Strasbourg, 15 December 2015 **CDL-AD(2015)011**

Study No. 719/2013 Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

REPORT

ON THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES

Adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015)

on the basis of comments by

Mr Iain Cameron (Member, Sweden)

TABLE OF CONTENTS

Executive summary

1. *The scope of the study*. As a result of the processes of globalisation and creation of the Internet, internal and external security threats may no longer be easily distinguished. Significant threats may come from non-state actors. Consequently, one of the most important developments in intelligence oversight in recent years has been that signals intelligence or SIGINT no longer relates exclusively to military and external intelligence, but also falls to some extent into the domain of internal security. Thus, signals intelligence can now involve monitoring "ordinary telecommunications" (it is "surveillance") and it has a much greater potential for affecting individual human rights. Different states organise their signals intelligence function in different ways. The summary which follows discusses issues generally, and should not be seen as asserting that all states follow a particular model of signals intelligence, or regulate it in a particular way.

2. *Is there a need for improved democratic control?* Strategic surveillance involves access both to Internet and telecommunications content and to metadata (all data not part of the content of the communication). It begins with a task being given to the signals intelligence agency to gather intelligence on a phenomenon or a particular person or group. Very large quantities of content data and metadata are then collected in a variety of different ways. The bulk content is subjected to computer analysis with the help of "selectors". These can relate to persons, language, keywords concerning content (industrial products, for example) and communication paths and other technical data.

3. Unlike "targeted" surveillance (covert collection of conversations by technical means (bugging), covert collection of the content of telecommunications and covert collection of metadata), strategic surveillance does not necessarily start with a suspicion against a particular person or persons. Signals intelligence aims to inform foreign policy generally and/or military/strategic security, and does not necessarily aim at investigating internal security threats. It has a proactive element, aiming at finding or identifying a danger rather than merely investigating a known threat. Herein lies both the value it can have for security operations, and the risks it can pose for individual rights.

4. Agencies engaged in signals intelligence tend to have the bulk of the intelligence budget, and they produce most intelligence, but the systems of oversight over them have tended to be weaker. There are a variety of explanations for this. Firstly, it is argued that access to mere metadata does not seriously affect privacy, and neither does access to content data because this is done by computerised search programmes ("selectors"). However, metadata can reveal much about private life, and the content selectors can be designed to collect information on specific human beings and groups. Secondly, telecommunications used to be mainly via radio, with an ensuing lower level of privacy expectations; however, the vast bulk of telecommunications now take place via fibre-optic cables. Thirdly, while strategic surveillance is aimed at external communications, it was argued that it is the privacy of non-citizens or non-residents which is affected; however, leaving aside the issue of whether such a distinction is acceptable under the European Convention on Human Rights (ECHR), for technical reasons there is an inevitable mixing of internal and external communications, and an ensuing risk of circumvention of tougher domestic controls and oversight which might exist over "ordinary" surveillance. Fourthly, controls have been weaker on account of the technical complexity and rapid technological growth of the area. It should be borne in mind, however, that if this sector is left unregulated, it will be the intelligence agency itself instead of the legislature which carries out the necessary balancing of rights, with the risk of erring on the side of over-collecting intelligence. The fifth reason is that various factors – too rapid growth in the size of a signals intelligence agency, rapid growth in technology, loss of institutional memory, political pressure to secure quick results – may adversely impact the integrity and professionalism of the staff. Finally, signals intelligence is an international co-operative network, which creates specific oversight problems.

5. Strategic surveillance is not necessarily “mass” surveillance but can be when bulk data are collected and the thresholds for accessing that data are set at a low level. Signals intelligence agencies tend to possess much more powerful computing facilities and thus have a greater potential to affect privacy and other human rights. They thus need proper regulation in a *Rechtsstaat*.

6. *Jurisdiction.* The collection of signals intelligence may legitimately take place on the territory of another state with its consent, but might still fall under the jurisdiction of the collecting state from the viewpoint of human rights obligations under the ECHR. At any rate, the processing, analysis and communication of this material clearly falls under the jurisdiction of the collecting state and is governed by both national law and the applicable human rights standards. There may be competition or even incompatibility between obligations imposed on telecommunications companies by the collecting state and data protection obligations in the territorial state; minimum international standards on privacy protection appear all the more necessary.

7. Accountability and organisation. Signals intelligence is expensive and requires sophisticated technical competence. Hence, while all developed states nowadays require a defensive function – cybersecurity – only some have an offensive signals intelligence capacity, either in the form of a specialist signals intelligence agency or by allocating a signals intelligence task to their external intelligence agency.

8. *Form of the mandate.* Most democratic states have placed at least part of the mandate of the signals intelligence function in their primary legislation, as required by the ECHR. More detailed norms or guidelines are normally set out in subordinate legislation promulgated either by the executive (and made public) or by the head of the relevant agency (and kept secret). There may be issues relating to quality of the law (foreseeability, etc) in this respect.

9. *Content of the mandate.* The mandate of a signals intelligence agency may be drafted in very broad terms to allow collection of data concerning “relevant” “foreign intelligence” or data of “relevance” to the investigation of terrorism. Such broad mandates increase the risk of over-collection of intelligence. If the supporting documentation is inadequate, oversight becomes very difficult.

10. Collection of intelligence for “the economic well-being of the nation” may result in economic espionage. Strategic surveillance is useful however in at least three areas of business activity: proliferation of weapons of mass destruction (and violation of export control conditions generally), circumvention of UN or EU sanctions, and aggravated money laundering. A clear prohibition of economic espionage, buttressed by effective oversight and the prohibition on letting the intelligence agencies be tasked by the government departments or administrative agencies involved in promoting trade, would be useful prevention mechanisms.

11. Bulk transfers of data between states occur frequently. In order to avoid circumvention of rules on domestic intelligence gathering, it would be useful to provide that the bulk material transferred can only be searched if all the material requirements of a national search are fulfilled, and this is duly authorised in the same way as searches of bulk material obtained through national searches.

12. Government control and tasking. The identity of the taskers depends on the nature of the intelligence sought (diplomatic, economic, military and domestic). Taskers should not, however, be regarded as external controls.

13. *Network accountability.* Due to their different geographical locations and the nature of the Internet, states frequently collect data which is of interest to other states or have access to different parts of the same message. The links between allied states as regards signals intelligence may be very strong. The "third party" or "originator rule" may thus be a serious obstacle to oversight and should not be applied to oversight bodies.

14. *Accountability and the case law of the European Court of Human Rights.* The European Convention on Human Rights consists of minimum standards, and it is only a point of departure for European states, which should aim to provide more extensive guarantees. The European Court of Human Rights ("the Court") has not defined national security but has gradually clarified the legitimate scope of this term. In its case law on secret measures of surveillance, it has developed the following minimum safeguards to be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; definition of the categories of people liable to have their telephones tapped and a limit on the duration of telephone tapping; 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 the tapes destroyed.

15. The Court's case law on strategic surveillance is so far very limited, although there is also national case law and the practice of oversight bodies based on the ECHR. Several of the standards related to ordinary surveillance have to be adapted to enable them to apply to strategic surveillance. The first safeguard (applicable only to states which allow the use of signals intelligence to investigate crimes) is that the offences which may be investigated through signals intelligence should be enumerated, and thus provision should be made for the destruction of data which might incidentally be gathered on other offences. The exception of transferring data to law enforcement should be narrowly defined and subject to oversight.

16. Another safeguard is a definition of the categories of people liable to have their communications intercepted. The power to contact chain (that is, identify people in contact with each other) should be framed narrowly: contact chaining of metadata should normally only be possible for people suspected of actual involvement in particularly seriously offences, such as terrorism. If the legislature nonetheless considers that such a widely framed contact-chaining power is necessary, then this must be subject to procedural controls and strict oversight.

17. As regards searches of content data, there are particular privacy implications when a decision is being considered to use a selector which is attributable to a natural person (for example, his or her name, nickname, e-mail address, physical address, etc.). Strengthened justification requirements and procedural safeguards should apply, such as the involvement of a privacy advocate. The safeguard is also relevant as regards subsequent decisions to transfer intelligence obtained by strategic surveillance to internal security agencies, to law enforcement or to foreign services.

18. Interception of privileged communications by means of signals intelligence is particularly problematic, as is use of signals intelligence against journalists in order to identify their sources. Methods must be devised to provide lawyers and other privileged communicants and journalists with some form of protection, such as requiring a high, or very high, threshold before approving signals intelligence operations against them, combined with procedural safeguards and strict external oversight.

19. The safeguard of setting out time limits is not as meaningful for strategic surveillance as it is for ordinary surveillance. Periods of surveillance tend to be long, and continually renewed. Retention periods also tend to be long: data originally thought to be irrelevant may, as a result of new data, come to be seen as relevant. Provision could be made for a requirement to make periodic internal reviews of the (continued) need to retain data. To be meaningful, such a requirement must be backed up by external oversight.

20. Two very significant stages in the signals intelligence process where safeguards must apply are the authorisation and follow-up (oversight) processes. That the latter must be performed by an independent, external body is clear from the Court's case law. The question which arises here is whether even the authorisation process should be independent.

21. *Internal and governmental controls as part of overall accountability systems.* For a number of reasons, it has been particularly tempting to rely primarily on internal controls in the area of strategic surveillance, but these are insufficient. Generally speaking, external oversight over signals intelligence needs to be strengthened considerably.

22. Parliamentary accountability. There are a number of reasons why parliamentary supervision of strategic surveillance is problematic. Parliamentarians have a lack of time to engage in the sort of standing oversight which is necessary and lack the technical expertise which is necessary to understand the area. The network character of co-operation between signals intelligence agencies also makes the activity more difficult for parliamentarians to supervise. All of these difficulties can be overcome, but more problematic is the fact that strategic surveillance involves an interference with individual rights. Supervision of such measures has traditionally been a matter for the judiciary.

23. A decision to use particular selectors resembles, at least in some ways, a decision to authorise targeted surveillance. As such, it can be taken by a judicial body or a body with a hybrid judicial/foreign policy competence. As regards follow-up (oversight), it is necessary to oversee decisions made by automated systems for deleting irrelevant data, as well as decisions by human analysts to keep the personal information collected, and to transfer it to other domestic and foreign agencies. This type of oversight is of a "data protection" character, most suitably assigned to an independent, expert administrative body, although this can, and should, be made accountable to the parliament.

24. *Judicial authorisation.* A system of authorisation needs to be complemented by some form of follow-up control that conditions are being complied with. This is necessary both because the process of refining selectors is dynamic and highly technical and because judges do not tend to see the results of the signals intelligence operations as these seldom lead to prosecutions. Thus the safeguards applying to a subsequent criminal trial do not become applicable.

25. *Accountability to expert bodies.* The boundary line between parliamentary, judicial, and expert bodies is not hard and fast; in some states, oversight bodies are a mixture of the three. Expert bodies have a particular role to play in ensuring that signals intelligence agencies comply with high standards of data protection.

26. *Complaints mechanisms.* Under the ECHR, a state must provide an individual with an effective remedy for an alleged violation of his or her rights. Notification that one has been subject to strategic surveillance is not an absolute requirement of Article 8 ECHR. If a state has a general complaints procedure to an independent oversight body, this can compensate for non-notification. There are certain requirements before a remedy can be seen as effective.

27. *Concluding remarks*. States should not be content with the minimum standards of the ECHR. Signals intelligence has a very large potential for infringing the right to private life and other human rights. It can be regulated in a lax fashion, meaning that large numbers of people are caught up in a trawl and intelligence on them is retained, or can be regulated relatively tightly, meaning that the actual infringement of the right to private life and other human rights is minimised. The Swedish and German models have definite advantages over the other models studied from this perspective. In any event it is necessary to regulate the main elements in statute form and to provide for effective mechanisms of oversight. The national legislature must be given a proper opportunity to understand the area and ensure the necessary balances.

I. Introduction

28. In 2007, upon an invitation of the Committee of Ministers of the Council of Europe, the European Commission for Democracy through Law (Venice Commission) adopted a report on the Democratic Oversight of the Security Services (CDL-AD(2007)016, hereafter "2007 report").

29. In November 2012, the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe requested the Venice Commission to prepare an update of that report. Mr Iain Cameron (member, Sweden) acted as rapporteur.

30. In May 2013, a query was addressed to all members of the Venice Commission on relevant developments in oversight of internal security. Information was received from Mr Sörensen (member, Denmark), Mr Haenel (member, France) and Mr Hoffmann-Riem (member, Germany). Useful information has also been received from Ms Sarah Cleveland (member, USA) and Professor Martin Scheinin, former United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, and representative of the International Association of Constitutional Law at the Venice Commission from March 2011 to June 2014.[1]

31. In the autumn of 2014, exchanges of views were held between Mr Cameron and the network of experts of the Fundamental Rights Agency of the European Union within the framework of its project on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies.

