eight purposes for which signals intelligence may be conducted (see paragraph 12 above). Although some of these purposes are generally framed, they are further elaborated upon in the preparatory works (paragraph 13), which is an essential source of Swedish legislation. The Court finds that these eight purposes are adequately indicated (cf. *Roman Zakharov*, cited above, §§ 246 and 248).

121. It is of further importance that signals intelligence conducted on fibre optic cables may only concern communications crossing the Swedish border in cables owned by a communications service provider. Communications between a sender and a receiver in Sweden may not be intercepted, regardless whether the source is airborne or cable-based.

122. It is true that the FRA may also intercept signals as part of its development activities which, it appears, mainly concern the collection of communications data. Such collection is made in order to monitor changes in the international signals environment and to develop the FRA's own signals intelligence technology, and may lead to data not relevant for the regular foreign intelligence being intercepted and read. Also, the search terms used for interception of communications data – whether part of the development activities or not – are less specific than those used for interception of the content of a communication (see paragraph 62 above). However, as noted by the Signals Intelligence Committee (paragraph 63), the development activities are essential for the proper functioning of the foreign intelligence and the information thereby obtained may be used in the regular foreign intelligence only if such use is in conformity with the purposes established by law and the applicable tasking directives. Moreover, the provisions applicable to the regular foreign intelligence work are also relevant to the development activities and to any interception of communications data, including the requirement of a permit issued by the Foreign Intelligence Court (paragraph 18). It is further of relevance in this context that, in its 2010 and 2016 reports, the Data Protection Authority found no evidence that personal data had been collected for other purposes than those stipulated for the signals intelligence activities (paragraphs 59-60). In these circumstances, the Court is satisfied that the scope of application of the development activities is sufficiently demarcated.

123. As from 1 January 2013, the Security Police and the NOA have been authorised to issue detailed tasking directives for signals intelligence. While, as pointed out by the applicant, the tasks of these authorities include crime prevention and investigation, section 4 of the Foreign Intelligence Act clearly excludes the use of foreign intelligence to solve tasks in the area of law enforcement or crime prevention (see paragraph 8 above).

124. Consequently, the Court finds that the law indicates the scope of mandating and performing signals intelligence conferred on the competent authorities and the manner of its exercise with sufficient clarity.

(iii) *Duration of secret surveillance measures*

(α) The parties' submissions

125. The applicant submitted that the legislation satisfied the minimum requirements in terms of duration of the permit.

126. The Government held that the Signals Intelligence Act clearly regulated the maximum duration of a permit and the conditions under which a permit could be renewed.

(β) The Court's assessment

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

128. As regards the first two safeguards, the Signals Intelligence Act stipulates that a permit may be granted for a maximum of six months and that it may be extended, following a new examination, for six months at a time (see paragraph 23 above). The examination preceding a renewal must be understood as encompassing a full review by the Foreign Intelligence Court as to whether the conditions set out in section 5 of the Act are still met (paragraph 19). The Act thus gives clear indications of the period after which the permit will expire and of the conditions under which it can be renewed.

129. In respect of the third safeguard, the circumstances in which interception must be discontinued, the legislation is not equally clear. There is no provision obliging the FRA, the authorities mandated to issue detailed tasking directives or the Foreign Intelligence Court to cancel a signals intelligence mission if the conditions for it have ceased to exist or the measures themselves are no longer necessary (cf. *Klass and Others*, cited above, § 52; and *Kennedy*, cited above, § 161).

130. Nevertheless, notwithstanding that the relevant legislation is less clear with regard to the third safeguard, it must be borne in mind that any permit is valid for a maximum of six months and that a renewal requires a review as to whether the conditions are still met. Furthermore, although the Foreign Intelligence Inspectorate is not tasked with inspecting every signals intelligence permit, it may decide that an intelligence interception shall cease, if during an inspection it is evident that the interception is not in

accordance with a permit (see paragraph 36 above). The Court also has regard to the fact that the permits in question concern the collection of intelligence related to threats to national security and are not targeting individuals suspected of criminal conduct, in which case the need for specific provisions on the cancellation of permits would have been more prominent. Moreover, as noted by the Data Protection Authority (paragraph 60), the FRA continuously reviews whether the specific personal data it has intercepted is still needed for its signals intelligence activities. In these circumstances, the Court is satisfied that there are safeguards in place which adequately regulate the duration, renewal and cancellation of interception measures.

