ACCESS TO INFORMATION BY INTELLIGENCE AND SECURITY SERVICE OVERSIGHT BODIES

(WORKING PAPER – FEBRUARY 2012)

AIDAN WILLS AND BENJAMIN S. BUCKLAND[♣]

1. INTRODUCTION[♠]

The Open Society Foundations, Justice Initiative (OSF-JI) Principles on National Security and Access to Information primarily focus on access to information by individuals and the media. However, as the principles acknowledge, there are some types of information that can legitimately be withheld from members of the public. As a result, certain areas of government activity, particularly in the national security domain, are inevitably shielded from public scrutiny. Yet, in a democratic polity, it is unacceptable for any areas of government activity to escape independent oversight. Accordingly, the task of scrutinising the activities of, *inter alia,* the intelligence and security services (I&SS) is delegated to specialised oversight bodies. The public, through its democratically elected representatives, gives oversight bodies the task of ensuring that I&SS are both effective

[♣] Aidan Wills and Ben Buckland work in the Research Division of DCAF, Geneva. Please send comments or questions to the following email addresses: a.wills@dcaf.ch and b.buckland@dcaf.ch

[♠] This paper draws upon a European Parliament-mandated study: Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (Brussels/Strasbourg: European Parliament, 2011). The text is also informed by the discussions at a DCAF-OSI workshop which brought together senior overseers of intelligence/security services, the police and armed forces from a range of jurisdictions, as well as academic experts. The workshop took place under the Chatham House rule and consequently contributions are not cited directly; the authors are indebted to invaluable contributions of those who attended. In addition, the authors would like to thank the Open Society Foundation Justice Initiative for providing generous support to the project. In particular, the authors are grateful to Sandra Coliver and Emi MacLean for their comments on earlier drafts. Finally, the authors would like to thank Gabriel Geisler and William McDermott who provided invaluable research and editorial assistance. The opinions expressed in this paper do not necessarily reflect the position of DCAF or the Open Society Foundations, Justice Initiative.

and operate in accordance with the law; "if parliament is blinded by insufficient access to national security information, the public is blinded as well."[1]

Access to information is the lifeblood of oversight bodies; it is essential to enabling such bodies to fulfil the role granted to them by the public.[2] Without information about the workings of an organisation, it is unlikely that an oversight body will be able to make a full and accurate assessment of the organisation's effectiveness, efficiency and compliance with national and international law. Incomplete access to information may have the negative consequence of providing a false sense of accountability, transparency and public confidence by giving the impression that overseers are fully aware of and actively scrutinising all I&SS activities.[3] The mere existence of oversight bodies does not guarantee proper scrutiny. Indeed, oversight 'with blind spots' can potentially be more harmful than no oversight at all.

In order to fulfil their functions, standing and ad hoc oversight bodies require access to all types of information relating to I&SS, including classified and otherwise confidential information not in the public domain.[4] This paper will focus on independent oversight bodies: oversight bodies that are not part of the services that they oversee or the executive branch. Such bodies include: parliamentary I&SS oversight committees,

---

[1] Wesley Wark, "Parliament Must Be Trusted With State Secrets," *The Globe and Mail*, 21 January 2011. In the text that follows we use the term 'parliament' in the broad sense of the word to refer to a variety of democratically elected bodies, variously labelled as legislatures, parliaments, assemblies, congresses and so forth.

[2] By information we refer to people, places and documentation, regardless of its form or the method by which it is stored.

[3] South African Ministerial Review Commission on Intelligence, Intelligence in a Constitutional Democracy, (Pretoria: September 2008), 226.

[4] In the text that follows we refer to all these bodies using the catch-all term "oversight body". In this paper, oversight refers to the scrutiny of an organisation's (or individual's) activities with the aim of evaluating its compliance with particular criteria and on this basis, issuing recommendations or orders. Oversight may cover all aspects of an organisation's work or may be confined to specific areas. Overseers may scrutinise these activities in accordance with very general criteria or may focus on aspects such as their compliance with the law or their overall effectiveness. Oversight is a term which can encapsulate processes such as monitoring, evaluation, scrutiny and review. Oversight should, however, be seen as distinct from concepts such as 'management' and 'control', which imply direct involvement in decision making regarding an organisation's policies or practices.

specialised and general non-parliamentary oversight bodies,[5] and commissions of inquiry. The practices and procedures that apply to access to information by such bodies are ordinarily different to those which apply to access to government documents and information by members of the public (through, for example, freedom of information requests).[6] Therefore, this issue merits examination as a separate issue.

Although the focus of this paper is on "institutional access" to information, it should also be noted that individual members of oversight bodies may also seek to access information relevant to their work. This is particularly true in the case of parliamentary oversight committees, where individual members may seek to use those tools and powers granted to all members of parliament (parliamentary questions, parliamentary privilege) in order to try and access information relevant to their oversight work.

While judicial bodies may also play an important role in this domain, they will not be discussed in this paper. Similarly, we will not consider the related issue of access by parliament as a whole or of access in other domains. The parliamentary and non-parliamentary oversight bodies discussed here may be responsible for the oversight of the armed forces, law enforcement, and border management agencies. However, for reasons of concision, this paper will focus largely on those bodies that oversee I&SS.[7] This is a narrower focus than that found in the principles more generally. We feel, however, that the examples discussed here have broader resonance beyond the specific examples discussed below.