32. The update report, dealing mainly with signals intelligence, but also with certain developments in oversight generally, was discussed at the meeting of the Sub-commission on Democratic Institutions on 19 March 2015 and subsequently adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015).

II. The scope of the present study – definitions

33. The most significant development, since the Commission's earlier study of 2007 on the democratic oversight of the security services relates to signals intelligence. Signals intelligence or SIGINT is a collective term referring to means and methods for the interception and analysis of radio (including satellite and cellular phone) and cable-borne communications. Traditionally, signals intelligence was mainly used to obtain military (defence) intelligence and, secondarily, foreign or diplomatic intelligence. Thus, it was primarily the domain of military or external intelligence agencies. However, as a result of processes of globalisation, together with the creation of the Internet, the distinctions between

[1] The rapporteur would also like to express his gratitude to Mr Douglas Cantwell for helpful comments and information on the US law and practice and Ms Hilde Bos regarding the Dutch oversight practice.

internal and external security are no longer so clear cut. Moreover, at least since the terrorist attacks of 11 September 2001, it has become understood that significant threats to national security can be posed by non-state actors.[2] As explained further in the next section, signals intelligence now has considerable impact on internal security and on the human rights of individuals.

34. The term "strategic surveillance" is often used to indicate that signals intelligence can now involve monitoring "ordinary communications" and this term is used in the present report.[3] The military elements of signals intelligence – the monitoring of the disposition of foreign military units, their preparedness, etc. might still be a significant part of the functions of a signals intelligence agency,[4] but these will not be part of the present report.[5]

35. The term "signals intelligence agency" is occasionally used in this report. As explained below, section V(C), the function of collecting strategic surveillance can be entrusted to a variety of different types of body, but what is being referred to is the function, irrespective of how this is organised. Whereas all states have an internal security function, not all states have the resources, or inclination, to have a strategic surveillance function. Thus, the comments on best practices regarding strategic surveillance are primarily addressed to those states which have such a function.

36. The report on democratic oversight of signals intelligence agencies should be read together with the report of 2007, as updated in 2015 (CDL-AD(2015)010), which sets out in detail the general principles of security oversight.

III. Is there a need for (improved) democratic control?

A. What is strategic surveillance?

37. The focus of the 2007 report was the oversight of security agencies. It began by explaining briefly what was being overseen and why, in other words: how security agencies gathered and analysed intelligence. Internal security agencies use, *inter alia* covert collection of conversations by technical means (bugging), covert collection of the content of telecommunications and covert collection of metadata.[6] The same must be done for strategic surveillance.

---

[2] See the 2007 report, para. 64, and "Liberty and Security in a Changing World, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies", 12 December 2013, p. 177. The latter report also, more controversially, questions whether the distinction between armed conflict and peace continues to be so viable.

[3] This follows the terminology of the German legislation, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) (Act Restricting the Privacy of Correspondence, Posts and Telecommunications), 26 June 2001 (Federal Law Gazette I, p. 1254, revised 2298), last amended by Article 1 of the Act of 31 July 2009 (Federal Law Gazette I, p. 2499 (hereinafter, "G 10 Act"). This terminology was also adopted by the European Court of Human Rights (see below, section VI). However, the term in the present report is given a slightly broader meaning than it has in the German legislation, to cover even the use of signals intelligence to collect information on identified individuals and groups.

[4] For example, the Swedish Signals Intelligence Agency, Försvarets Radio Anstalt (FRA), estimates that at least 50% of its work has this military character.

[5] This is appropriate bearing in mind the fact that Article 1d of the Statute of the Council of Europe provides that the organisation does not have competence in matters of defence. Human rights issues can arise as a consequence of military uses of signals intelligence, e.g. where data produced as a result of strategic surveillance is used as the basis for a military response to a non-state threat, such as a drone attack on suspected terrorists. However, this issue will not be examined.

[6] Simply put, metadata is "data on data". In the context of telecommunications it is usually seen as all data not part of the content of the communication (although the boundaries between the two are not always clear). It means such things as numbers called, duration of call, location of the caller and the recipient, etc.

38. All of these methods of surveillance used by internal security agencies are "targeted" in the sense that they begin with the hypothesis that a person, or persons, have committed, are committing, or are planning the commission of a security offence, or, for states which do not limit the mandate of the security agency to investigating offences, are engaged in conduct threatening national security. All these methods interfere with Article 8 ECHR and other human rights and so a threshold is set in the law for initiating surveillance: there must be concrete facts indicating the criminal offence/security-threatening conduct, and the investigators must have "probable cause", "reasonable suspicion" or satisfy some similar test.

39. The decision to permit surveillance tends to be taken by a person or body removed from the day-to-day conduct of the investigation, usually a court, but in some states a prosecutor, or a government minister. The permission is limited to a particular person, persons, or location and is given for a set period of time. The procedure before the permission-granting body is invariably secret. For interceptions of the content of communications, or metadata in internal security or law-enforcement operations, the telecommunications company is ordered to facilitate the interception, or hand over the metadata. If the telecommunications surveillance, together with other material, leads to sufficient evidence being gathered of involvement in security crime, then a prosecution may be brought. The telecommunications interception will then (in most states) be admissible evidence. Where there is insufficient evidence that an offence has been or is being committed, but reasonable suspicions remain, an investigation can continue. Security investigations tend to be longer lasting than ordinary law-enforcement investigations. Where an investigation involving surveillance terminates, many states make a requirement that, after a given period of time, a person subject to such surveillance should be notified (if this can be done without imperilling investigation methods or sources).

40. At various stages in the proceedings, safeguards exist to weigh human rights against effectiveness in investigation of crime or threats against national security, to reduce the intrusion into human rights as much as possible and to limit the scope for abuse of power.

41. The safeguards for obtaining metadata for law enforcement or internal security purposes have tended to be less than those applicable to bugging or interception of the content of telecommunications, on the basis that access to metadata has been argued to involve less of an interference with privacy and other human rights.

42. Strategic surveillance involves access both to Internet and telecommunications content and to metadata. It begins with a task being given to the signals intelligence agency to gather intelligence on a phenomenon or a particular person or group. Very large quantities of content data, and metadata, are then filtered and collected in a variety of different ways.[7] The bulk content is subjected to computer analysis with the help of "selectors".[8] These can relate to language, persons, keywords concerning content (e.g. industrial products), communication paths and other technical data or all of these. This is one of the important stages for balancing personal integrity concerns against other interests. In practice, whether

[7] For technical details, see M. Cayford, C. van Gulijk and P.H.A.J.M. van Gelder, "All swept up: An initial classification of NSA surveillance technology", in Nowakowski et al. (eds), *Safety and Reliability: Methodology and Applications*, Taylor and Francis, 2015, part of the SURVEILLE research project. An explanation of the SIGINT process as a whole can be found in Chapter 2 of the report of the National Research Council of the National Academies, *Bulk Collection of Signals Intelligence: Technical Options*, National Academy Press, 2015 (hereinafter: "National Research Council").

[8] The National Research Council uses "discriminant" to refer to terms employed to filter collection; as the collection process occurs in real time, the terms must of necessity be simpler than those used to search the bulk collected data ("selectors"). A "query" directed to collected data can combine several "selectors" (ibid., pp. 38-9). For the sake of simplicity, "selector" is used for both terms in the present report.

this process adequately limits unnecessary intrusion into innocent personal communications depends on both the relevance and specificity of the selector used and the quality of the computer algorithm employed to sort for relevant data within the parameters chosen (however, see also paragraph 58 below).

43. The bulk metadata is analysed to identify communication patterns This usually takes the form of checking whether previously identified suspect telephone numbers (X) are in contact with other numbers (Y) and then whether Y is in contact with other numbers (Z) (so-called "contact chaining"). Contact chaining by means of metadata analysis is also used for internal security and law-enforcement investigations, but, as shown below (section VI), there are (or can be) differences, both as regards the scope and quantity of the chaining and as regards the applicable safeguards for privacy.

44. After the initial computerised searching and deletion/refining, human analysts subject the data which is left to further analysis, deleting irrelevant material (often called "minimisation"). This is another important stage for balancing privacy concerns against other interests. The material left is further refined and added to with other intelligence material, to produce a final product which is then stored for future use, disseminated, etc.

45. The body which can task the signals intelligence agency to produce the requested intelligence will usually be set out in law or subordinate legislation: it may be a government minister, a government department, the armed forces (or part thereof) or an external or internal security agency. Determining the selectors most likely to produce the requested intelligence is to a large extent a technical issue. Thus, devising the specific selectors used is usually seen as a matter for the signals intelligence agency. However, in recognition of the impact the bulk collection and the use of selectors can have on human rights, several states now provide for a separate authorising body. This body can authorise either the bulk collection, or the list of selectors to be used for particular intelligence gathering operations, or both. The authorising body may be a government minister (which obviously may be the same body as the tasking body) or an external judicial or quasi-judicial body.

46. The process of devising and refining selectors is dynamic. The signals intelligence agency continually tests search methods, communication channels, etc. anticipating and dealing with actual or potential countermeasures by the target. In the course of such testing, useful intelligence may also be obtained.

47. Strategic surveillance thus differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. It does not necessarily start with a suspicion against a particular person or persons. It can instead be proactive: finding a danger rather than investigating a known danger. Herein lays both the value it can have for security operations, and the risks it can pose for individual rights. Prosecution is not the main purpose of gathering intelligence. The intelligence is, however, stored and used in a number of ways which can affect human rights. Nonetheless, despite the differences between targeted and strategic surveillance, it is apparent that at various stages in the proceedings safeguards can exist, or can be created, to weigh privacy and other human rights against effectiveness in investigation of crime or threats against national security, to reduce the impact on human rights and to limit the scope for abuse of power.

B. Weaker controls over strategic surveillance?

48. In those states which have them, agencies engaged in signals intelligence tend to have the bulk of the intelligence budget, and produce most intelligence, but it is fair to say that they have tended to have weaker systems of oversight. There are a variety of explanations for this. The first has already been mentioned, namely that access to mere metadata is assumed not to seriously affect privacy. As shown below in this section, this is no longer

correct. As regards the privacy impact on access to the content communications, the argument has been made that, unlike when a human analyst listens to a telephone conversation, the application of computerised search programmes (the selectors) to bulk data does not involve an interference with privacy. However, this argument is incorrect, at least from a human rights perspective: the selectors are devised by human beings. While selectors aimed at identifying a product, such as a chemical precursor, do not have a direct impact on human rights, selectors attributable to individuals or groups do.[9]

49. A second, historical, explanation is the fact that international telecommunications used to be by means of radio. Expectations of privacy were generally less with radio.[10] However, the vast bulk of both national and international telecommunications is now by fibre-optic cable. Moreover, the amount of such traffic has increased enormously.

50. A third explanation is that strategic surveillance has grown out of military signals intelligence and is (or is intended to be) aimed at external (foreign) communications. Thus, it could be argued that interception of external communications primarily affected the privacy of non-citizens or non-residents. Whether, and if so, how, it is permissible to distinguish between citizens/residents on the one hand and non-citizens/non-residents on the other is considered below (section V(C)). Of course, monitoring how one's citizens' communicate with foreigners also means monitoring one's citizens. Anyway, most digital telecommunication is now automatically routed to the most convenient/cheapest routes, and/or goes via the Internet, meaning that communications which were previously internal (between individuals both present in the same state) now often cross national boundaries. And any communication with a foreign server, or by using a foreign Internet service provider (ISP), is in one sense an "international" communication. Even to the extent that internal and external threats can be distinguished, and as mentioned above, this is no longer so easy, the nature of telecommunications now means that significant amounts of "internal" communications are likely to be collected in the course of gathering up relevant "external" communications. Thus, this inevitable (for technical reasons) mixing of the internal and external becomes an important argument for improved controls over strategic surveillance. To put it another way, there is a risk of circumvention of tougher domestic controls and oversight which might exist over "ordinary" surveillance (see below V(C)).

51. A fourth explanation for the fact that weaker controls have applied has been the technical complexity and rapid technological growth of the area. It has been difficult for politicians and lawyers to understand how strategic surveillance works, how it affects privacy and other human rights and how to go about devising appropriate checks and balances. Where such an area is left unregulated, it is the security and intelligence agencies which end up doing the necessary balancing between different interests, not the legislature. And as pointed out in the 2007 report, security and intelligence agencies have a natural tendency to want more information.[11]

52. Fifthly, the primacy the executive has in many states in the areas of foreign policy and defence, either by virtue of the constitution, or *de facto*, by virtue of its control over information in these areas, can also have contributed to the lack of legislation in certain states. There is a link here to the third reason: it is likely that an agency which is designed to

[9] One can argue that the interference with private life arises not at the point that the data are collected, but first after automated minimisation processes have been applied to them. It is only the data which are retained after these processes which can be accessed. However, the mere collection of the data can affect other human rights (below, paras. 62-63, 92).