(iv) *Authorisation of secret surveillance measures*

(α) The parties' submissions

131. The applicant submitted that, although signals intelligence could not be conducted without prior authorisation by the Foreign Intelligence Court, the court's impartiality and independence from the Government could be questioned and its activities were covered by complete secrecy. Its hearings and decisions had never been made public. The same was true for information about the number of hearings, the number of permits granted or rejected, any reasoning of its decisions or the amount or type of search terms being used. As to the composition of the court, its members were elected for a limited period of time, except for the president.

132. The Government emphasised that all signals intelligence conducted required a permit from the Foreign Intelligence Court, including the FRA's development activities. The Government also stressed that the court was independent from Parliament and public authorities. Although its activities were governed by secrecy, a privacy protection representative was present to safeguard the interests of individuals.

(β) The Court's assessment

133. As the Court has previously held, the authorisation of telephone tapping by a non-judicial authority may be compatible with the Convention (see, for example, *Klass and Others*, cited above, § 51; and *Weber and Saravia*, cited above, § 115), provided that that authority is sufficiently independent from the executive (*Roman Zakharov*, cited above, § 258). However, the rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control normally offering the best guarantees of independence, impartiality and a proper procedure (*Klass and Others*, cited above, §§ 55 and 56). Prior judicial authorisation may serve to limit the authorities' discretion in interpreting the scope of mandating and

performing signals intelligence. Thus, a requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness (*Roman Zakharov*, cited above, § 249). Nevertheless, prior authorisation of such measures is not an absolute requirement *per se*, because where there is extensive subsequent judicial oversight, this may counterbalance the shortcomings of the authorisation (*Szabó and Vissy*, cited above, § 77).

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

135. The main rule is that the court shall hold public hearings but, when secrecy applies, hearings may be held in private. As submitted by the applicant, and confirmed by the Government, the court's activities are in practice covered by complete secrecy. A hearing has never been open to the public and all decisions are confidential. As noted by the applicant, no information is disclosed to the public about the number of hearings, the number of permits granted or rejected, the reasoning of the court's decisions or the amount or type of search terms being used.

136. The Court is mindful of the fact that the nature of signals intelligence requires that surveillance is done in secret (see paragraph 101 above). It must therefore be accepted that, where there is a system of prior authorisation, sensitive aspects of the authorising body's activities are withheld from the public for as long as required in the individual case, in order not to defeat the purpose of the signals intelligence. However, such a procedure could only be accepted where there are adequate safeguards in place.

137. The Government have submitted that the lack of transparency is compensated by the presence of the privacy protection representative. He or she must be present during the court's examination, except in very urgent cases. The representative is either a present or former permanent judge or attorney and has access to all the case documents and may make statements. He or she does not appear on behalf of any individual concerned by the signals intelligence permit at issue, but protects the interests of the general public.

138. The Court is of the view that, while the privacy protection representative cannot appeal against a decision by the Foreign Intelligence Court or report any perceived irregularities to the supervisory bodies, the presence of the representative at the court's examinations compensates, to a limited degree, for the lack of transparency concerning the court's proceedings and decisions.