---

[5] Examples of such bodies include: ombuds institutions, supreme audit institutions and anti-corruption bodies.

[6] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (Brussels: European Parliament, 2011), 121.

[7] The term 'I&SS' here refers to a state body that collects, analyses and disseminates information—on threats to national security or other national interests—to policy-makers and other executive bodies. Such entities may perform these 'intelligence functions' exclusively outside of their state's territorial jurisdiction (e.g., the UK's Secret Intelligence Service), exclusively within their state's territory (e.g., Germany's Federal Office for the Protection of the Constitution), or both inside and outside their territory (e.g., the Dutch General Intelligence Service or AIVD). In a few states (e.g., in Sweden and Denmark), these bodies may also possess police powers and are therefore sometimes called 'police security services'. Please note that for reasons of consistency, we will use the term 'I&SS' to refer to all of the aforementioned bodies, e.g., organisations which are variously labelled as 'security services', 'domestic intelligence agencies' or 'intelligence services'.

In many states, access to information by oversight bodies cannot be taken for granted and there is a pressing need to identify good practices that can help to strengthen legal and institutional frameworks in this regard. It is this access that is the subject of the following paper. A second aim of this paper is to provide a comparative overview of national practices in this area. It is hoped that this will serve as a useful background to contextualise the section on access to information by oversight bodies of the OSF-JI Principles on the Right to Information and National Security.

The following text is organised into four main parts. First, we look at overseers' information needs. Second, we discuss the powers and methods available to them in accessing information. Third, we turn to limitations on their access. Finally, we will address the issue of protection of information by oversight bodies.

2. INFORMATION

The following section addresses relevant legal frameworks, as well as the ways in which mandates shape overseers' information needs.

Access to information by oversight bodies should always be enshrined in and regulated by law. This helps to provide them with some degree of certainty regarding the types of information that they can (and cannot) access, as well as potentially giving them grounds upon which to challenge any refusal to grant access. Access to information by parliamentary oversight bodies is commonly governed by separate regulations to those governing parliamentary access to information in other fields (such as trade policy, for example). For example, the UK Intelligence and Security Committee (a committee of parliamentarians) access to information is regulated by legislation which also covers the activities of two of the UK's I&SS. Elsewhere, the German *Bundestag's* Parliamentary Control Panel is governed by its own statute, which includes detailed provisions on access to information.[8] Access to information by non-parliamentary oversight bodies (such as Canada's Security Intelligence Review Committee and the Belgian Standing Intelligence Agencies Review Committee) is generally regulated by the legislation upon which they are based. Such legislation is sometimes part of broader legislation on the I&SS (as is the case in Canada and The Netherlands).

The legal framework for access to information by oversight bodies is typically comprised of five elements, each of which will be discussed in more detail below:

1. the right to demand or request information relevant to their mandate from the I&SS, the executive branch and other relevant parties;
2. the concomitant obligation of compliance on the part of these actors;
3. the powers and methods available to oversight bodies to ensure such access;
4. possible limitations (if any) on access to classified information; and

[8] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.* See, for example: Germany, Parliamentary Control Panel Act; UK, Intelligence Services Act, Schedule 3, 1994; Italy, Law 14/2007; Spain, Ley 11/2002.

5. requirements for the proactive disclosure of certain types of information to overseers on the part of the executive and I&SS, without being requested to do so.

In law, it is good practice to impose no restrictions on access to information by oversight bodies. This includes all information regardless of its form, level of classification, author or addressee.[9] In some states this can include information held by the executive, I&SS and other public bodies, as well as information received from foreign entities. Table 1 provides an overview of the scope of access to classified information by a selection of specialised (parliamentary and non-parliamentary) oversight committees in Europe.

In practice, the types of information that overseers require in order to effectively fulfil their functions will depend on and be defined by the nature of their mandate. Indeed, in the absence of this link "there is a risk that overseers will either be unable to effectively fulfil their mandates due to a lack of information or will attempt to access information that may be unrelated to their work."[10] For this link to function effectively, both parties need a clear understanding of the overseer's mandate. Overseers obviously require an understanding of their mandate in order to know what types of information they should seek. Similarly, it is essential that employees of I&SS and the executive branch possess a proper understanding of overseers' mandates. This helps to avoid situations in which they obstruct overseers' attempts to access information out of ignorance of their role. In view of this, some oversight bodies make efforts to increase their visibility and understanding of their work through, for example, training courses for new staff of I&SS.

With regards to the oversight of I&SS, mandates vary both in terms of the subject of their oversight (for example, policy, finance, operations, administration) as well as the criteria used for oversight (for example, compliance with the law, propriety, effectiveness, efficiency). Mandates are often framed in terms of either the 'subject' or the 'criteria' of

[9] This is, for example, the case in the Belgian Standing Intelligence Agencies Review Committee (Committee I) (discussed in Wauter Van Laethem, in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*), the US Congressional Intelligence Oversight Committee (Kate Martin, in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*) and the Dutch Review Committee on the Intelligence and Security Services.