[10] The "reasonable expectations of privacy" test can be criticised, *inter alia* for making privacy contingent on technology. At least for states bound by the ECHR, no distinctions between radio and cable traffic can be drawn today, see below section VI.

[11] 2007 Report, paragraph 58.

provide intelligence to inform foreign policy generally and/or military/strategic security has been perceived as requiring a different form of oversight than an agency which is designed to provide intelligence on internal security threats and which has (or has had) a more palpable impact on the human rights of citizens or residents. An agency which has not had to think so much about how its work impacts upon human rights, i.e. including foreigners' human rights, has now had to start thinking in such terms. By contrast with the rapid technological growth in the area, the creation of a "rights-respecting" organisational culture is a relatively slow process.

53. Sixthly, since the terrorist attacks of 11 September 2001, the budgets and manpower of many signals intelligence agencies have been increased significantly. As the 2007 report notes,[12] such rapid expansion creates various risks. The natural tendency of intelligence agencies to gather too much intelligence can be insufficiently held in check, especially if the integrity and professionalism of the staff (the main restraint on too much intelligence gathering) is weakened by political pressure.

54. Finally, signals intelligence is to a significant extent an international co-operative network, and there are particular problems involved in overseeing an international network (see below, section V(E)). However, one can note here that the allegations made of lack of control over signals intelligence also focused attention on intelligence exchange. Although it is argued that data transferred are covered by equivalent national standards of personal integrity protection, "national security" is routinely an exception to these national standards. A possible consequence of this is that, when data are transferred, foreign intelligence and security agencies might not need to comply with any of the originator state's rules on data protection.

C. Mass surveillance?

55. Bearing these points in mind, it is undoubtedly appropriate to have a proper discussion regarding oversight of strategic surveillance, and such discussions have been occurring in a number of states. The issue became particularly topical as a result of detailed allegations made by a former US National Security Agency (NSA) contractor, Edward Snowden, in June 2013. Fears were expressed as a result of these allegations that the activities of the NSA in particular, but also the equivalent signals intelligence agencies in other states, including several Council of Europe states, involved "mass surveillance". The concern caused by these allegations about NSA capabilities and practices was exacerbated by the fact that US companies dominate the Internet, and much Internet traffic is routed through the Internet "backbone" in the US. It led, *inter alia* to the UN General Assembly adopting a resolution on the right to privacy in the digital age,[13] an inquiry in the Liberty committee of the European Parliament[14] and the Parliamentary Assembly of the Council of Europe,[15] and to proposals made by service providers[16] and an NGO coalition[17] for global regulatory principles.

---

[12] 2007 Report, paragraph 64.

[13] General Assembly Resolution 68/167. "The right to privacy in the digital age", 18 December 2013. See also Report of the Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age", A/HRC/27/37, 30 June 2014.

[14] European Parliament, LIBE, "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs" (2013/2188(INI)), 21 February 2014.

[15] PACE, Committee on Legal Affairs and Human Rights, "Mass surveillance", Rapporteur: Mr Pieter Omtzigt (report April 2015).

[16] "Global Government Surveillance Reform: The Principles", 9 December 2013, available at: www.reformgovernmentsurveillance.com.

[17] "International Principles on the Application of Human Rights to Communications Surveillance". Final version May 2014, https://en.necessaryandproportionate.org/text.

56. Mass surveillance is not a legal term. It can be seen as a contrast to "targeted" surveillance (above). One associates the term with police states, such as Nazi Germany or the pervasive surveillance carried out by the secret police in the Soviet Union and Eastern Europe during the time of the Warsaw Pact states of the whole, or a large part of, the population.

57. One can argue, broadening the perspective, that strategic surveillance is only one part of an overarching trend towards more proactive surveillance of the population; gathering data on a large segment of the population, retaining it for a period of years and making it available for searches. Other such examples are legal requirements on companies to retain and make available airline passenger name record (PNR) data, telephony and Internet metadata and financial transactions.

58. Intercepting bulk data in transmission, or requirements on telecommunications companies to store and then provide telecommunications content data or metadata to law-enforcement or security agencies, involves, as such, an interference with the privacy and other human rights of a large proportion of the population of the world, as very many people are now using telecommunications.[18] Together with changed social behaviour, at least in the developed world – putting a large part of one's private life in social media and rarely turning off one's mobile phone – such data can provide a great deal more information about people, including information about the core of personal integrity than was the case when metadata consisted of lists of landlines called, and the duration of these calls.[19] Simply knowing that one's online behaviour is being recorded and may subsequently be scrutinised by law-enforcement or security agencies can and does affect a person's behaviour.

59. As far as metadata is concerned, for EU states, a recognition of the greater impact this entails on personal integrity came recently when the Court of Justice of the European Union (CJEU) annulled the EU data retention directive.[20] Courts in EU states have followed suit, stressing the need for improved controls over metadata collection.[21] Retention/transfer requirements for metadata also entail a certain chilling effect on freedom of expression and association and the right to seek information freely, all of which can be constitutional rights.[22]

60. However, at least from a European perspective, the main interference is with privacy/data protection[23] and the main interference with this occurs when the stored personal data are accessed in some way by law-enforcement/security and intelligence agencies and subjected to processing by them (or by the telecommunications companies on their behalf).

---

[18] Cf. UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 4th Annual Report, 23 September 2014, A/69/397, paras. 18-19; Council of Europe Commissioner for Human Rights, Comment, 24 October 2013.

[19] Cf. Opsahl K. (2013), "Why Metadata Matters", Electronic Frontier Foundation, www.eff.org/deeplinks/2013/06/why-metadata-matters, Tokmetzis, D., www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/. See also Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies) https://wcd.coe.int/ViewDoc.jsp?id=2074317.

[20] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* and *Seitlinger and Others*, 8 April 2014.

[21] See, e.g. Austrian Constitutional Court, decision G 47/2012 and others of 27 June 2014. In some cases, the negative judgments preceded that of the CJEU; see in particular, the judgment of the German Federal Constitutional Court (Bundesverfassungsgericht) in 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 regarding the data retention directive.

[22] See below, section VI.

[23] The relationship between privacy and data protection is not discussed in the present study. They are, for example, separate rights under the EU Charter of Fundamental Rights, whereas they are two different elements of the same right under Article 8 ECHR.

61. Having said this, the two interferences are obviously linked: a retention/transfer requirement creates a potential for mass surveillance. This becomes actual mass surveillance if the threshold requirements for permitting access to this data are set low, and the personal data of many people is in fact accessed. This applies irrespective of the agency or agencies doing the accessing. Metadata in particular can be subject to automated processing, which explains part of its value to law-enforcement and internal security agencies.

62. Compared to law-enforcement or internal security agencies, signals intelligence agencies tend to possess much more powerful computing facilities, and thus have an ability to process and analyse vast amounts of data. Their potential to engage in "mass surveillance" is thus correspondingly greater.

63. Whether, in fact, signals intelligence agencies are engaged in gathering intelligence on large numbers of people is the subject of dispute. The US Office of the Director of National Intelligence (ODNI) 2013 Transparency Report indicated that in that year, over 90 000 foreign individuals and entities were targeted under section 702 of the Foreign Intelligence Surveillance Act (FISA).[24] Such a target list compared to, say, 3 billion people regularly using the Internet and telecommunications communications, is relatively speaking, not "mass surveillance". However, one must also take into account first that "entities" means a much higher number of individuals, that the targets are in communication with other people and, second, the error rate, resulting in the collection of communications of people other than the direct targets. A (modest) error factor of 9 would give at least 810 000 individuals' communications being intercepted, stored and processed.[25] While diligent minimisation by human analysts should remove some of the obvious errors, it will certainly not remove them all, and one must not take for granted that the human minimisation is diligent, at least as far as foreigners are concerned (this may not be a prioritised task for the agency).[26] The global security responsibilities, and so intelligence needs, of the US must be borne in mind. Still, it seems apparent that the NSA collects and, even after minimisation, stores data on large numbers of people.

64. But the important issue is not determining whether or not this, and equivalent measures by other signals intelligence agencies is "mass surveillance"[27] – a term which anyway is not legal in character – but deciding how strategic surveillance should be properly regulated in a *Rechtsstaat*.

---

[24] See http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013. See further www.washingtonpost.com/world/national-security/us-releases-data-on-sensitive-surveillance-programs-for-first-time/2014/06/27/46bbd47e-fe3a-11e3-8176-f2c941cf35f1_story.html.

[25] Barton Gellman, Julie Tate, and Ashkan Soltani. "In NSA-intercepted data, those not targeted far outnumber the foreigners who are" *The Washington Post* (5 July 2014).

[26] Cf. Barton Gellman, "How 160,000 intercepted communications led to our latest NSA story", www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html.

[27] The National Research Council report instead uses the terms "bulk" and "targeted" collection. It is pointed out that it is misleading to say that any collection using selectors is "targeted", because using a wide selector (e.g. "Syria") will mean that a great deal of data are collected. Under their definition, it is not the amount of the data which makes them "bulk" but the fact that a (larger) proportion of extra data is collected beyond currently known targets, National Research Council, p. 33.

IV. Jurisdiction

65. Strategic surveillance is conducted both within the territory of a state and outside it, by units operating from military bases in allied states, embassies or in ships and aircraft on, respectively, over the high seas. The collection of intelligence on or over the high seas, or in the territory of another state, with that state's permission, will not be in violation of the customary international law norm of non-intervention.[28] However, the case law of the European Court of Human Rights, and the UN Human Rights Committee clarifies that human rights obligations under these treaties can extend to activities conducted wholly extraterritorially.[29] Collection facilities in military bases, or vessels situated outside national territory can thus also be within "jurisdiction" for states parties to these treaties.[30] In any event, the processing, analysis and communication of this material is clearly within national jurisdiction and is governed both by national law and states' applicable human rights obligations.[31]

66. Two further points should be noted here. It may be technically possible for an agency in one state (A) remotely to gain access to computers physically situated within the territory of another state (B), and use this access to plant malware on the computer, allowing it to be monitored. This technical capability does not alter the fact that the computer is within the territory of B, and clearly within its criminal and administrative law jurisdiction.[32] Thus, if A plants malware for security/law-enforcement purposes in computers in B, then this risks violating the norm of non-intervention if it is not done in compliance with B's law (if this is possible under the law of B at all).

67. Another related issue arises from the fact that a state (A) may impose legal obligations upon companies incorporated under its law offering computer services to individuals and companies in state B to make available the data generated as a result of these services to agencies in A for the purposes of law enforcement or protection of national security. Such

[28] There is still the question of proof. In *Weber and Saravia v. Germany*, Application No. 54934/00, decision of 29 June 2006, the applicants had argued that by intercepting private communications beginning and ending in another country the German authorities were violating international law. The Court considered that the term "law" refers back to national law, including rules of public international law applicable in the state concerned. However, the Court required proof in the form of "concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law" (para. 87). The Court in these circumstances found that the applicants failed to prove their allegations.

[29] For the ECHR, see *Ilaşcu and Others v. Republic of Moldova and Russia,* Application No. 48787/99, 8 July 2004, *Öcalan v. Turkey*, Application No. 46221/99, 12 May 2005, *Al-Saadoon and Mufdhi v. the United Kingdom*, Application no. 61498/08, 2 March 2010, *Al-Jedda v. the United Kingdom*, Application no. 27021/08, 7 July 2011, Hassan v. UK, Application No. 29750/09, 16 September 2014, Jaloud v. the Netherlands, Application No. 47708/08, 20 November 2014. In 2014, the Human Rights Committee stated: "The State party should: (a) Take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the [ICCPR], including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance;" (CCPR/C/USA/CO/4, para. 22). See also UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 4th Annual Report, 23 September 2014, A/69/397.

[30] See Venice Commission Opinion no. 363/2005, on the International Legal Obligations of Council of Europe Member States in Respect of Secret Detention Facilities and Inter-State Transport of Prisoners, adopted by the Venice Commission at its 66th Plenary Session (Venice, 17-18 March 2006), *Medvedyev and Others v. France,* 29 March 2010, *Hirsi Jamaa and Others v. Italy*, 23 February 2012.

[31] In *Weber and Saravia v. Germany*, the Court considered that "Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany" (para. 88).

[32] Cf. Convention on Cybercrime, 2001, ETS No. 185, Articles 2-6, 22.

disclosure obligations may be backed by criminal sanctions under A's law. This disclosure will not be "unauthorised", in the sense that the contract between the service provider and the individual/company which provides for maintaining the confidentiality of this data will usually make an exception for national regulatory legislation. However, the issue which arises here is the possible conflict which might arise between such legislation in A and data protection legislation which may be applicable in B (and which may also be criminally sanctioned). US companies dominate the provision of Internet services (such as Microsoft, Apple, Google, Facebook, Twitter), meaning that US disclosure obligations come under particular focus. In any event, the risk that companies are being placed under competing, or even incompatible obligations, is a good reason for attempting to reach minimum international standards on privacy protection.