139. More importantly, taking into account that proceedings and decisions relating to secret surveillance largely require secrecy, the Court

considers that what is essential for the protection of individuals' rights in the context of the regime under consideration is that the FRA's signals intelligence is subject to a system of prior authorisation whereby the FRA must submit for independent examination an application for a permit to conduct surveillance in respect of each intelligence collection mission. As an additional safeguard against abuse and arbitrariness, the task of examining whether the mission is compatible with applicable legislation and whether the intelligence collection is proportional to the resultant interference with personal integrity has been entrusted to a body whose presiding members are or have been judges. Furthermore, the supervision of the Foreign Intelligence Court is extensive as the FRA, in its applications, must specify not only the mission request in question and the need for the intelligence sought but also the signal carriers to which access is needed and the search terms – or at least the categories of search terms – that will be used (see paragraphs 18-20 above). The Court therefore considers that the judicial supervision performed by the Foreign Intelligence Court is of crucial importance in that it limits the FRA's discretion by interpreting the scope of mandating and performing signals intelligence.

140. As a final point under this heading, it should be noted that the FRA itself may decide to grant a permit, if it is feared that the application of a permit from the Foreign Intelligence Court might cause delay or other inconveniences of essential importance for one of the specified purposes of the signals intelligence. In this context the Court reiterates the need for safeguards to ensure that such emergency measures are used sparingly and only in justified cases (*Roman Zakharov*, cited above, § 266). As the legislation states that such a decision must be followed by an immediate notification to and a subsequent rapid review by the Foreign Intelligence Court where the permit may be changed or revoked, the Court finds this procedure acceptable (cf. *Szabó and Vissy*, cited above, § 81).

141. In light of the foregoing, the Court finds that the provisions and procedures relating to the system of prior court authorisation, on the whole, provide important guarantees against abuse.

(v) *Procedures to be followed for storing, accessing, examining, using and destroying the intercepted data*

(α) The parties' submissions

142. The applicant argued that the procedures in these aspects were regulated in only very broad terms. For example, there was no general obligation to destroy data.

143. The Government pointed out that the Foreign Intelligence Inspectorate was responsible for scrutinising the treatment and destruction of data in general and had a mandate to terminate surveillance and order the

destruction of data that had been collected in a way that was incompatible with a permit issued by the Foreign Intelligence Court.

(β) The Court's assessment

144. The Court notes that personnel at the FRA treating personal data are security cleared and, if secrecy applies to the personal data, subject to confidentiality. They are under an obligation to handle the personal data in a safe manner. Also, they could face criminal sanctions if tasks relating to the treatment of personal data are mismanaged (see paragraph 30 above). Furthermore, the FRA must ensure that personal data is collected only for certain expressly stated and justified purposes, determined by the direction of the foreign intelligence activities through tasking directives. The personal data treated also has to be adequate and relevant in relation to the purpose of the treatment. No more personal data than what is necessary for that purpose may be processed. All reasonable efforts have to be made to correct, block and obliterate personal data which is incorrect or incomplete in relation to the purpose (paragraph 28).

145. Contrary to the applicant's claim, there are several provisions regulating the situations when intercepted data has to be destroyed. For example, intelligence must be destroyed immediately if it 1) concerns a specific natural person and has been determined to lack importance for the purpose of the signals intelligence, 2) is protected by constitutional provisions of secrecy for the protection of anonymous authors or media sources, 3) contains information shared between a criminal suspect and his or her counsel and is thus protected by attorney-client privilege, or 4) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information (see paragraph 25 above). Moreover, if communications have been intercepted between a sender and receiver both in Sweden, despite the ban on the interception of such communications, they must be destroyed as soon as their domestic nature has become evident (paragraph 26). Also, where a temporary permit granted by the FRA has been revoked by the Foreign Intelligence Court, all intelligence collected on the basis of that permit must be immediately destroyed (paragraph 27).

146. Although the FRA may maintain databases for raw material containing personal data up to one year, it has to be kept in mind that raw material is unprocessed information. That is, it has yet to be subjected to manual treatment. The Court accepts that it is necessary for the FRA to store raw material before it can be manually processed. At the same time, the Court stresses the importance of deleting such data as soon as it is evident that it lacks pertinence for a signals intelligence mission.