[10] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* 121.

oversight. This has an impact on the information needs of an oversight institution. For example, a mandate to examine the administration and finances of an I&SS may demand significantly less detailed access to information pertaining to operations. On the other hand, oversight bodies mandated to oversee the effectiveness and/or legality of all aspects of a service's work may require a significant or, indeed, granular level of detail regarding operational activities.[11] Finally, oversight bodies with a complaints-handling role have specific information requirements relating to their duties to investigate and, if necessary, to provide some form of redress.

Regardless of the mandate, oversight bodies are likely to require access to all or some of the following categories of information: internal guidelines and manuals; ministerial instructions or directives; policy documents; accounts and other financial data; details of complaints made to I&SS; operational instructions and reports; communications records; and files or archives on persons, groups or issues.

Clearly formulated legal mandates can be seen as providing an objective basis for overseers' "need to know." In the absence of this, disputes surrounding access to information are more likely to arise.

Beyond the question of mandates, some authors argue that the level of access to information should vary depending on the type of oversight body in question. In particular, it is often posited that parliamentary oversight committees should not be afforded the same level of access to information as non-parliamentary bodies such as inspectors general and supreme audit institutions (SAIs).[12] This view is often premised on the assumption that, as political bodies, parliamentary oversight committees cannot be trusted to handle classified information appropriately. We take issue with this assertion. As we argue throughout this paper, access to information is essential to the proper functioning and credibility of all oversight bodies and should thus be determined by their mandates (and their interpretations thereof) rather than by their institutional

[11] Stuart Farson, "Establishing Effective Oversight Institutions," (Working Title), Tool 2, eds., Hans Born and Aidan Wills (forthcoming).

[12] See, for example, Laurie Nathan, "Intelligence Transparency, Secrecy and Oversight in a Democracy" (Working Title), Tool 3, eds., Hans Born and Aidan Wills (forthcoming).

composition. Furthermore, experience from numerous jurisdictions has illustrated that parliamentary oversight bodies are more than capable of properly handling classified information.[13]

Regardless of their mandate or the type of institution, it is good practice for the law to empower oversight bodies to determine what information is necessary for their work and be able to demand access to such information.[14] The law on oversight of the Dutch I&SS by the non-parliamentary Review Committee on the Intelligence and Security Services (CTIVD) provides a good example in this regard:

> The relevant Ministers, the heads of the services, the co-ordinator and furthermore everyone involved in the implementation of this act and the Security Investigations Act will, if requested, furnish all information to the supervisory committee and will render all other assistance the supervisory committee deems necessary for a proper performance of its duties.[15]

Such provisions can be seen as underpinning the independence of oversight bodies. Indeed, the operational independence and effectiveness of oversight bodies can be seriously undermined if the subjects of oversight (i.e., the executive and services) are able to determine what information is relevant and, thus, made available to overseers. This can happen when the law affords the executive or directors of services discretion to withhold certain types of information (see section 4.1 below, for more details).

The fact that oversight bodies can access any information does not, however, mean that they should access any information without good reason for doing so. Norwegian law provides an interesting example in this regard. The *EOS Utvalget* Committee (a non-parliamentary oversight body which can include parliamentarians) has access to all

---

[13] For further details on the protection of information by oversight bodies, please see: Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 137-144.

[14] See for example, the South African Intelligence Services Oversight Act, Section 7(8)(a); see also, Verhoeven in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* and Craig Forcese, "Complaints Handling" (Working Title), Tool 3, eds., Hans Born and Aidan Wills (forthcoming).

[15] Dutch Intelligence and Security Services Act 2002, Article 73(1)

information it deems necessary. However, the law explicitly instructs that "the Committee shall not seek more extensive access to classified information than is necessary for purposes of monitoring."[16] In addition to guidance provided in law, overseers should (and do) exercise appropriate professional discretion when determining what information they need to know in order to fulfil their mandate.

The I&SS and the executive branch are sensitive to what are known as "fishing expeditions" by overseers, whereby they cast about in search of information without proper reason and outside the context of investigations or periodic oversight activities. This is particularly relevant with regard to parliamentary oversight bodies because there may be concerns that some parties' representatives may seek to gather information which they can use for political purposes.[17]

With this in mind, the law may include provisions which only permit particularly sensitive types of information to be made available to a parliamentary oversight body if a qualified majority (representing cross-party support) of its members request it. An example of this type of mechanism can be found in Hungary, where the votes of two-thirds of the parliament's National Security Committee are required in order for the committee to access specific information concerning I&SS methods.[18] This must take place within the context of an investigation by the committee. Similarly, in Bosnia and Herzegovina, in cases involving suspected illegal activity within the Intelligence and Security Agency, the parliamentary committee can, given the consent of a simple majority of members, compel the Chair or the Director General "to provide information" essential for oversight, regardless of its sensitivity.[19] This type of mechanism can assuage concerns (on the part of the services and the executive) regarding attempts to

---

[16] Norway, Instructions for the Monitoring Intelligence, Surveillance and Security Services (EOS), (issued pursuant to Section 1 of Act No. 7 of 3 February 1995 relating to the of Monitoring Intelligence, Surveillance and Security Services), Section 5.