V. Accountability – constitutional and organisational contexts

A. Organisation

68. As noted in the 2007 report, states differ as to how they organise their security functions and this is an important part of the context of oversight, as the oversight arrangements track the way the security function is organised. The cost of data storage and bandwidth has gone down rapidly but signals intelligence is still expensive, and requires sophisticated technical competence. As already mentioned, many states do not have this competence, or are unwilling to undertake the expenditure involved. All developed states nowadays nonetheless require a defensive – cybersecurity – function. For those states who have an offensive signals intelligence capacity, some states organise this in the form of a specialist signals intelligence agency (e.g. US, UK, Sweden), whereas in others the foreign (external) intelligence agency has this as one of its tasks (Germany, France). In the Netherlands, the civil and military intelligence and security services have created a combined team: the Joint SIGINT Cyber Unit.

B. Form of the mandate

69. Most democratic states, in recognition of the impact strategic surveillance has on human rights, have placed at least part of the mandate of the signals intelligence function in primary legislation.[33] As explained below in section VI, this is also a requirement in the case law of the European Court of Human Rights. More detailed norms, or guidelines, are normally set out in subordinate legislation promulgated by the executive (which, if in the form of executive orders, will usually be published) or by the head of the agency in question (which will usually be secret). The technical nature of the subject, and the international co-operation, by which bulk data are transferred between signals intelligence agencies, can give rise to quality of law issues (foreseeability, etc.). This arose, for example, as regards the mandate of the British signals intelligence, GCHQ, before the Strasbourg Court in 2008, and again, in 2014, before the British Investigatory Powers Tribunal, IPT (see below section VI).

C. Security priorities/the content of the mandate

70. How broadly or narrowly drafted the agency's mandate is, is a crucial part of limiting the scope for abuse. The mandate of the signals intelligence agency to a large extent determines the tasks of the external control and/or oversight body or bodies and this justifies dealing with it in some detail here. Where the mandate of a signals intelligence agency is framed very broadly to allow the collection of data concerning "relevant" "foreign intelligence" or data of "relevance" to the investigation of terrorism, then over-collection of intelligence is very likely (see 2007 report, paragraph 58). The US Privacy and Civil Liberties Oversight

[33] See, e.g. Sweden, Defence Intelligence Act (2000:133), Signals Intelligence Act (2008:717), Germany, G 10 Act, UK, Regulation of Investigative Powers Act (RIPA) 2000.

Board (PCLOB) found that the NSA had, lawfully, collected very large amounts of foreign intelligence under the section 702 programme (see below paragraph 117). However, the supporting documentation behind this collection was often inadequate. The agency had contented itself with justifying the foreignness of the target, not explaining in what ways the collection of intelligence about it would promote the national security of the US.[34] A similar conclusion was reached by the Dutch oversight body, the CTIVD.[35] The Dutch experience shows that even where the oversight body has the formal power to express opinions on the proportionality/appropriateness of particular intelligence gathering operations (below, section X), this is of little use if there is no documentation to analyse.

71. Signals intelligence operations aimed at obtaining intelligence on terrorism can usually be assumed to be better documented (partly because specific security or law-enforcement investigations are already in operation, and thus to some extent the supporting documentation is already there). However, as shown below in section VI, a threshold of, for example "information of relevance to terrorism" is significantly lower than a threshold that the individual being monitored must be involved in a specific terrorist offence (or at least criminal terrorist conduct of some sort).

72. Another issue related to the mandate is the distinction which has operated – particularly in the US, but even in other states[36] – between citizens and residents on the one hand, and non-citizens and non-residents on the other. This issue is relevant as regards possibly differential standards to be satisfied for targeting, but also as regards retaining, communicating, etc. data. Because of the frequency with which communications, in the modern globalised world, occur between citizens and non-citizens of a particular state, more permissible standards for targeting and retention of communication that involves at least one non-citizen creates the potential for abuse, as a loophole to collect information on citizens who would otherwise be protected under domestic law. Furthermore, such an automatic distinction can be criticised on fundamental grounds: the rights under both the ICCPR and the ECHR apply to everyone within a state's jurisdiction.[37] All individuals thus have privacy rights vis-à-vis states party to these conventions. The applicable US regulation now provides that all individuals have privacy rights.[38] And the aforementioned difficulty in practice of distinguishing between internal and external communications (above section IV) is alleged to

[34] PCLOB, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", 2 July 2014 (hereinafter, PCLOB Section 702 report) p. 135 "The Board's review of the Section 702 program showed that the procedures for documenting targeting decisions within the NSA, and the procedures for reviewing those decisions within the executive branch, focus primarily on the foreignness determination – establishing that a potential target is a non-U.S. person reasonably believed to be located abroad … [these] typically indicate what category of foreign intelligence information they expect to obtain from targeting a particular person in a single brief sentence that contains only minimal information about why the analyst believes that targeting this person will yield foreign intelligence information. As a result, the Section 702 oversight team from the DOJ and the ODNI cannot scrutinize these foreign intelligence purpose determinations with the same rigor that it scrutinizes foreignness determinations." The PCLOB recommended improvements in motivation and documentation (p. 134) and that this be overseen by FISC (p. 136).

[35] De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD, Review Committee on the Intelligence and Security Services) Annual Report 2011-2012, p. 96.

[36] The safeguards in the German legislation (below, paras. 112-114) do not apply to non-citizens/non-residents, a significant defect from the human rights perspective and something which has been criticised by German commentators, see Huber B., "Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite", *Neue Juristische Wochenschrift*, 2013, No. 35, 2572-2576.

[37] See the criticism expressed by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 4th Annual Report, 23 September 2014, A/69/397.

[38] Presidential Policy Directive (PPD) 28 (hereafter, PPD-28), section 4 "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information". It does not change the position of the US government that the ICCPR has no extraterritorial effect.

work to non-citizens' benefit, as it means that, in practice, the higher (citizen) standards are applied in the automated minimisation processes.[39] If this is correct, then it is an important step forward, and one which other concerned states should also take, if they have not already done so.[40] However, this recognition of foreigners' privacy rights still presumably allows different tests of relevance, proportionality and necessity as regards targeting, retention, deletion and communication.[41]In any event, without strong independent oversight of the databanks (below section X), it is not possible to have any confidence that excessive amounts of personal data on foreigners are not being kept (and used in different ways).

73. Allowing the collection of signals intelligence for "the economic well-being of the nation"[42] gives rise to the suspicion that signals intelligence is being used for purposes of economic espionage, to win commercial advantages for companies incorporated in a state's own jurisdiction in public procurement or other areas. The interconnection of private and public interests in defence contracting in some states can strengthen such suspicions. There are however at least three areas of business activity where strategic surveillance is useful (in addition to whatever use it might have in guarding against offensive economic espionage directed against one's own corporations). These three areas are proliferation of weapons of mass destruction (and violation of export control conditions generally), circumvention of UN/EU sanctions and aggravated money laundering. If a wide ground is used, this should be supplemented by clear prohibitions on economic espionage, as the applicable US regulations now do,[43] buttressed by effective oversight and prohibitions on letting government departments or administrative agencies concerned with promoting trade task the signals intelligence agency.

74. A particular issue, bearing in mind the close co-operation which allegedly exists between certain western signals intelligence agencies, is the risk of circumvention of stronger domestic surveillance procedures. States tend to provide that where both participants in a telecommunication are within the state's jurisdiction, then this is an internal communication, even if the communication, or some of it, in some way crosses the national boundary. Automated systems weed out such internal communications, even if there is an error rate (inevitable if one wants to avoid external communications accidentally being deleted). This solves a part of the problem but not all of it. As already noted, there is a possibility that the agency in X-land might ask the agency of Y-land to collect intelligence on an X-land citizen or resident, thus avoiding any legal limits which the X-land agency might be subject to as regards domestic intelligence operations. This particular issue can be partly dealt with by prohibiting, in law, the X-land agency from actively requesting other friendly agencies to collect intelligence on X-land citizens or residents. One can also say that, in this

[39] PCLOB, Section 702 Report, p. 100 "as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies' minimization and/or targeting procedures. While these procedures are legally required only for U.S. persons, the cost and difficulty of identifying and removing U.S. person information from a large body of data means that typically the entire dataset is handled in compliance with the higher U.S. person standards".

[40] See, e.g. Sweden where the relevant act (2008:717) on signals intelligence provides for a minimisation duty regarding selectors (section 5), and destruction requirements in sections 3 and 7. There is no explicit limiting of this to citizens.

[41] See, for example section 7 of the Swedish ordinance (2008:261), where the communication of intelligence to foreign agencies is forbidden where this is contrary to Swedish interests, meaning that it is easier to communicate intelligence concerning non-Swedish citizens/residents.

[42] See, e.g. the UK RIPA section 5(3), although section 5(5) specifies that the information to be obtained must relate "to the acts or intentions of persons outside the British Islands".

[43] PPD-28 section 2 "In no event may signals intelligence collected in bulk be used for the purpose of … affording a competitive advantage to U.S. companies and U.S. business sectors commercially". A footnote specifies that "Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage".

area, institutional rivalry might buttress such a limit: the agency responsible for internal security in X-land will, or should have, exclusive competence to engage in intelligence gathering operations in X-land. One ought to be able to rely to some extent on the fact that this agency will jealously guard this exclusive competence.[44] Having said this, such an institutional rivalry works (if at all) vis-à-vis agencies in the same state. If a very powerful foreign signals intelligence agency offers to provide useful intelligence to the internal security agency in X-land, it is very unlikely to be refused. The internal security agency will be strongly against prohibiting the passive receipt of such intelligence (and the boundary line between active and passive may not be as clear as one might think, when the agencies in question have "shared understandings" developed over many years of co-operation). Moreover, as already mentioned, bulk transfer of data occurs. This makes sense from an effectiveness perspective (best use of spare capacity, translating and other expertise, etc.) but also gives rise to a risk of circumvention of rules on domestic intelligence gathering. A suitable safeguard in both cases is to provide that the bulk material transferred can only be searched if all the material requirements of a national search are fulfilled and this is duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.[45]

75. A "foreign policy" limit which can be mentioned here is an undertaking not to transfer intelligence which would enable a country to repress free speech or democracy activists. The US has extensive intelligence exchange arrangements even with autocratic governments, and such a limit can be found in Presidential Policy Directive (PPD) 28.[46]

76. In conclusion on the mandate, two examples can be given. Under the UK Regulation of Investigative Powers Act 2000, section 5(3), a warrant may be issued (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; (c) for the purpose of safeguarding the economic well-being of the United Kingdom; or (d) for the purpose, in circumstances appearing to the secretary of state to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement. While there are provisions limiting further the ways in which intelligence can be collected, the basic purposes are expressed in very general terms.[47]

77. Under the Swedish Signals Intelligence Act (2008:717), section 1 (rapporteur's translation):

> "Signals intelligence in defence intelligence may only be used in order to identify 1. External military threats to the country, 2. The conditions for Swedish participation in peace support and humanitarian international operations or [a] security threat to Swedish interests in the implementation of such efforts, 3. Strategic matters regarding

[44] For example under the Swedish Defence Intelligence Act, section 4, the signals intelligence agency is not to participate in criminal investigations. This is interpreted as meaning that operations directed by the signals intelligence agency and using selectors associated with a particular individual must cease when and if a criminal investigation is opened against him or her, as surveillance measures governed (and limited) by the Code of Judicial Procedure apply (Prop. 2006/07:63, p. 108).

[45] See below section VI regarding the British case of *Liberty (The National Council For Civil Liberties) v. GCHQ, SIS, the Security Service*, UK Investigative Powers Tribunal [2014] UKIPTrib 13_77-H, judgment and order, [2015] UKIPTrib 13_77-H.

[46] Section 2 "In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion.".

[47] Cf. PPD-28 and the relevant section of the Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 USC paras. 1801 to 1885c), namely 50 USC para. 1881a(a), (below note 114) together provide a much tighter set of permissible grounds.

international terrorism and other serious transnational crime that could threaten essential national interests, 4. The development and proliferation of weapons, military equipment and products referred to in the Act (2000:1064) on the control of dual-use products and of technical assistance, 5. Serious external threats to public infrastructure, 6. Conflicts abroad with implications for international security, 7. Foreign intelligence operations against Swedish interests, or 8. Foreign power's actions or intentions of significant importance to Swedish foreign, security and defence policy."

78. The same section contains a further legal ground, in recognition of the fact that the signals intelligence agency engages in continuous testing and that this, too, impacts upon human rights, namely "If it is necessary for defence intelligence signals may be electronically obtained by signals interception also to 1. follow changes in the signals context of the outside world, technological developments and signal protection, and 2. continuously develop the technology and methodology needed to conduct activities under this Act". Testing is also subject to judicial authorisation (below, paragraph 120).[48]

79. The Venice Commission has previously expressed the view that it is "absolutely essential" that main norms concerning the internal security services be as clear as possible so that the tasks they can lawfully engage in are clearly defined and that more specific regulations should only be allowed to be kept secret to the extent that it is absolutely necessary.[49] The same applies to signals intelligence.