147. In sum, examining the legislation on storing, accessing, examining, using and destroying intercepted data, the Court is satisfied that it provides adequate safeguards against abuse of treatment of personal data and thus

serves to protect individuals' personal integrity (cf. *Roman Zakharov*, cited above, §§ 253-256; and *Kennedy*, cited above, §§ 162-164).

(vi) *Conditions for communicating the intercepted data to other parties*

(α) The parties' submissions

148. The applicant submitted that the conditions for communicating data left a large discretion to the FRA, for instance through the lack of specification as regards the foreign authorities and international organisations to whom data could be communicated.

149. The Government maintained that the procedures for communicating data, including the communication to other states and international organisations as part of Sweden's international cooperation, contained sufficient safeguards and that supervision was provided by the Foreign Intelligence Inspectorate.

(β) The Court's assessment

150. With regard to the communication of intercepted data to other parties, the purpose of signals intelligence naturally demands that it may be reported to concerned national authorities, in particular the authority which ordered the mission. Furthermore, given the context – the collection of intelligence on foreign circumstances that may have an impact on Swedish national security and other essential national interests as well as the country's participation in international security operations – it is evident that there must be a possibility of exchanging intelligence collected with international partners. Thus, the FRA Personal Data Processing Act allows the communication of personal data to other states or international organisations if necessary for the activities of the FRA within international defence and security cooperation and as long as it is not prevented by secrecy. Further discretion is given to the Government, which may decide to communicate personal data to states or organisations in other cases when necessary for the activities of the FRA, thus presumably in cases where such communication would otherwise be prevented by rules of secrecy. The FRA Personal Data Processing Ordinance adds that such disclosure is permitted for the benefit of the Swedish Government and Sweden's comprehensive defence strategy as long as it does not harm Swedish interests (see paragraph 35 above). The relevant provision of the Public Access to Information and Secrecy Act contains an exception to the rule of secrecy in relation to foreign authorities and international organisations in cases where an express legal provision allows disclosure or when the information in an analogous situation may be given to a Swedish authority and the disclosing authority finds it to be consistent with Swedish interests (paragraph 58). Thus, whereas national interests are taken into account, the legislation does not indicate that possible harm to the individual concerned must be

considered. Furthermore, the legislation only in very broad terms mentions that the data may be communicated to “other states or international organisations”; there is no provision requiring the recipient to protect the data with the same or similar safeguards as those applicable under Swedish law. Also the situation where data may be communicated – when necessary for “international defence and security cooperation” – opens up for a rather wide scope of discretion. In the Court’s view, the mentioned lack of specification in the provisions regulating the communication of personal data to other states and international organisations gives some cause for concern with respect to the possible abuse of the rights of individuals. On the whole, however, the Court considers that the supervisory elements described below sufficiently counterbalance these regulatory shortcomings.

(vii) *Supervision of the implementation of secret surveillance measures*

(α) The parties’ submissions

151. The applicant, pointing to the findings of the National Audit Office, submitted that the Foreign Intelligence Inspectorate’s own documentation of its supervisory work was scarce and that the Inspectorate lacked specified goals.

152. The Government submitted that an assessment of the report of the National Audit Office had been communicated to Parliament. The Office’s overall conclusion was that the Inspectorate had been given the necessary prerequisites to carry out its supervisory functions in an efficient and effective manner. The FRA had taken the Inspectorate’s views seriously and implemented measures accordingly. As to the Inspectorate’s goals, these were clearly specified in the legislation.

(β) The Court’s assessment

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

154. As to the requirement of independence, the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it has found sufficiently independent the bodies composed of members of Parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by Parliament or by the Prime Minister (see *Roman Zakharov*, cited above, § 278, with further references).

155. As regards the supervisory body's powers and competence, it is essential that it has access to all relevant documents, including closed materials, and that all those involved in interception activities have a duty to disclose to it any material required. Other important elements to take into account when assessing the effectiveness of the supervision are the supervisory body's powers with respect to any breaches detected and the possible public scrutiny of its activities. Moreover, it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples (see *Roman Zakharov*, cited above, §§ 281-283, with further references).