[17] Venice Commission Report, para. 115.

[18] Hungary – Act No. CXXV of 1995, Section 16(2).

[19] Bosnia and Herzegovina, Law on OSA, Official Gazette BiH No. 12/04 Article 21, cited in Denis Hadžović, Emsad Dizdarević, "Bosnia and Herzegovina" (Chapter 3) in *Intelligence Governance in the Western Balkans,* Hans Born, Miroslav Hadžić and Aidan Wills (forthcoming).

obtain information for partisan political purposes. While it is clearly preferable for no limitations to exist on access, such an option (when restricted in applicability to the most sensitive categories of information: sources and methods, for example) may, nevertheless, be preferable to blanket restrictions on access to information. This mechanism does have disadvantages, however. Most significantly, parliamentary oversight is often highly politicised and the likelihood of securing a qualified majority to obtain information against the wishes of the government of the day is fairly remote.

3. POWERS AND METHODS

While the preceding section addressed the information requirements of oversight bodies, the following section will examine the methods and powers by which they can ensure such access. In order for overseers to make use of their right to access information they need concomitant powers.

3.1 PASSIVE AND ACTIVE ACCESS TO INFORMATION

Overseers access information using a range of methods and powers that will be discussed below. Before turning to this discussion, however, it is worth noting an important distinction between two modes of access: active and passive.[20]

"Active" access refers to the ability of oversight bodies to *request* or to *demand* access to particular information necessary to the fulfilment of their mandate. This distinction is highly significant because the executive and I&SS are not legally obliged to respond favourably to *requests* from overseers, and consequently, they cannot enforce such access. By contrast, the right to demand access to information implies that the executive and I&SS are required to comply. In order for such access to be effective, the power to *demand* information is essential, supported by appropriate enforcement powers and the necessary expertise and resources (see section 3.5 below).

The second, "passive" mode refers to the proactive disclosure of information by the executive and I&SS to oversight bodies. Proactive disclosures typically occur on a periodic basis and the types of information which must be disclosed are normally prescribed by law. Such disclosures normally take the form of written reports and hearings. Common types of information subject to proactive disclosure include:

- unlawful activity (including, for example, human rights violations, fraud, corruption);[21]

[20] See also Monica Den Boer, "Conducting Oversight" (Working Title), Tool 3, eds., Hans Born and Aidan Wills (forthcoming).

- intelligence failures;
- information sharing and cooperation agreements;[22]
- covert action (which may include notification prior to the commencement of an operation);[23]
- general activities and threat assessments (including annual activity reports);[24]
- financial information and reports;[25]
- changes to internal regulations and rules.[26]

Oversight bodies may also be permitted to receive information from complainants.[27] In addition, the law may require (or otherwise encourage) employees of the executive branch and the services to disclose information showing wrongdoing to oversight bodies (i.e., whistleblowing).[28]

Alongside issues raised in the media and by civil society organisations, proactive disclosure of information is an important basis for the work of oversight bodies. Proactive disclosures are particularly important for parliamentary oversight

---

[21] For a good example regarding financial malpractice, see : South African Public Finance Management Act, 1996. Section 52.2(a-b); US National Security Act, 1947, Section 102a(c)(7b).

[22] See, for example, Canada, Canadian Security Intelligence Service Act, 1984. Section 17.2.

[23] The US Congress provides the best example of this practice, for a comprehensive overview, see : Alfred Cumming, "Sensitive Covert Action Notifications: Oversight Options for Congress," Congressional Research Service, Washington D.C. April 2011; Alfred Cumming, "Gang of Four: Congressional Intelligence Notifications, Congressional Research Service, Washington D.C. March 2011.

[24] See, for example, legal requirements in Spain. Law 11/2002 A.11.2 ; 11.4 ; Germany, Parliamentary Control Panel Act, Section 4.1; Australian IGIS Act, Section 32A

[25] See, for example, Federico Fabbrini and Tommaso Giupponi, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Italy" Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*; Susana Sanchez, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Spain" Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[26] See, for example, Hungary, Act No. CXXV of 1995. Section 14.3 ; Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for threat Assessment. A.33.

[27] Craig Forcese, "Complaints Handling" (Working Title), Tool 8, eds., Hans Born and Aidan Wills (forthcoming). See, for example, the Hungarian Parliament's National Security Committee, the Swedish Commission on Security and Integrity Protection and the Australian Inspector General for Intelligence and Security.

[28] See, in this regard, Benjamin S. Buckland and Aidan Wills, *Blowing in the Wind? Whistleblowing in the Security Sector* (forthcoming).

committees, whose members may not always have sufficient time or the requisite knowledge and expertise to uncover relevant information themselves.[29]

Proactive disclosure often serves as the basis for active requests or demands for additional information, as it gives oversight bodies an indication of the direction in which their inquiries should proceed. As such, proactive disclosure, while necessary, is not sufficient for ensuring that oversight bodies have access to the information they need. A reliance on information that is proactively disclosed by the executive and security services could lead to unacceptable levels of filtering of information received by oversight bodies. This may undermine their credibility and independence.