D. Governmental control and tasking

80. As already mentioned, signals intelligence can be used to obtain diplomatic intelligence, economic intelligence, military intelligence and domestic-related intelligence. As regards the first category, the tasker is likely to be the government itself. The same applies to the second category, although here administrative agencies such as the customs authority can also be assumed to be a tasker. The armed forces, defence intelligence, etc. are the taskers of the third category. As regards the fourth category, the important factor is the link, if any, which is made to investigation of security crime.

81. A number of different variations can be discerned. National law can allow an internal security or police body to "task" the signals intelligence agency, either for only "strategic" intelligence (such as in Sweden) or for this purpose as well as for the purpose of an intelligence gathering operation aimed at individuals or groups relating to specific security offences (such as in the US). An alternative system is that there is no right to task, but a possibility for, or a duty on, the signals intelligence agency to transfer intelligence indicating that a security/organised crime offence has been committed to the police/internal security agency relevant for investigating such offences.

82. In all cases, oversight is required, but the different types of function require different types of oversight.

83. For all the taskers, it is important to remember that, as they are consumers of the intelligence they request, they should not be seen as external controls over the intelligence gathering process (2007 report, paragraph 112).

[48] Intelligence obtained as a result of testing may be retained, in order to assist in designing future operations, but may not be communicated to the tasker or any other body, Prop 2006/07:63, p. 109.

[49] See Venice Commission, CDL-INF(98)6, p. 7 and 2007 report, paras. 25 and 227.

E. Network accountability

84. Due to their geographical location, different states have access to different cable and satellite-borne telecommunications, which means that data are frequently collected which are of interest to other states. Moreover, the nature of the Internet, with communications being broken down into "packets", sent on different routes, and then "reassembled" means that different states can obtain access to different parts of the same message. Thus, while many states co-operate with each other by exchanging domestic and foreign intelligence with one another (and such arrangements can also be part of a treaty obligation), the links between allied states as regards signals intelligence can be even stronger. Some states have standing co-operative arrangements and tight organisational links between their signals intelligence agencies. The "third party" or "originator" rule (by which any use of intelligence transferred from one agency to another is subject to the permission of the former) can thus be an even more serious obstacle to oversight.

VI. Accountability for security activities and the case law of the European Court of Human Rights

A. The European Convention on Human Rights and strategic surveillance generally

85. To begin with, it should be recollected that the European Convention on Human Rights consists of minimum standards. Thus, the Court's case law is only a point of departure for European states. Obviously, the standards developed by the Court cannot apply to the US, or other states not party to the Convention.

86. In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; definition of the categories of people liable to have their telephones tapped and a limit on the duration of telephone tapping; 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 the tapes destroyed.[50] It should be stressed that several of these standards have to be adapted to apply to strategic surveillance (dealt with in the next subsection).

87. The Court has so far only looked at two cases relating to strategic surveillance, *Weber and Saravia v. Germany* and *Liberty and Others v. UK.*[51] The latter case concerned only the issue of "accordance with the law". The former case was an admissibility decision, albeit an unusually detailed and well-reasoned decision. But the issues of "necessity in a democratic society"/proportionality and remedies have not yet been extensively discussed by the Court. Nor can it be said that the standards set out in Weber and Saravia judgment, which concern the German model, are necessarily wholly applicable to national legislation which is constructed in a different way.[52] Having said that the Strasbourg Court's case law is limited, this is not the same thing as saying that the Convention case law is limited: the Dutch

[50] See e.g. *Weber and Saravia v. Germany*, op. cit., para. 95.

[51] *Liberty and Others v. UK*, Application No. 58243/00, 1 July 2008.

[52] For example, an oversight safeguard noted by the Court was marking of intelligence obtained as a result of signals intelligence operations, as otherwise the task of the oversight body is made more difficult, as this intelligence is merged with other intelligence obtained by the BND. This safeguard is not necessary where the database only consists of signals intelligence, provided that only the signals intelligence agency has access to the database.

oversight body, the CTIVD, and the UK IPT have discussed the application of the Convention standards to their respective national laws, and these will also be treated here.

88. The first issue to note is that "national security" is not limited to investigation of security offences which have been committed in the past, are ongoing or will be committed in the future.[53] The wording of Article 8 expressly allows interferences in private life in the interests of national security, for the economic well-being of the country, public safety or for the prevention of disorder or crime. The gathering of foreign intelligence, not connected, or immediately connected, to criminal offences can fall partly within several of the above grounds. As noted above, the fact that a treaty, the ECHR, by necessity sets out very general grounds does not mean that the national legislator should not attempt to obtain a higher degree of precision and legal certainty (see above section V(C)).

89. Secondly, as regards the extent of interference with personal integrity, there is no distinction between interception of cable or radio-borne communications.[54]

90. Thirdly, as regards which Convention rights strategic surveillance interferes with, the main articles at issue are articles 8 and 13. However, in Weber and Saravia the Court considered that the first applicant, a journalist, could claim that her rights under Article 10 were also affected.[55] That the freedoms of expression and information are at issue is also buttressed by other authorities. The Court has on occasion referred to the chilling effect on freedom of expression which a sanction or disclosure order can have on journalists.[56] And, as noted above, it has also stressed in the security context that there is a right to seek information.[57] The CJEU has also noted the possible chilling effect on freedom of expression and information which blanket retention of metadata can have,[58] as have UN and IACHR special rapporteurs.[59]

91. Fourthly, the European Court of Human Rights has clarified that strategic surveillance involves multiple interferences with personal integrity. The first interference is when there is an authorisation to intercept telecommunications, that is when the law specifies that telecommunications companies must allow access in some way to the signals intelligence agency to all, or given categories of these communications, or the signals intelligence agency is given a legal power to acquire all or given categories of these communications. As explained above in section IV, for strategic surveillance of content, the material actually examined is obtained by searching the bulk material acquired by means of computer algorithms (selectors). Thus, the implication of the Court's approach is that there must be

---

[53] *Weber and Saravia v. Germany*, para. 104.

[54] This follows from the fact that the Court made no mention of any such distinction in either *Liberty and Others v. UK*, or *Weber and Saravia v. Germany*.

[55] *Weber and Saravia v. Germany*, para. 145 "there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone … the transmission of data to other authorities, their destruction and the failure to notify the first applicant of surveillance measures could serve further to impair the confidentiality and protection of information given to her by her sources." One might argue by reference to ECHR Article 16 that foreign journalists need not have exactly the same Article 10 rights as citizens, however, the Court has clarified that this article should be interpreted restrictively (*Piermont v. France*, 27 April 1995, A/314).

[56] See, for example *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, Application No. 39315/06), 22 November 2012.

[57] *Youth Initiative for Human Rights v. Serbia*, above.

[58] CJEU, *Digital Rights Ireland Ltd* judgment of 8 April 2014,para. 28.

[59] Joint Statement of the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

legal authority for issuing selectors as regards the content of the data, and, as regards metadata, for issuing instructions for contact chaining and otherwise analysing this data.

92. The second interference is after the bulk data has been processed and analysed, at the point that it is transmitted to, and used by authorities other than the signals intelligence agency. Thirdly and finally, the Court considers that an interference with private life occurs in so far as the rules provide for the destruction of the data obtained and for the refusal to notify the persons concerned of surveillance measures taken.[60] This means that a specific statutory authority – accessible and otherwise fulfilling the Court's case law on quality of law – must exist for each of these interferences.

93. Fifthly, the Court has stressed the need for statute law to govern the main elements of secret surveillance. Case law, even where it lays down detailed standards and comes from the Supreme, or Constitutional Court, is in itself not sufficient to regulate the area[61] and nor is subordinate legislation. The purpose of defining powers with precision is to reduce the scope for misuse of, or overuse of, power. Where a power is framed in broad terms in a statute, and oversight is limited to checking if an agency remains within its statutory mandate, then the oversight is of limited use.[62] Moreover, other things being equal, the more the power in question interferes with privacy, the greater the potential damage to privacy if the power is misused or overused. Precision focuses the minds of everyone involved in the investigation and authorisation process on their responsibilities, which are ultimately backed up by the criminal offence of misuse of office. However, the main issue here is what parts of the system can be subject to internal, that is secret, regulation (see also below, paragraph 107). This involves looking behind the idea of statutory law to identify its underlying values. These could be said to be three; foreseeability/stability, democratic legitimacy and institutional competence. A statutory regulation is more stable and more transparent than regulation by means of subordinate legislation. As regards the second of these, little need be said: suffice it to say that it is for the representatives of the people to draw balances between competing interests in an area as important as this. The third value relates to the time and expertise which the parliament has at its disposal to devise appropriate general rules, and the completeness of the debate (taking into account all the relevant factors) which accompanies, or should accompany, discussion of legislative proposals. In any event, the Strasbourg Court dismissed the UK government's arguments in the Liberty case that the accessibility requirements should be lower.[63] The Court stated that it "does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other."

[60] Op. cit., para. 79. In *Liberty and Others*, the Court contented itself with stating that it "considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied" (para. 57).

[61] See *Heglas v. Czech Republic*, Application No. 5935/02, 1 March 2007, para. 74.

[62] For example, the narrowness of the review performed by the IPT (see below para. 95) can be criticised. See, e.g. Justice, *Freedom from suspicion: surveillance reform for a digital age* (2011) p. 133-153, Leigh, I., "A view from across the Channel: intelligence oversight in the United Kingdom", in van Laethem, W. and Vanderborght, J. (eds), *Regards sur le control*, Intersentia, 2013.

[63] The Court's emphasis of the accessibility requirements in this case are probably due to the wide, indeed "virtually unfettered" (para. 64) discretion the British legislation gave to the authorising body.

94. The Court went on to list the issues which should be accessible in statute law, referring to its earlier decision in Weber and Saravia:

> "In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order … Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in [the amended G10 Act] … The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications".[64]

95. Sixthly, although the Court does not appear to have considered this issue directly, it is a logical consequence of its findings on accessibility that separate precise legal authority must exist for other methods signals intelligence agencies might possess of obtaining data. One of these methods is by obtaining bulk raw data from friendly signals intelligence agencies. This was the main issue before the UK IPT in a judgment in a case brought by a number of NGOs against the British signals intelligence agency, GCHQ. GCHQ and the British Government assured the IPT that this transferred material could only be searched if permission was given in the same way as for a search made of raw data gathered by GCHQ itself. However, before this disclosure was made, this had not been clear. This was the reason for the IPT finding that, during the period before these disclosures were made, GCHQ's searching of this transferred material had not been "in accordance with the law".

96. As noted above in section IV, a signals intelligence agency, through agreement with ISPs, or even without this agreement, might be able to access stored data, e.g. in the "cloud". Here it should be stressed that even if the ISP gives its consent, for states bound by European principles of data protection, it is not possible to argue that such access does not involve an interference with privacy and/or the freedom of correspondence.[65] For such personal data, the interference thus occurs even if the legal "owner" or controller of the data gives its consent. Thus, it follows that statutory authority must also exist for such a power of access without consent. The same can be said for the even more controversial power of remotely hacking into computers, and planting malware. This is equivalent to a search and seizure, with the difference that it is covert and continuous throughout the period of operation of the malware, rather than open and on one occasion only. Following the Strasbourg Court's case law on search and seizure, if this is to be allowed at all, it can only be with a very limited list of offences, with clear statutory authority, judicial authorisation,[66] minimisation and destruction requirements and, bearing in mind its covert nature, strict oversight.[67]

---

[64] Op. cit., para. 68.

[65] See, e.g. the judgment of the German Federal Constitutional Court (2 BvR 902/06) to the effect that e-mails on a server are protected by the constitutional right of communication.

[66] See, e.g. the Belgian law providing for a quasi-judicial review commission to give *ex ante* "binding advice" to the security agencies when they use this, and other "exceptional measures" (Law on Intelligence and Security Services 1998, articles 18(2) (3) as amended by the law of 14 February 2010).

[67] See, e.g. *Wieser and Bicos Beteiligungen GmbH v. Austria,* Application No. 74336/01, 16 October 2007 (regarding the physical seizure of computers in a lawyer's office – found disproportionate). See also the judgment of the German Federal Constitutional Court in 1 BvR 595/07 which found that, in view of the gravity of the

B. Adapting ECHR standards to strategic surveillance

97. To turn now to the question of how to adapt the safeguards devised by the European Court of Human Rights for ordinary surveillance to strategic surveillance,[68] the first such safeguard relates to the nature of the offences which may give rise to an interception order. This primarily applies to states which provide for the use of signals intelligence to investigate security offences, and certain other offences, such as aggravated money laundering. For such states, it is necessary to enumerate these offences, and provide for destruction of data which might incidentally be gathered on other offences. The exception to this – allowing transfer to law enforcement – must be narrowly defined and subject to oversight, as otherwise the risk is that the exception becomes the rule, and the safeguard loses its value.[69] This safeguard is relevant as regards both contact chaining of metadata and searches of content.