156. The members of the Foreign Intelligence Inspectorate are appointed by the Government on terms of at least four years and the president and vice-president are current or former permanent judges. The other members are suggested by the parliamentary party groups (see paragraph 37 above). The Court, therefore, finds no reason to question the independence of the Inspectorate.

157. The Inspectorate shall examine in particular the search terms used, the destruction of intelligence and how reports are communicated; the FRA shall report to it the search terms which directly relate to a specific natural person (see paragraph 36 above). The Inspectorate has access to all relevant documents (paragraph 39). It is within its powers to decide that the collection of intelligence shall cease or that information collected shall be destroyed, if during an inspection it becomes evident that the collection has not been in accordance with a particular permit; though, as of yet, no such measure has proved necessary (paragraphs 36 and 39). The Inspectorate is also in charge of the signal carriers, which includes ensuring that the FRA is only provided with access to signal carriers insofar as such access is covered by the permit (paragraph 24). The Inspectorate is to forward to the FRA, and if needed to the Government, any opinions or suggestions for measures to which the inspections give rise (paragraph 38).

158. The Court considers that the supervision of the Foreign Intelligence Inspectorate is of particular value in ensuring that the provisions applicable to the activities of the FRA are respected and that, generally, signals intelligence is performed in a manner which offers adequate safeguards against abuse. The above-mentioned rules governing the work of the Inspectorate indicate that it has been given sufficient powers to carry out this task. Moreover, contrary to the applicant's claim, the Court understands the report of the National Audit Office as concluding that the Inspectorate has been able to carry out its supervisory task efficiently. The Office also found that the FRA has taken the Inspectorate's views and suggestions seriously and have implemented measures based on them (see paragraph 40 above). The Court is therefore satisfied that the Inspectorate's supervision is efficient, not only in theory but also in practice.

159. The Court also finds that the Inspectorate's activities are open to public scrutiny. Beyond the audit provided by the National Audit Office, the Inspectorate submits annual reports to the Government on its activities; these reports are available to the public (see paragraph 38 above).

160. As regards personal data, further supervisory functions are provided by the Data Protection Authority. The Authority has on request access to personal data that is processed, documentation on the treatment of personal data along with the security measures taken on such treatment and access to the facilities connected to the processing of personal data. If the Authority finds that personal data is or could be processed illegally, it shall take remedial action through remarks to the FRA. The Authority may also apply to an administrative court to have illegally processed personal data destroyed (see paragraph 43 above). The Authority's supervision led to reports published in 2010 and 2016, in which some aspects of the FRA's activities were criticised. Issues of personal data and personal integrity, however, were generally considered to have been dealt with in a satisfactory manner (paragraphs 59-60).

161. Having regard to the above, the Court finds that the supervisory elements provided by the Foreign Intelligence Inspectorate and the Data Protection Authority fulfill the requirements on supervision in general. Moreover, the Parliamentary Ombudsmen and the Chancellor of Justice have general supervisory responsibilities in regard to the FRA.

(viii) Notification of secret surveillance measures

(α) The parties' submissions

162. The applicant submitted that the obligation on the FRA to notify natural persons when search terms directly related to them had been used was void of any practical meaning, since notifications had never been made due to secrecy.

163. The Government confirmed that a notification had never been given by the FRA for reasons of secrecy, but submitted that this was compensated by the remedy according to which the Foreign Intelligence Inspectorate could check at the request of an individual whether his or her communication had been subject to signals intelligence.

(β) The Court's assessment

164. The Court reiterates that it may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods

and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not “necessary in a democratic society”, as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (see *Roman Zakharov*, cited above, § 287, with further references).