3.2 METHODS OF ACCESS

This sub-section will provide an overview of the main methods used to access information held by I&SS and the responsible executive bodies. Where possible, overseers use as diverse a range of methods as possible in order to ensure that they gather information from multiple sources.[30] It should be noted that the type of methods used, as well as the genres of information required by overseers, depend on the type of oversight being undertaken. For example, periodic inspections of the use of intelligence collection powers are likely to follow a standard methodology, including, *inter alia*, viewing samples of warrant applications.[31] By contrast, investigations into particular cases or thematic issues, such as cooperation with foreign I&SS, are likely to involve a broader range of methods.

3.2.1 INTERVIEWS AND HEARINGS

The most common method of access to information available to oversight bodies are meetings, hearings and interviews with relevant persons. These may take the form of regular or *ad hoc* hearings with relevant ministers and agency directors. Equally, some

[29] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 86-91; 100; 129.

[30] See for example the work of Canada's Security Intelligence Review Commission, Security and Intelligence Review Commission, Annual Report 2009-2010, 9.

[31] UK Intelligence Services Commissioner, *Report of the Intelligence Services Commissioner 2010*, HC1240, 11-12.

oversight bodies meet agency officials on a more informal basis to learn more about their activities; such meetings do not necessarily take place in the context of any formal oversight activity.[32] In addition to periodic hearings, most oversight bodies have the power to summon such persons at their discretion or conduct interviews *in situ* (often within the context of inspections).

While some oversight bodies do not have the power to compel such individuals to appear before them, in practice, they are unlikely to want to risk the bad publicity that would be the consequence of any outright refusal.[33]

With regards to employee below the level of director, access is often more restricted and may require political approval.[34] The French parliament's *Délégation parlementraire au renseignement* DPR, for example, is not permitted to invite anyone below the level of director to appear before it.[35] In some parliamentary systems it may be seen as problematic to require civil servants to appear before an oversight committee because they are not considered politically responsible or accountable. If a body does have the power to call such individuals, this should not be subject to approval by the executive. This is, for example, the case in the Italian Parliament, where the Parliamentary Committee for the Security of the Republic (COPASIR) must first request approval from the Prime Minister before asking officers below the level of director to appear before it.[36] Such limitations can interfere with the operational independence of oversight bodies by introducing a political filter that may shield sensitive issues from proper scrutiny.

---

[32] Australian Inspector General of Intelligence and Security, *Annual Report 2008-2009*, 36-37, 49.

[33] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 136.

[34] For example, the US Congressional Intelligence Committees (cited in Martin, Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*) and the Hungarian Parliament's National Security Committee (cited in Gabor Földvary, in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*.

[35] See, Charlotte Lepri, Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[36] Italy, Law 14/2007, Article 31(2).

On occasion, former employees of I&SS may have information which is relevant to the work of overseers. It is, therefore, good practice for overseers to be able to call such individuals to appear before them. This is the case, for example, in Belgium, where the Standing Intelligence Agencies Review Committee (an autonomous non-parliamentary body) may order former members of the I&SS to testify under oath, with penalties for non-compliance.[37] However, elsewhere, overseers have no access or may require ministerial authorisation to hear testimony from former civil servants, as is the case for The Dutch Review Committee on the Intelligence and Security Services (CTIVD).[38] It is interesting to note that the Committee has criticised the fact that it is dependant upon the permission of the executive in order to access information from persons in this category.[39]

Some oversight bodies may also be empowered to request or require testimony from members of the public who may have relevant information about the activities of the I&SS.[40] Equally, members of the public may appear before oversight bodies in cases relating to complaints.[41]

3.2.2 SITE VISITS AND INSPECTIONS

Many specialised oversight bodies, including parliamentary committees, have the power to inspect installations under the control of the I&SS. This is the case, for example, in New Zealand, where the Inspector General of Intelligence and Security has the power of entry onto I&SS premises, after having notified the agency director.[42] In many other cases, oversight bodies have the power to make unannounced visits.

---

[37] Art 24, para 2, law on the regulation of the control of police services, intelligence services and the coordinating organ for threat analyses, 1991 (version 2011)

[38] Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report 2009-2010*, 13.

[39] Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report 2009-2010*, 13.

[40] See, for example, the Norwegian EOS Utvalget Committee, *Annual Report 2008*, 51.

[41] See, for example, Canada's Security Intelligence Review Committee.

[42] Other examples include: the German Parliament's Control Panel (cited in De With and Kathmann, Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*); the Italian COPASIR (Italy, Law, Article 31(14–15)); the Australian Inspector General for Intelligence and Security (Australia, Inspector General of Intelligence and Security Act 1986, Section 9b, 18–19); and the Dutch Parliament's Intelligence

Inspections can serve to enhance an oversight body's understanding of an I&SS, and they are a useful opportunity for oversight bodies to conduct interviews with a number of staff and access physical and electronic records.[43] They may be particularly important in cases where the I&SS have powers of arrest and detention. In such cases, inspections are an opportunity to ensure that detention and questioning is carried in compliance with the law. In Australia, for example, the Inspector General has the right to be present while the Australian Security Intelligence Organisation (a domestic intelligence agency) questions any individual.