98. Another safeguard is a definition of the categories of people liable to have their communications intercepted. By this is meant, the extent of the connection the people in question have to the offence (or the conduct damaging to national security). Obviously this includes people suspected of (specified) offences, but the law can also specify that people in contact with such people can, under certain circumstances, be subjected to telecommunications interception. As regards contact chaining of metadata, normally only people suspected of actual involvement in particularly seriously offences, such as terrorism should be used as the basis for contact chaining. Where such a person (A) is in contact with other people (B, C, D) it is only where there are separate grounds for suspecting B, C, D of involvement in terrorism that it should be possible to go on to check B, and C and D's own networks of contacts.[70] By contrast, if the power to contact chain is framed in terms of simple "relevance" for the investigation of terrorism, even if some evidential standard (e.g. "reasonable articulable suspicion") is required, this has the potential to expand greatly the potential net of surveillance. For example, if the initial suspect has 100 contacts, and each of these contacts in turn has 100 contacts, then it is easy to see how the net of surveillance can grow exponentially, and cover huge numbers of people without any connection whatsoever to terrorism. It is difficult to see how such an expansive approach to contact chaining can be

---

encroachment, the secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is only permissible constitutionally if factual indications exist of a concrete danger to a predominantly important legal interest. These "predominantly important interests" are the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence. Adequate procedural safeguards, judicial authorisation, minimisation and destruction requirements, were also found to be necessary.

[68] One can mention here a safeguard not relevant for targeted surveillance, namely a quantitative restriction. For example, the German G 10 Act section 10(4) provides that the order to acquire bulk content "shall specify what proportion of the transmission capacity available on these transmission paths may be monitored. In [strategic surveillance], this proportion may not exceed 20%." The actual proportions taken are in practice considerably less. However, even – say – 8% of the traffic is considerable. The Swedish act does not provide for a maximum proportion of the traffic, but states that the signal bearers must be specified and the acquiring of bulk data is not permissible if the underlying purpose can be achieved in a less restrictive way and unless it is adjudged that the value of the information which is expected to be produced by the acquiring of the data is clearly greater than the restriction in privacy which the acquiring can entail (section 5). This is a condition applied by the judicial authorising body and monitored by the external oversight body (below paras. 120-122); such limits must obviously be subject to external oversight if they are to have any meaning.

[69] For example, when it assessed the constitutionality of the amendments to the German law on strategic surveillance, the Bundesverfassungsgericht (BVerfG) added an additional safeguard here, specifying that the more minor the offence is, the more concrete the indications must be that a given person has committed it, before transfer of information is allowed, BVerfG, 1 BvR 2226/94, 2420/95 and 2437/95, 14 July 1999. The G 10 Act, section 7, provides exhaustive lists of authorities to which transfers of signals intelligence may occur, and for what purposes. Section 7a provides for conditions on transfer of signals intelligence to foreign agencies.

[70] For the US practice, see below para. 116.

proportionate (or, indeed, a sensible use of the resources of the signals intelligence agency).[71]

99. One method of trying to limit an overly-expansive approach to contact chaining is to place strict limits on the power to query collected bulk metadata.[72] Another is to create an internal privacy advocate, as an institutional mechanism for protecting the interests of people who may have nothing to do with the offence being investigated. The advocate can raise arguments on their behalf, and try to ensure that the search parameters at the time of targeting are limited as much as possible.[73]

100. As regards searches of content data, privacy issues are particularly raised when a decision is being considered to use a selector which is attributable to a natural person (such as his or her name, nickname, e-mail address, physical address, etc). Strengthened justification requirements and procedural safeguards should apply in such a situation, such as the involvement of a privacy advocate. Safeguards are also necessary as regards subsequent decisions to transfer intelligence on individuals obtained by strategic surveillance to internal security agencies, to law-enforcement or to foreign services.[74]

101. There are two categories of people who the European Court of Human Rights has considered as deserving of special protection: on the one hand, lawyers and others who are entitled to "privileged communications", such as priests, and on the other, journalists. A safeguard which is used in ordinary surveillance is to require erasure of "privileged communications". This means that such people should not normally be targeted either by means of metadata contact chaining or by using selectors. Moreover it means that if their communications have been swept up indirectly, they should be destroyed and that this should be overseen by either an internal legally qualified "gatekeeper" and/or an external oversight body. The Court's case law, *inter alia*, *Klass v. Germany*, *Kopp v. Switzerland* and a letter interception case, *Erdem v. Germany*,[75] indicate that the Convention does not require states to abstain totally from engaging in surveillance of "privileged communications". But unless there is evidence of involvement of the lawyer, priest, etc. in crime or conduct damaging to national security, interception of privileged communications by means of signals intelligence should not be lawful.[76]

[71] PCLOB's conclusion was that the NSA's section 215 programme did not meet the test of efficacy and recommended its termination. PCLOB, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court", 23 January 2014.

[72] Here one should note that, under the (annulled) EU data retention directive, metadata could be retained for a period of up to two years, and could be searched to investigate any "serious crime". The vagueness of the term "serious crime" was one of the reasons for the CJEU annulling the directive.

[73] There is empirical evidence that such privacy advocates in law-enforcement and internal security surveillance can have some significance in helping ensure that the parameters of investigations really are drawn as narrowly as possible. See the Swedish official inquiry into secret surveillance, SOU 2012:44. Privacy advocates (nominated by the Bar Council and appointed by the government) represent the interests of targeted persons and organisations in the authorisation process before the Swedish Defence Intelligence Court (below para. 132).

[74] For example, the BVerfG found that the arrangements for retention and use of information by the intelligence service (section 3(4)) and transfer of information to the government (section 3(3)) were insufficiently specified in the original German law.

[75] Application No. 38321/97, 5 July 2001.

[76] For example, both the German G 10 Act (section 3b) and the Swedish Signals Intelligence Act (section 7) provide for destruction of privileged communications.

102. Journalists are another group which requires special protection. Here the issue of whistle-blowing is relevant. Contact-chaining journalists will produce lists of their sources. For a civil servant, even the risk of discovery is likely to act as a powerful disincentive to giving information to a journalist. Having said this, there can be no absolute prohibition of contact-chaining journalists where there are very strong reasons for doing so (most likely the leaking of top secret information). There is, moreover, the difficulty of determining the boundaries of the profession of journalists. Unlike lawyers and priests, this profession is not so easily identified; NGOs engaged in building public opinion and even bloggers might claim on good grounds to be entitled to equivalent protections.

103. One solution is to provide for a similar level of protection to that for lawyers and other privileged communicants. Another is to have a high, or very high, threshold before approving signals intelligence operations against journalists, combined with procedural safeguards and strong external oversight. Indirect collection of information on journalists is, relatively speaking, more likely, bearing in mind the way they work, and destruction requirements, properly overseen, should also apply here.

104. The safeguard of setting out time limits is not as meaningful for strategic surveillance as it is for ordinary surveillance. Ordinary surveillance is expensive in terms of man hours spent listening to tapes, and possibly translating these. From the perspective of effectiveness, law-enforcement and internal security surveillance should also be kept short. This is not so true for strategic surveillance. Periods of surveillance tend to be long, and continually renewed. Retention periods also tend to be long: data originally thought to be irrelevant may, as a result of new data, come to be seen as relevant.[77] One can, however, as is the case in the German law (above) provide for a requirement to make periodic internal reviews of the (continued) need to retain the data. To be meaningful, such a duty must be backed up by external oversight.

105. It is apparent that the two most significant safeguards are the authorisation process (of collection and of access to the collected data) and the follow-up (oversight) process. That the latter must be performed by an independent, external body is apparent from the Court's case law. The question which arises here is whether even the authorisation process should be independent.

106. As noted above, in section V(D), some states, e.g. the United Kingdom or the Netherlands have as the authorising body, a government minister who is – obviously – not independent from the executive. In *Popescu v. Romania*,[78] the Court considered that the Romanian authority which ordered the surveillance (the prosecutor) was not independent from the executive. It stated that the authorising body must be independent and that there should either be judicial control or independent control over the issuing body's activity. Similarly, in the Iordachi and Association for European Integration and Human Rights and Ekimdzhiev cases the Court stressed that independent controls should exist at both the authorisation stage and the follow-up stage. The Court has a preference for judicial authorisation, even if, in *Kennedy v. the United Kingdom*,[79] it accepted the British system of ministerial authorisation. It may be that the court demands higher standards where there is evidence that the law is not being followed in practice. Whatever the case, if a holistic approach is taken, assessing the system as a whole, then it seems clear that where a system lacks independent controls at the authorisation stage, this should mean that very

[77] This was the main reason why the US National Research Council report considered it could be problematic to impose more limits on collection. Tighter limits on subsequent access to the collected bulk data go some way to minimising the risk of abuse (op. cit. at p. 51).

[78] Application No. 71525/01, 26 April 2007.

[79] Application No. 26839/05, 18 May 2010.

strong safeguards must exist at the follow-up/oversight stage, for example, the power to take binding decisions.[80] And, naturally, higher constitutional standards can apply, requiring both independent authorisation and oversight.

VII. Internal and governmental controls as part of overall accountability systems

107. As noted by the 2007 report, internal controls are the primary safeguard for a rights-respecting agency which does not abuse power. Recruitment and training are key issues.[81] Internal rules specify in more detail what vaguer statutory norms actually entail and thus are particularly important in the area of signals intelligence. These are of necessity secret. Thus, it is important to require the agency to build in respect for privacy and other human rights when promulgating internal rules.[82] For the reasons set out in section IV, it has been particularly tempting to rely primarily on internal controls in the area of strategic surveillance. The Dutch and British systems for ministerial authorisation, bearing in mind the major restraints on government ministers' time, and their many other responsibilities, mean that in practice, the minister will be almost wholly dependent on his or her civil servants. However, for reasons set out in the 2007 report, internal controls are insufficient. As already noted, the logical consequence, where there is no independent preventive authorisation mechanism, is that the post-hoc oversight mechanisms must be particularly strong. That it is a mistake to rely primarily on internal controls was also the conclusion of the US Presidential Review Board: external oversight over the US NSA must be considerably strengthened.[83]

VIII. Parliamentary accountability

108. There are a number of reasons why parliamentary supervision of strategic surveillance is problematic. First, the technical sophistication of signals intelligence makes it difficult for parliamentarians to supervise without the aid of technical experts. Second, the general problem of parliamentarians finding sufficient time for oversight along with all their other duties is particularly acute as regards strategic surveillance. If one wishes to control the dynamic process of refining the selectors (as opposed to a post-hoc scrutiny), then a standing body is necessary. Thirdly, the high degree of network co-operation between certain signals intelligence agencies means an added reluctance to accept parliamentary oversight, which can thus affect not simply one's own agencies, but also those of one's allies. As previously noted, in some states the doctrine of parliamentary privilege means that parliamentary committees cannot be security-screened, adding to an already-existing fear of leaks. The other, crucial, factor is that strategic surveillance involves an interference with individual rights. Supervision of such measures has traditionally been a matter for the judiciary. The constitutional principle of separation of powers can make it problematic for a parliamentary body to play such a quasi-judicial role.

---

[80] See, for example the powers of the German G 10 Commission (G 10-Kommission) (para. 112) or the Swedish SIUN (para. 121).

[81] The Swedish external oversight body SIUN (below para. 121) is expressly required by statute to monitor issues of recruitment and training. Several of PCLOB's recommendations in the Section 702 report relate to improved privacy "sensitivity" training.

[82] Here one should note that institutionalising respect for human rights comes in both when the internal rules are being devised, and, because of the importance of automated minimisation systems, at the point these rules are "translated" into software.

[83] The Board stated: "Americans must not make the mistake of trusting officials", "Liberty and Security in a Changing World", op. cit. p. 114. External oversight can strengthen the internal culture of the agency in a number of ways. For example, the Swedish Signals Intelligence Agency has an "integrity council" consisting of three judges who have an advisory role when the agency is devising internal rules.

109. To explain this last point in a bit more detail: as the previous sections have shown, balancing of privacy and other human rights concerns against other interests comes in at several points in the process, but two crucial points are when a decision is made to use particular selectors, and when human analysts decide whether or not to keep the information in question. The first type of decision resembles, at least in some ways, a decision to authorise targeted surveillance. As such, it can be taken by a judicial body. As the decision involves considerable policy elements, knowledge of intelligence techniques and foreign policy are also desirable. Finding a group of people who combine all three types of competence is not easy, even for a large state. Thus, it is easier to create a hybrid body of judges and other experts.