165. The Court, mindful of the fact that the applicant is not a natural person, notes that, in theory, the FRA is obliged to inform a natural person, if search terms directly related to him or her have been used, about when and why the collection took place. The person shall be notified as soon as it can be done without detriment to the foreign intelligence activities, but at the latest one month after the signals intelligence mission was concluded. However, the obligation to notify does not apply where secrecy applies. The parties, as well as the Data Protection Authority in its report of 6 December 2010 (see paragraph 59 above) and the Signals Intelligence Committee in its report of 11 February 2011 (paragraph 64), have confirmed that in practice a notification has never been made, due to secrecy. Thus, the Court agrees with the applicant that the obligation on the FRA to notify individuals lacks practical significance.

166. The Court has previously found that the absence of a requirement to notify the subject of interception of postal and telephone communications at any point in time or in any circumstances was incompatible with the Convention, in that it deprived the subject of the interception an opportunity to seek redress for unlawful interferences with his or her rights under Article 8 and rendered the remedies available under national law theoretical and illusory rather than practical and effective (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, §§ 90 and 91). By contrast, in the case of *Kennedy*, the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his or her communications were being or had been intercepted could complain about an unlawful interception to a tribunal, whose jurisdiction did not depend on notification to the subject that there had been an interception of his or her communications (*Kennedy*, cited above, § 167).

167. Taking into account that the requirement to notify the subject of secret surveillance measures is not applicable to the applicant and is, in any event, devoid of practical significance, the Court accordingly finds it pertinent to examine the issue of notification together with the remedies available in Sweden; two issues that are inextricably linked (see *Roman Zakharov*, cited above, § 286).

(ix) Available remedies

(α) The parties' submissions

168. The applicant submitted that persons who had availed themselves of the possibility to request an investigation by the Foreign Intelligence Inspectorate had received a standardised reply that no unlawful surveillance had taken place. The applicant also stressed that the Inspectorate had no power to order compensation to be paid. No complaints regarding signals intelligence conducted by the FRA had been received by the Data Protection Authority after 2009. In regard to the Parliamentary Ombudsmen, the Chancellor of Justice and the other remedies mentioned by the Government, the applicant did not see any prospects of success unless there was evidence to establish that an individual had in fact been subjected to unlawful interception.

169. The Government emphasised that Swedish legislation offered several remedies. Beyond the possibility for individuals to request the Foreign Intelligence Inspectorate to check if his or her communications had been intercepted, the FRA was obliged, upon request, to inform the individual if his or her personal data had been treated or not and to correct, block or destroy personal data that had not been processed in accordance with law. In addition, complaints could be addressed to the Parliamentary Ombudsmen and the Chancellor of Justice, who had the power to investigate that relevant laws had been properly applied and, in so doing, were entitled to have access to documents of courts and administrative authorities, including the Foreign Intelligence Court and the FRA. Although they could not render legally binding decisions, their opinions commanded great respect in Swedish society. Also the Data Protection Authority, aside from being the supervisory authority on the FRA's treatment of personal data, could examine individual complaints. Furthermore, it was possible for an individual to bring an action for damages, report a matter for prosecution and bring a claim for compensation for violations of the Convention.

170. The International Commission of Jurists, Norwegian Section, submitted that remedies were not available to non-Swedish citizens, despite the fact that Swedish signals intelligence was focused on communications crossing the Swedish border.

(β) The Court's assessment

171. As the Court noted above, in the case of *Kennedy* the absence of a requirement to notify the subject of interception was compatible with the Convention, because the jurisdiction of the tribunal where the interception could be challenged did not depend on a prior notification (see *Kennedy*, cited above, § 167). Under the Signals Intelligence Act, the Foreign Intelligence Inspectorate, at the request of an individual, investigates whether his or her communications have been intercepted through signals

intelligence. If so, the Inspectorate verifies whether the interception and treatment of the information was in accordance with law. The Inspectorate must notify the individual that an investigation has been carried out. A request can be made by legal and natural persons regardless of nationality and residence (see paragraph 46 above). The Inspectorate has the power to decide that the collection of intelligence shall cease or that the intelligence shall be destroyed (paragraph 36).