3.2.3 DIRECT ACCESS

Among the most formidable powers of access to information afforded to oversight bodies is that of direct access to agency databases and files. In practice, this means that overseers have access to all information stored electronically by an I&SS, without the need to request specific documents or information. Oversight bodies with such powers normally have their own permanent offices within the premises of an I&SS. For example, the Dutch CTIVD and Belgian Committee I both have facilities of this type, which permit them to log in directly to an agency's files.[44]

Such access permits oversight that is free of any "filtering" by the services and may permit in-depth oversight of operation activities, insofar as this may be relevant to an overseer's mandate. However, it should be noted that overseers may, nevertheless, be reliant on the assistance of the services to navigate and interpret the information to which they have access. Furthermore, such methods are only useful in cases where relevant records are maintained.

---

and Security Services Committee (The Netherlands, Rules of Procedure of the Dutch Second Chamber 1994, Chapter 7, Paragraph 5).

[43] See, for example, the Canadian Security and Intelligence Review Committee, *Annual Report 2009-2010*, 25-26.

[44] Nick Verhoeven and Van Laethem both in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*.

3.3 FORMAL AND INFORMAL POWERS

Legal powers to enforce access to information are an important corollary to the methods of access discussed above. There are several powers which, while seldom used, serve to reinforce the position of oversight bodies when seeking information from the executive and I&SS.

First, it is good practice for the law to require relevant persons to cooperate with requests for information from oversight bodies and to proscribe administrative or criminal penalties for any failure to do so. Indeed, the failure to provide information can, in some circumstances, be considered obstructing an investigation and carry significant criminal or other penalties (such as a bar on public service).[45] This implies that oversight bodies can refer such failures to law enforcement and/or to prosecutorial authorities. It is important to note that an individual's obligation to provide information to an oversight body generally overrides any obligation concerning professional confidentiality or the non-disclosure of classified information. It follows that the law should also protect persons from retaliation or punishment for disclosing information to an overseer. This is the case in South Africa, for example, where section 15(3) of the *Public Audit Act* states that:

> (a) A person who is required in terms of any legislation to maintain secrecy or confidentiality, or not to disclose information relating to a matter, may be required by the Auditor-General to comply with any of the requirements in this section, even though the person would be otherwise in breach of that person's obligation of secrecy or confidentiality or non-disclosure.
>
> (b) Compliance with a requirement of this section is not a breach of any applicable legislation imposing the relevant obligation of secrecy or confidentiality or nondisclosure.[46]

Second, some oversight bodies can subpoena persons and documents which they deem to be relevant to their work (see Table 1 for an overview of investigatory powers held by

[45] This is the case, for example, in Belgium. See Articles 48 and 49 of the Belgian *Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment*, 18 July 1991.

[46] Republic of South Africa *Public Audit Act*, No. 25 of 2004, Sections 15-16.

European intelligence and security oversight bodies).[47] This imposes a legal requirement on relevant persons to appear before oversight bodies or to provide them with specific information when requested to do so. In addition to this, overseers can require that testimony is given under oath or affirmation, which renders any deliberate failure to provide accurate or complete information a criminal offence.[48] Accordingly, overseers can seek the assistance of law enforcement agencies or the police to enforce such powers.[49]

Third, some oversight bodies may have direct recourse to law enforcement powers (including powers of search and seizure) in order to access necessary information. In South Africa, for example, the Auditor-General may, under the authority of a warrant, enter and search premises and seize relevant information, with the assistance of law enforcement agencies, if necessary.[50] Elsewhere, the Police Ombudsman of Northern Ireland has recourse to similar powers.

Such powers may be particularly necessary with regards to the oversight of operational activities, which the I&SS or the executive view as particularly sensitive, and about which they may be unwilling to yield information.[51] Furthermore, strong investigatory powers give oversight bodies a degree of predictability in their work and can help them to avoid incessant legal or other conflicts regarding rights of access. It should, nevertheless, be noted that such powers do not necessarily guarantee that overseers can access all necessary information. Overseers need to know what they are looking for and

---

[47] See, for example: The Netherlands, Intelligence and Security Services Act 2002, Article 74; Australia, Inspector General of Intelligence and Security Act 1986, Sections 18–19. On the US Congressional Intelligence Committees, see Martin, in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[48] See, for example: Australia, Inspector General of Intelligence and Security Act 1986, Sections 18–19; Belgium, Act Governing Review of The Police and Intelligence Services and of The Coordination Unit for Threat Assessment, Article 48.

[49] See, for example: Belgium, Act Governing Review of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 48; Germany, Parliamentary Control Panel Act, Section 5.

[50] South Africa, *Public Audit Act*, Vol. 474 Cape Town 20 December 2004 No. 27121, Article 16. See also the Police Ombudsman of Northern Ireland. Police (NI) Act 1996, Section 56 (3).

[51] For example, Canada's Security Intelligence Service Act explicitly mentions subpoena powers in this context (CSIS Act, Section 50).

they cannot always be aware of (let alone prevent) the concealment or destruction of relevant information by I&SS.

3.4 INDIRECT POWERS

Although recourse to strong investigatory powers can be important for facilitating overseers' access to information, such powers are not a prerequisite for accessing information. Overseers have a number of other instruments at their disposal for persuading or even compelling the executive and the I&SS to provide them with information.