110. The second type of decision is of a "data protection" character, which can be overseen afterwards by an expert administrative body. Such a body must be independent and have appropriate powers.[84] Neither of these types of decision is "political" in nature. On the other hand, what is more political is the prior decision taken – that somebody, or something, is of sufficient importance to national security to need intelligence about. This is the type of decision which would benefit from a (closed) discussion in a political body, where different spectrums of opinion are represented. Another type of policy-oriented issue is deciding on the general rules regarding how and under what circumstances signals intelligence can be collected[85] or be exchanged with other signals intelligence organisations[86] A third such issue is making a general evaluation of the overall effectiveness and efficacy of signals intelligence measures. A fourth role for a political body is to engage in a continuous dialogue with whatever expert oversight body is established.

111. Two parliamentary models can be mentioned here. As with all oversight, it should be remembered that while the oversight body must have sufficient powers on paper, it is how it exercises these powers in practice which is important. In the US, the senate and house committees on intelligence receive regular classified briefings from intelligence officials, including on the functioning of the NSA's strategic surveillance. However, criticism has been expressed of the oversight performed by the intelligence committees in the area of strategic surveillance, both from members of other congressional committees and from academic commentators.[87] It is certainly the case that the size of the US intelligence community, and the breadth and depth of the issues to be looked at, mean that the congressional committees might feel obliged to focus their attention on a particular issue – as the senate committee has done as regards the CIA rendition programme. And penetrating the particularly arcane world of signals intelligence means identifying the right questions to ask, and considerable persistence in continuing to ask them. The members of the senate committee can bring in their own (security-cleared) staff, but this is not the case for the house committee. In particular instances, due to the classified nature of material being discussed, congressional oversight has been hampered by fragmentation,[88] by limitations such as a prohibition on

[84] See below paras. 124 and 132. As regards the independence of data protection bodies see EU directive 95/46/EC on data protection and 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, CETS No. 181. It is also possible for an expert administrative body to exercise remedies functions, see below paras. 137-138.

[85] See for example the hearings held before the British ISC, which gave NGOs an opportunity to give their views on this issue, http://isc.independent.gov.uk/public-evidence.

[86] In any event, these general arrangements should be subject to some form of external authorisation, or at least, oversight. See, for example European Parliament, op. cit. p. 218.

[87] See e.g. Zegart, A. B., "The Domestic Politics of Irrational Intelligence Oversight", 126 *Political Science Quarterly* (2011) pp. 1–27, *Wall St Journal*, 29 July 2014, *The Washington Post*, 19 August 2013 and Colaresi, M. P., *Democracy Declassified: The Secrecy Dilemma in National Security*, OUP 2014.

[88] The Department of Homeland Security reports to 92 committees and sub-committees of congress, see Bipartisan Policy Organisation, "Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report", 2014, p. 21.

removing any briefing materials or notes from specially designated areas of the Capitol building, or limitations that prevent members of congress from bringing their legal counsel to briefings.[89] Congress exerts power over the intelligence community primarily through the threat, or promise, of legislation and through budget appropriations (although neither the senate nor the house intelligence committees have power over appropriations). Political agreement is necessary to make either of these methods work properly. One can also speculate as to the perceived political price that a legislator pays in the eyes of the public if he or she publicly advocates for greater oversight in the cases of SIGINT. Because the perceived harm to any individual is low, there is no sense of an individualised harm that motivates voters to pressure officials (and if anyone is harmed, it is probably a foreigner). By contrast there is considerable public fear that greater oversight will foreclose prevention of the next big terrorist attack, for which elected officials will be held accountable. In any event, it is revealing that the main official criticism of the NSA programme has so far been expressed by the executive-appointed expert body, the PCLOB (although its members are confirmed by the senate), not the senate or house committees on intelligence.

112. The German model is both a control and an oversight mechanism. As far as concerns control, the telecommunication links to be subject to surveillance in a particular area of risk are defined by the German Federal Ministry of the Interior. The Parlamentarisches Kontrollgremium (PKGr), the Parliamentary Control Panel, has to approve these. Thus, it exercises a degree of control over the "tasking" and the decision on what signal bearers to intercept and to what extent. The second stage is the approval of the selectors. These are decided by the interior ministry, on the proposal of the BND, but subject to the approval of the expert body, the G 10 Commission. This consists of four ordinary, and four substitute members. They are elected by the PKGr at the start of each parliamentary term and may, but need not, be members of the Bundestag. The chair of the G 10 Commission must be qualified to hold judicial office. Thus, the G 10 is a hybrid body, given political legitimacy through being elected by the PKGr.

113. For strategic surveillance, the G 10 verifies the legality of the selectors (including the issue of proportionality). As regards oversight of the data, the G 10 Commission monitors in particular the BND's minimisation of the data. The G 10 Commission must be notified in all cases where there is a question as to whether data within the "core area" of privacy has been collected and retained, and in some cases it decides whether the data should be erased or retained. The G 10 Commission makes occasional inspections of the databanks, *inter alia* to check if data are being erased as required. It also monitors and must be informed of transfers of intelligence which are made to friendly foreign agencies.[90]

114. As regards more general oversight, the government has a special legal duty to provide the PKGr with half-yearly statistics regarding the use of the G 10 Act, and over the forwarding of personal data deriving from strategic surveillance to foreign public authorities, such as the intelligence services of friendly states, and to supranational and intergovernmental agencies. The PKGr has *proprio motu* investigative powers and resources. Thus, broadly speaking, the PKGr deals with the policy-type of issues, whereas the G 10 Commission deals with the quasi-judicial control of selectors and the administrative control of the databanks.

[89] See generally, www.washingtonpost.com/politics/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html.

[90] It should be noted that questions have been raised by German commentators concerning the staff/technical expertise available to the G 10 Commission, and the time it in fact devotes to the approval process at its monthly meetings. See, e.g. the commentary by Roggan, F., *G-10-Gesetz*, Nomos, 2012.

IX. Judicial review and authorisation

115. The extent to which judicial authorisation/oversight can work for strategic surveillance can be discussed.[91]

116. The United States has a system of judicial authorisation, the Foreign Intelligence Surveillance Court (FISC). While the FISC has authorised, on an individual basis, targeted surveillance within the US since 1978, it has had a more limited, supervisory, role to play in strategic surveillance. Under section 215 Foreign Intelligence Surveillance Act, the government must apply for a warrant before a judge of the 15-member FISC.[92] The FISC approves both the "primary order" authorising the overall programme and "secondary orders", which require individual phone companies to provide information to the NSA. Every order is subject to renewal every 90 days. The FISC process for considering applications may include a hearing, and FISC judges have the authority to take testimony from government employees familiar with the technical details of an application. If issued, a warrant requires a telecommunications provider to furnish information to the NSA on a periodic basis. Telephony metadata from different providers is aggregated and stored on NSA networks with FISC-ordered restrictions on when and how the metadata-base can be accessed. To access the stored metadata, the data must be "queried" by entering a telephone number or other identifier associated with a foreign terrorist organisation. Before querying can occur, a high-ranking NSA official or a specially authorised official must determine there is a "reasonable articulable suspicion" that the identifier is associated with a foreign terrorist organisation that is the subject of an FBI investigation. A query will reveal metadata about telephones in direct contact with the "seed," known as the first "hop." It can also include subsequent "hops," or numbers indirectly connected to the seed. Initially, neither FISC nor the NSA limited the number of hops that could be used to connect other numbers to the seed. In March 2009, the government implemented software changes to limit the number of permitted hops to three.[93] In January 2014, President Obama further limited the number of hops to two.[94] Once information from the two hops is sifted, it may be provided to other intelligence agencies. In 2015, it was announced that the "reasonable articulable suspicion" determinations, previously overseen internally, by the US Department of Justice, would now (except in emergency situations) also have to be individually approved by FISC.[95]

---

[91] Judicial safeguards can also come in at stages other than authorisation/oversight, e.g. when signals intelligence is used in subsequent administrative, civil or criminal proceedings – even if this is only likely to arise rarely. In the US, an "aggrieved person" — a term that includes non-US persons — is required to be notified prior to the disclosure or use of any section 702-related information in any federal or state court. The aggrieved person may then move to suppress the evidence on the grounds that it was unlawfully acquired and/or was not in conformity with the authorising section 702 certification (50 USC para. 1806(e)). Determinations regarding whether the section 702 acquisition was lawful and authorised are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived, 50 USC para. 1806(f) and (g). See PCLOB Section 702 Report, p. 100.

[92] FISC judges are appointed by the president from among the federal judiciary and serve seven-year terms.

[93] Memorandum of the United States in Response to the Court's Order Dated January 28, 2009, p. 20, "In re Prod. of Tangible Things From [REDACTED]", No. BR 08-13 (FISA Court, 17 February 2009).

[94] "Transcript of President Obama's Jan. 17 speech on NSA reforms", 17 January 2014, www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html ("Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization, instead of the current three").

[95] For details, see http://icontherecord.tumblr.com/ppd-28/2015/overview.

117. As regards the bulk acquisition of content data under section 702, the US Attorney General and Director of National Intelligence make annual certifications authorising this targeting to acquire foreign intelligence information, without specifying to FISC the particular non-US persons who will be targeted. There is no requirement that the government 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 must meet the statutory definition of foreign intelligence information.[96] Section 702 requires the government to develop targeting and "minimisation" procedures that must satisfy certain criteria. As part of the FISC review and approval of the government's annual certifications, the court must approve these procedures and determine that they meet the necessary standards. The targeting and minimisation procedures must be provided to the congressional intelligence committees, as well as the committees on the judiciary of the senate and the House of Representatives.[97]

118. FISC thus annually authorises and sets conditions on the section 702 programme as a whole, in particular specifying general limits on the selectors which can be used, the data which must be deleted and the types of queries which may be made of the bulk data collected. It does not authorise the use of selectors in individual cases.[98] A problem has been the lack of external follow-up that FISC's conditions are being complied with (as pointed out above, the process of refining selectors is dynamic and highly technical) and that high standards of data protection are in fact operational.[99] PCLOB has therefore recommended that the government submit, together with its annual applications, a random sample of tasking sheets and a random sample of the NSA's and CIA's US person query terms, with supporting documentation. The sample size and methodology should be approved by the FISC. This would give FISC a better basis to assess how its conditions are working in practice.[100]

119. Moreover, it should be noted that a large portion of US SIGINT collection falls outside of the ambit of the FISC. Surveillance of foreign nationals under Executive Order 12333 is not subject to domestic regulation under FISA. Due to general lack of transparency around the programme, there has been no public acknowledgement of how much data are collected

[96] The definition of foreign intelligence information purposes is limited to protecting against actual or potential attacks; protecting against international terrorism, and proliferation of weapons of mass destruction; conducting counter-intelligence; and collecting information with respect to a foreign power or foreign territory that concerns US national defence or foreign affairs, see 50 USC para. 1881a(a).

[97] See the description set out in PCLOB, Section 702 Report, p. 6. See also Donohue, L. K., "Section 702 and the Collection of International Telephone and Internet Content", (2014), available at http://scholarship.law.georgetown.edu/facpub/1355/, p. 30.

[98] For European states, *ex ante* judicial approval in individual cases is to be preferred (see above, section VI). As shown below, the Swedish court approves selectors in individual cases. However, US intelligence needs are very large, and the number of selectors is also likely to be very large and constantly changing. One should bear in mind that judicial approval is not a panacea (2007 report, paras. 205-216). If a court is given large numbers of selectors to approve, and little time in which to work, then the obvious risk is that its review will be superficial.

[99] *The Washington Post*, 16 August 2013.

[100] PCLOB, Section 702 Report, p. 141. There is now a further layer of external oversight in the US system in that PCLOB is an independent agency within the executive branch, established by statute (see Pub. L. No. 110-53, para. 801(a), 121 Stat. 266, 352-58 (2007). The act requires that all five board members be appointed by the president, by and with the advice and consent of the senate, for staggered six-year terms. The act further requires that the board be bipartisan in composition. No more than three of the five members may be from the same political party, and before appointing members who are not from the president's political party, the president must consult with the leadership of the opposing party. However, the statutory safeguards for privacy in FISA are mainly designed to protect US persons' privacy. PCLOB's oversight is mainly directed at securing compliance with the statute (cf. para. 74) and so it has primarily been concerned with improving privacy protection for US persons. It intends to address the question of safeguards for foreigners in the future.

under Executive Order 12333, relative to SIGINT conducted under the programmes that fall within FISC oversight.