172. Like in the *Kennedy* case, the Court is therefore satisfied that the remedy offered by the Foreign Intelligence Inspectorate is not dependent on prior notification. Although the Inspectorate may decide on the discontinuation of intelligence collection or the destruction of intelligence, unlike in *Kennedy*, it may not order compensation to be paid. However, with regard to compensation *per se*, the Court is mindful that there is an effective remedy in Sweden in that compensation from the State can be sought through the Chancellor of Justice or the domestic courts (see paragraph 53 above).

173. The Inspectorate examines if the individual's communications have been intercepted using signals intelligence. However, that examination is limited to the question whether or not the collection of intelligence was in accordance with law. The individual cannot obtain information whether his or her communications have actually been intercepted, only if there has been any unlawfulness. As pointed out by the applicant, the Inspectorate does not give any reasons for its conclusions reached on the issue of lawfulness. In contrast, the Court noted in *Kennedy* that the publication of the tribunal's legal rulings enhanced the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167). Moreover, as the decision of the Inspectorate is final, an individual who is not satisfied with the response from the Inspectorate may not seek review by, for instance, making an appeal to a court.

174. As to the remedies available directly through the FRA, the Court makes the following observations. The FRA is, upon request, required to inform an individual whether personal data concerning him or her has been processed. A request may be submitted once per calendar year. If such data has been treated, the FRA must specify what information on the individual is concerned, from where it was collected, the purpose of the treatment and to which recipients or categories of recipients the personal data has been reported (see paragraph 47 above). The Court notes that such an obligation is well-tailored to lower suspicion and concern among the general public that secret surveillance measures are being abused.

175. However, like the notification requirement, there is no obligation on the FRA to give information if secrecy applies to it. While the FRA's decisions may be appealed against to the Administrative Court in Stockholm (see paragraph 49 above), the Court has to assume that, like with other aspects of the FRA's activities, strict secrecy applies and, therefore, no

information on personal data is given to requesting individuals. In the absence of examples provided by the Government that illustrate the effectiveness of this remedy, the Court cannot find that it has practical importance. Furthermore, the FRA's procedure to correct, block or destroy personal data (paragraph 48) is dependent on the individual's knowledge that personal data has been registered and the nature of that data. Therefore, that remedy must be deemed to be ineffective in practice.

176. The Court notes, however, that Swedish law provides for several remedies of a general nature, in particular the possibility of addressing individual complaints to the Parliamentary Ombudsmen and the Chancellor of Justice (see paragraphs 51-53 above). These two institutions examine whether courts and authorities and their officials comply with laws and regulations and fulfil their obligations, not the least in regard to citizens' fundamental rights and freedoms. They are thus authorised to scrutinise the work of the courts and authorities involved in signals intelligence activities and there appears to be no impediment preventing an individual from introducing a complaint about an interference of privacy rights. The two institutions have the right of access to documents and other materials for the performance of their scrutiny. While their decisions are not legally binding, their opinions command great respect in Sweden. They also have the power to initiate criminal or disciplinary proceedings against public officials for actions taken in the discharge of their duties. As regards the Chancellor of Justice, it is also of relevance that a practice has developed in the last several years according to which the Chancellor may receive and resolve individual compensation claims for alleged violations of the Convention (paragraphs 53 and 172).

Moreover, the Court notes that the Data Protection Authority may receive and examine individual complaints under the Personal Data Act (paragraph 54).

177. To sum up, the Court observes that the Swedish remedies available for complaints relating to secret surveillance do not include the recourse to a court, save for an appeal against the FRA's decisions on disclosure and corrective measures, which remedies the Court have as such found to be ineffective. Furthermore, there does not appear to be a possibility for an individual to be informed of whether his or her communications have actually been intercepted or, generally, to be given reasoned decisions. Thus, in regard to the final stage of supervision of signals intelligence measures – reviews requested by individuals after the measures have been carried out – the Swedish system does not offer the same guarantees in these respects as the scrutiny in the United Kingdom, examined in the *Kennedy* case.