First, parliamentary oversight bodies can make use of parliaments' formidable budgetary powers to force the executive to disclose information which the committee deems relevant. Notably, they can work with other relevant committees (e.g. budget or finance committees) to deny or decrease funding for aspects of a service's work unless requested information is disclosed. This practice has sometimes been used in the US. Congress to extract information from the executive.[52]

Secondly, both parliamentary and non-parliamentary oversight bodies always have the option of publicly reporting failures to comply with requests for information. This may be done on an *ad hoc* basis or through annual reports. This type of negative publicity can be extremely harmful to the reputation of an I&SS or the executive and can serve to encourage compliance.

Finally, it should not be assumed that the executive and I&SS are inherently hostile to providing overseers with information. They normally have an important stake in the credibility and effectiveness of a system of oversight because this helps to ensure their own credibility and to promote public confidence.[53] In view of this, it is not usually in the interests of the executive and the I&SS to be seen publicly to be obstructing the work of

[52] See for example, Louis Fisher, "Congressional Access to Information: Using Legislative Will and Leverage," *Duke Law Journal* 52, no. 2 (November 2002), 323-402.

[53] Ian Leigh, Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 297.

oversight bodies. Indeed, the obstruction of the work of overseers may have the paradoxical effect of provoking calls by parliament and the public for endowing overseers with greater investigatory powers.[54]

Before concluding this section, it is important to note that trust is the most important facilitator of access to information by oversight institutions. In many cases, overseers rely on a good working relationship with those they oversee in order to guarantee that they receive all relevant information in a timely and smooth manner. While it is important that oversight bodies have the powers discussed above, their use may, nevertheless, be counterproductive in the pursuit of effective oversight in the long term. Frequent use of such powers implies a lack of mutual trust between overseers and the overseen and is likely to increase resistance to cooperation on the part of the I&SS. Ultimately, these powers are best viewed as an option of last resort, in the event that an agency or the executive fails to cooperate with an investigation.

3.5 MAKING USE OF INFORMATION: EXPERTISE AND RESOURCES

Oversight bodies require financial and human resources in order to gather and interpret information.[55] While no oversight body has sufficient resources to examine all of the activities (and thus access all of the information) relevant to their mandate,[56] their capacity to properly scrutinise selected activities is hugely dependent on human resources. Extensive access to information is futile unless oversight bodies have the appropriate capacities to use it.

Adequate numbers of staff with appropriate expertise are fundamental to the effectiveness of oversight bodies. Members of both parliamentary and non-parliamentary oversight bodies are typically very senior figures who often do not have the time or specialised expertise to pore over and interpret detailed information. This is

---

[54] Ian Leigh, Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 297.

[55] See, for example, European Commission for Democracy Through Law (2007), 'Report on the Democratic Oversight of the Security Services', adopted by the Venice Commission at its 71st plenary meeting, Venice, 1–2 June 2007, 36.

[56] By way of example, see Canadian Security and Intelligence Review Committee, *Annual Report 2009-2010*, 9-10 ; see also, CTIVD, *Annual Report 2009-2010*, 5.

particularly true of parliamentary oversight bodies whose membership may change relatively frequently, and whose members are amongst the most senior parliamentarians.

In view of this, staffers perform much of the research and analytical work which is central to oversight bodies' functions. This includes identifying relevant issues to examine, questions to ask and information to request. In order to perform these tasks, staffers need access to all of the information that members can access, and it is good practice for them to be permitted to attend all relevant meetings.[57] It is noteworthy that staffers can include both persons employed by a parliamentary or non-parliamentary oversight body and (in the case of parliamentary oversight) advisors to parliamentarians or political parties.

In addition to "in-house" staff, many oversight bodies can engage the services of external experts to assist with specific investigations.[58] This can be highly beneficial in helping oversight bodies to interpret *inter alia* complex technical information about the activities of I&SS. In common with permanent staff, external experts ordinarily require security clearance in order to be hired by an oversight body.

[57] This is not the case in Germany, for example.

[58] The Luxembourgois Parliamentary Control Committee can, after consulting with the Director of the Intelligence Services and with a two thirds majority, decide to engage an independent expert to assist it, cited in the Venice Commission Report 2007, para. 130. See also, the Norwegian EOS Utvalget, *Annual Report 2008,* 51; and Hungary, Act No. CXXV 1995, Section 14(5).

TABLE 1: POWERS AND METHODS AVAILABLE TO SELECTED PARLIMENTARY AND NON-PARLIAMENTARY INTELLIGENCE AND SECURITY OVERSIGHT BODIES[59]

STATE	Receive and review annual reports of agencies	Periodic meetings with management of agencies	Invite management to give testimony at other times	Invite external experts	Invite members of the public	Subpoena intelligence officers to testify	Subpoena members of the executive branch to testify	Subpoena agencies to provide evidence	Inspect premises of intelligence agencies
Austria - *Standing Subcommittee of the Interior Affairs Committee*				0	0				
Belgium - *Standing Intelligence Agencies Review Committee*	0	0	0	0	0	0			0
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	0	0	0	0				0	0
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*	0	0	0	0					0
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	0	0							
Estonia - *Security Authorities Surveillance Select Committee*	0	0	0	0	0				0
Finland - *The Administration Committee*	0	0	0	0	0				
Germany - *Parliamentary Control Panel (PKGr)*	0	0	0	0	0				0
Germany - *G10 Commission*		0	0	0	0				
Greece – *Authority for Communication Security and Privacy (ADAE)*			0	0	0				
Hungary - *Committee on National Security*	0	0	0	0	0			0	0
Italy - *COPASIR*	0	0	0	0				0	0

[59] Adapted from Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 2011, 134-5.