120. An example of a model which combines judicial authorisation with expert follow-up comes from Sweden. A defence intelligence court was established (Försvarsunderrättelsedomstolen or UNDOM) together with a control and monitoring body, the defence intelligence inspection (Statens inspektion för försvarsunderrättelseverksamheten or SIUN).[101] UNDOM consists of two former senior judges and six lay members (mainly former politicians from several different political parties). The judges are appointed by the government after an open recruitment process in the judicial council. The former politicians are appointed by the government after consultations between the parties represented in the parliament. UNDOM is thus a hybrid body. It is assisted by a small registry. UNDOM approves applications, setting further conditions on these. It also approves applications from the signals intelligence agency for testing (above paragraph 77).

121. SIUN also consists of two former senior judges and four former politicians, drawn from different political parties and appointed in the same way as UNDOM. SIUN is thus also a hybrid body. It is assisted by a small secretariat. The government, and other specified bodies may task the signals intelligence agency, FRA, to produce foreign intelligence on a particular issue. This decision is not subject to oversight. FRA then requests a warrant from UNDOM, which sets out what selectors can be used and which signal bearers crossing national boundaries (i.e., which cables, going to which destinations) can be monitored. The raw intelligence is then delivered by telecommunications operators to a location physically under the control of SIUN, which monitors whether the conditions relating to signal bearers set by UNDOM have been complied with before transferring it to FRA. SIUN then monitors FRA's application of the selectors set by UNDOM. If SIUN considers that UNDOM's conditions are being diverged from, it can terminate the search and order destruction of any material gathered.

122. The system is thus a control rather than oversight system, although SIUN also has oversight and complaints functions (see below) in that it is to monitor whether FRA complies with requirements on handling personal data.[102] The Swedish model has only been in place since 2009 and so is relatively new. It has certain major advantages resulting from its expert knowledge, hybrid (legal/political) nature and through being appointed after all-party consultations. Having said this, there is a downside of specialisation. Developing the necessary competence in this area is a slow process. Having, and keeping, expert staff assistance is crucial to the integrity of the monitoring, at the same time as it is difficult to provide a satisfactory career path for staff in such small administrative agencies.

X. Accountability to expert bodies

123. The boundary line between parliamentary, judicial, and expert bodies is not hard and fast. Both the Swedish and German models can be seen as a mixture of all three and, in addition, as exercising control functions. By contrast, the Belgian, Dutch, Norwegian and since 2013, the Danish expert oversight bodies are more clearly expert oversight bodies, not

[101] See Signals Intelligence Act (2008:717) as amended by Prop. 2008/09:201, Förstärkt integritetsskydd vid signalspaning, (Enhanced protection of integrity in signal interception) 20 May 2009. More detailed rules can be found in the ordinance containing the instructions for SIUN, 2009:969. The basic rules which both FRA and the defence intelligence agency must comply with, and which SIUN oversees, are set out in the Defence Intelligence Act (2000:130).

[102] Act on processing of personal data in FRA's intelligence and testing activities (2007:259). The oversight body, SIUN, was itself evaluated by the Swedish National Audit Commission and the oversight found to be satisfactory in general (RiR 2015:2, Kontrollen av försvarsunderrättelseverksamheten). The data inspection board also supervises personal data held by the FRA.

exercising control functions.[103] All these bodies have similar mandates and similarly wide reaching supervisory powers (including over whatever strategic surveillance is used by the bodies they monitor). To use the Dutch model as an example: the CTIVD was established by statute (Intelligence and Security Services Act 2002, ISS Act 2002) and its main task is to review whether the ISS Act 2002, the law governing the activities of the General Intelligence and Security Service, GISS (and the Defence Intelligence and Security Service, DISS), is being implemented lawfully (including the principle of proportionality). Two of the three-member body must be lawyers (Article 65(4)). It is assisted by a secretary and, currently, six investigators. The CTIVD performs its oversight task in two ways: it conducts in-depth investigations resulting in review reports that are made public, and it monitors a number of activities of the services. It has far-reaching statutory powers for the purposes of performing its main review task (sections 74-77, ISS Act 2002). It has access to all relevant classified information held by the services, and this includes access to intelligence being sent to and received from friendly foreign agencies (i.e. the originator rule does not apply).

124. The CTIVD has published several detailed reports on strategic surveillance.[104] The first questioned whether the existing practices were in accordance with the law. It was also critical of the lack of documentation justifying particular signals intelligence operations. The second report is an in-depth analysis of the ways in which the Dutch security and intelligence services acquire and use personal communications data and exchange these with foreign agencies.

125. In conclusion on expert oversight bodies, it is important to stress that these must have unrestricted access to the personal information contained in the signals intelligence agency's databanks if they are to be a meaningful safeguard.[105] The "originator" or third party rule cannot apply to the oversight body. While an expert body in this respect mainly functions to check that the signals intelligence agencies' own routines on minimisation, etc. are functioning correctly, to undertake this task they must be able to do spot checks and thematic studies of the actual data. Thus, they must have their own, residual, investigative capability, preferably (as with the Dutch and Swedish oversight bodies) having direct access to databanks holding personal information. To focus their attention, one can by law require the signals intelligence agency proactively to provide oversight agencies with certain particularly sensitive categories of data.[106] The issue of who may query the bulk data collected and for what purposes, or how data from it can otherwise be disseminated is also something which must be overseen. The trend is nowadays for "fusion centres" for data of interest to internal security. This can obviously greatly increase the size of the group who have access to personal data obtained through signals intelligence. The same can be said about using private contractors. Lax controls on acquisition, combined with lax minimisation rules and lax controls on access to the data is obviously a dangerous combination. But even strong controls on acquisition and minimisation will not be sufficient if there is wide access to the database.

---

[103] For the Danish reform, Law 162, 2013 and the travaux préparatoires (Betaenkning om PET og FE, Nr. 1529, 2012). As noted above, in the US system, PCLOB now exercises a similar general oversight function over signals intelligence.

[104] See in particular, CTIVD, Report 28, "the use of Sigint by DISS", and CTIVD, "Report 38 on the processing of telecommunications data by GISS and DISS" http://english.ctivd.nl/.

[105] See in particular the 2007 report para. 87 "Unless and until they are in a position to make a reasonably informed "second assessment", a monitoring body is not a real safeguard", and para. 237 "Bearing in mind the crucial importance of data banks to the work of a security agency, and the already mentioned distinction between security intelligence and "hard" data … it is imperative that some such supervisory body exists in every State, and that it has sufficient powers, in law and practice, to perform control functions satisfactorily.".

[106] See, for example the German rules above positive reporting duties for data concerning the core of personal integrity.

XI. Complaints mechanisms

126. As noted above, a standard requirement in ordinary surveillance is that the target is notified when the surveillance has ceased, and notification can occur without jeopardising confidential methods, or ongoing operations. In internal security operations, non-notification tends to be the rule.[107] One can have a notification requirement with strategic surveillance too, where selectors have been used which are directly attributable to a particular physical person. This can be found in section 11a of the Swedish Signals Intelligence Act and in the German legislation (G 10 Act, section 12, though only for German residents or nationals). In both cases, exceptions apply where notification would jeopardise security. In the German law, the G 10 Commission must in each individual case approve non-notification. Thus the notification requirement, even if it only rarely leads to actual notification, can still serve a useful function in curbing overuse, because the strategic surveillance agency knows that every time the content of the communications of a citizen or resident has been monitored, it must inform the oversight body of this and convince it that its reasons for not subsequently notifying the person are justified. Notification (and non-notification) figures, if published, can also serve to assuage public concerns regarding the scale of the surveillance.[108]

127. Under the ECHR, a state must provide an individual with an effective remedy for an alleged violation of his or her rights. There are certain requirements before a remedy can be seen as effective.[109] Notification that one has been subject to strategic surveillance is not an absolute requirement of Article 8 ECHR. If a state has a general complaints procedure to an independent oversight body, this can compensate for non-notification. Notification need not be a condition of making a complaint. An example of a general complaints procedure is section 10a of the Swedish Signals Intelligence Act, which provides that "The controlling authority is obliged, at the request of an individual to check on whether his or her messages have been obtained in connection with signals intelligence under this Act and, if so, whether the retrieval and processing of data collected has been in accordance with law. The controlling authority shall inform the individual that the check has been performed." There is no explicit limiting of this to citizens.[110]

XII. Concluding remarks

128. Signals intelligence has a very large potential for infringing privacy and certain other human rights. Understanding strategic surveillance merely through the lens of the right to privacy may not completely capture its potential harm. Unlike the situation for rendition, where the harm is clear, immediate and individualised, the damage insufficiently regulated and controlled signals intelligence can do to society is more diffuse and long term. The existing situation can result in competing or incompatible obligations being placed on companies (typically disclosure vs. data protection) and in circumvention of stronger

[107] The CTIVD experience is that in the case of SIGINT notification never occurs, CTVID Report 24, "on the lawfulness of the performance of GISS of its obligation to notify", p. 23.

[108] In Germany, annual figures are published for notifications made, and not made, see Deutscher Bundestag, Drucksache 18/3709, 8 January 2015, pp. 5 and 8.

[109] See, *mutatis mutandis* "Eradicating impunity for serious human rights violations", Guidelines adopted by the Committee of Ministers, 30 March 2011. Criteria for an effective investigation, are adequacy, thoroughness, impartiality and independence, promptness and public scrutiny.

[110] One can also note that the Dutch CTIVD acts as an internal complaints advisory committee. The advice of the CTIVD is sent to the minister, but ultimately the minister gives an independent decision on the complaint. If the minister does not adopt the advice of the CTIVD, he or she must enclose the advice when sending his/her decision to the complainant. If the complainant disagrees with the decision given by the minister, he or she may lodge the complaint once again, this time with the national ombudsman. The CTIVD handles about 10-15 complaints each year. Around a third of complaints tend to be manifestly ill-founded, a majority is ill-founded, and a minority is founded or partly founded. See, e.g. CTIVD Annual Report 2013-2014, p. 9-11.

domestic telecommunications surveillance procedures. Agreement on minimum international standards on privacy protection thus appears to be necessary.

129. Signals intelligence can be regulated in a lax fashion, meaning that large numbers of people are caught up in a net of surveillance, or relatively tightly, meaning that the actual infringement of individuals' privacy and other human rights is more limited. For parties to the ECHR, it is necessary in any event to regulate the main elements of signals intelligence in statute form. The national legislature must be given a proper opportunity to understand the area and draw the necessary balances. However, European states should not be content with satisfying the quality of law standards of the ECHR. Only strong independent control and oversight mechanisms can assuage public concern that signals intelligence is not being abused.

Glossary

BND	*Bundesnachrichtendienstes,* German Federal Intelligence Service: the foreign intelligence agency of Germany
Bulk data	Very large quantities of communications data (content data and metadata) collected by automated processes
Cable-borne communication	Communication via cable (e.g. fibre optic or copper cables)
CGHQ	*Government Communications Headquarters*, the UK signals intelligence agency
CTIVD	*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten,* Review Committee on the Intelligence and Security Services
Contact chaining	A process of identifying metadata communication patterns which usually takes the form of checking whether previously identified suspect telephone numbers are in contact with other numbers and then whether these numbers are in turn in contact with other numbers
Content data	The content of a telecommunication or stored data, e.g. the words written in an e-mail message or spoken during a telephone call
FRA	*Försvarets Radio Anstalt*, Swedish signals intelligence agency
G10 Commission	German independent oversight body for communications interception, established by the Federal Act Restricting the Privacy of Correspondence, Posts and Telecommunications (set out in Article 10 of the Federal Constitution, and thus called "the G10 Act")
ISP	Internet service provider
Metadata	"Data on data". In the context of telecommunications, this usually includes all data not part of the content of the communication, e.g. numbers called, duration of call, location of the caller and the recipient, etc. Metadata can be analysed for communications patterns
Minimisation	Deletion by human analysts of material irrelevant to an investigation, collected as part of a telecommunications interception
NSA	*National Security Agency*, the United States signals intelligence agency
PCLOB	Privacy and Civil Liberties Oversight Board, United States executive appointed independent oversight body for SIGINT issues
PKGr (or PGr)	*Parlamentarisches Kontrollgremium*, German parliamentary control panel
Selector	Terms used either to filter bulk data in real time or to query collected bulk data. These can relate to language, persons, key words concerning content, communication paths and other technical data, or all of these.

SIGINT (signals intelligence)	Collective term referring to means and methods for the interception and analysis of radio (including satellite and cellular phone) and cable-bound communications
Signals intelligence agency	An intelligence agency engaged in SIGINT collection and analysis, either as its sole purpose or as one of its purposes
SIUN	*Statens inspektion för försvarsunderrättelseverksamheten*, Swedish defence intelligence oversight body
Strategic surveillance	Collection of very large amounts of electronic content data and metadata which are then subjected to computer analysis with the help of selectors
Targeted surveillance	Monitoring of individuals or groups by police or an intelligence agency, initiated after satisfying an independent body that there are concrete facts indicating, and reasonable suspicion, that the targeted individuals or group are involved in crime or threats to national security
UNDOM	*Underrättelsedomstolen*, Swedish defence intelligence court