178. Nevertheless, there are several remedies by which an individual may initiate an examination of the lawfulness of measures taken during the operation of the signals intelligence system, notably through requests to the

Foreign Intelligence Inspectorate, the Parliamentary Ombudsmen and the Chancellor of Justice. In the Court's view, the aggregate of remedies, although not providing a full and public response to the objections raised by a complainant, must be considered sufficient in the present context, which involves an abstract challenge to the signals intelligence regime itself and does not concern a complaint against a particular intelligence measure. In reaching this conclusion, the Court attaches importance to the earlier stages of supervision of the regime, including the detailed judicial examination by the Foreign Intelligence Court of the FRA's requests for permits to conduct signals intelligence and the extensive and partly public supervision by several bodies, in particular the Foreign Intelligence Inspectorate.

(x) *Conclusion*

179. The Court is mindful of the potentially harmful effects that the operation of a signals intelligence scheme may have on the protection of privacy. Nevertheless, the Court acknowledges the importance for national security operations of a system such as the one examined in the present case. It notes, in this respect, the similar conclusions drawn by the Venice Commission (see paragraph 69 above). Having regard to the present-day threats being posed by global terrorism and serious cross-border crime as well as the increased sophistication of communications technology, the decision to set up a bulk interception regime in order to identify such threats was one which fell within the respondent State's margin of appreciation. As noted above (paragraph 112), in deciding on the type of regime necessary, the margin afforded was a wide one.

180. As noted simultaneously, the State's discretion in operating the interception regime is more narrow. When examining the Swedish system of signals intelligence *in abstracto*, the Court has had regard to the relevant legislation and the other information available in order to assess whether, on the whole, there are sufficient minimum safeguards in place to protect the public from abuse. While the above assessment has disclosed some areas where there is scope for improvement – notably the regulation of the communication of personal data to other states and international organisations (see paragraph 150 above) and the practice of not giving public reasons following a review of individual complaints (paragraphs 173 and 177) – the Court is of the opinion that the system reveals no significant shortcomings in its structure and operation. The regulatory framework has been reviewed several times, in order to expand the use of signals intelligence but also, more importantly, with the aim to enhance protection of privacy. It has developed in such a way that it minimises the risk of interference with privacy and compensates for the lack of openness. In particular, the scope of the signals intelligence measures and the treatment of intercepted data are clearly defined in law, the authorisation procedure is detailed and entrusted to a judicial body and there are several independent

bodies tasked with the supervision and review of the system. The Court's finding that the system reveals no significant shortcomings is the result of an examination *in abstracto* and does not preclude a review of the State's liability under the Convention where, for example, the applicant has been made aware of an actual interception.

181. Accordingly, making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security, the Court finds that the Swedish system of signals intelligence provides adequate and sufficient guarantees against arbitrariness and the risk of abuse. The relevant legislation meets the "quality of law" requirement and the "interference" established can be considered as being "necessary in a democratic society". Furthermore, the structure and operation of the system are proportionate to the aim sought to be achieved.

There has accordingly been no violation of Article 8 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

182. The applicant complained that it has had no effective domestic remedy through which to challenge the violation of its rights under Article 8 of the Convention. The applicant relied on Article 13 of the Convention, which reads as follows:

"Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

183. The Government contested that argument.

184. Having regard to the findings under Article 8 (see, in particular, paragraph 178 above), the Court considers that, although the present complaint is closely linked to the complaint under Article 8 and therefore has to be declared admissible, it raises no separate issue under Article 13 of the Convention.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Joins* to the merits the Government's objection regarding the applicant's lack of victim status and *declares* the application admissible;
2. *Dismisses* the Government's above-mentioned objection;
3. *Holds* that there has been no violation of Article 8 of the Convention;

4. *Holds* that there is no need to examine separately the complaint under Article 13 of the Convention.

Done in English, and notified in writing on 19 June 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Stephen Phillips
Registrar

Branko Lubarda
President