STATE	Receive and review annual reports of agencies	Periodic meetings with management of agencies	Invite management to give testimony at other times	Invite external experts	Invite members of the public	Subpoena intelligence officers to testify	Subpoena members of the executive branch to testify	Subpoena agencies to provide evidence	Inspect premises of intelligence agencies
Latvia - *National Security Committee*	0	0	0	0	0				
Lithuania - *Committee on National Security and Defence*	0	0	0	0	0				
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	0	0	0	0	0	0	0	0	0
Poland (Sejm) - *Special Services Oversight Committee*	0	0	0	0	0				
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	0	0	0	0	0				0
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	0	0	0	0	0				0
Slovakia - *Committee for the oversight of the Slovak Information Service - Committee for the oversight of the National Security Authority of Slovak Republic*	0	0		0	0				0
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	0	0	0	0					0
Sweden - *The Commission on Security and Integrity Protection*	0		0	0					
The UK - *Intelligence and Security Committee (ISC)*	0	0	0	0	0				0

4. LIMITATIONS ON OVERSEERS' ACCESS TO INFORMATION

As we argued above, it is good practice for oversight bodies to have access to all information which they deem to be necessary for the fulfilment of their functions. Oversight bodies do, however, face a plethora of legal and practical restrictions on their access to information (see Table 2 for an overview of restrictions on access to information by oversight bodies in Europe). The purpose of this section is to highlight some of these restrictions and to offer examples of how they can be framed in a way that has the least impact on democratic oversight.

It is of fundamental importance that any limitations on overseers' access to information should be clearly and narrowly defined in law. This helps to ensure predictability and makes it easier for overseers to challenge denials in specific cases. Furthermore, we can identify five principles that should govern any use of legal provisions permitting the limitation of access to information by oversight bodies.

First, any decision to deny access to information to an oversight body should be made by the minister responsible for the I&SS concerned and not by the services alone. This ensures that there is political responsibility and accountability for the use of any limitations. This is one of the notable proposals made in the UK Government's recent Green Paper which dealt with, *inter alia*, reform of the Intelligence and Security Committee.[60]

Second, the invocation of such clauses should be adequately motivated and accompanied by a detailed written justification.[61] As the German Constitutional Court stated in a case concerning access to information by an *ad hoc* parliamentary committee of inquiry examining various matters relating to the I&SS: "in order to permit the verification of the weighing of interests, […] the refusal [to grant access to information] has to be accompanied by substantiated reasoning."

[60] UK Government Green Paper on Justice and Security, CM 8194, October 2011.

[61] See for example, the German PKGrG Act, Section 6(2)

Third, overseers should to be able to apply for the judicial review of any decision to invoke a particular limitation. It is noteworthy in this regard that several parliamentary groups in the German *Bundestag* successfully took the federal government to the Constitutional Court for both failing to provide information and for preventing employees of the federal government from testifying about certain matters before a parliamentary committee of inquiry.[62]

Fourth, overseers should have and make use of the right to publicise the fact that they have been denied access to information and to explain the impact this has had on their work.

Finally, we argue that the law may prohibit the use of limitations in cases in which an oversight body is investigating serious violations of the law.[63]

Before turning to a discussion of the legal limitations on overseers' access to information, it is worth briefly noting that the existence of restrictions will be influenced by a complex set of historical and institutional factors. Notably, parliamentary access to information will be heavily influenced by the electoral system, the constitutional balance of power and the system of government (whether, for instance, the executive is situated within parliament or outside it in a presidential system, for example).

It should also be noted at the outset that the absence of formal limitations does not translate seamlessly into consistent and easy access to information by oversight bodies. Indeed, delaying tactics on the part of the I&SS can be as damaging as any outright refusal.[64] On the other hand, even where clear limitations exist, they may not be invoked by the executive or security services; as we argued above, the I&SS have a stake in the

[62] German Federal Constitutional Court Press Office, *Press Release No. 84/2009* of 23 July 2009 (in English) pertaining to order of 17 June 2009 – BvE 3/07 (German only).

[63] German Federal Constitutional Court Press Office, *Press Release No. 84/2009* of 23 July 2009 (in English) pertaining to order of 17 June 2009 – BvE 3/07 (German only).

[64] CTIVD, *Annual report 2009-10*, 13.

credibility of oversight and may, thus, be willing to cooperate even in cases where they may not have to.

4.1 EXECUTIVE DISCRETION

Perhaps the most common and potentially most significant limitation on access to information by oversight bodies are legal provisions which grant the executive and/or directors of I&SS broad discretion to limit access. Such provisions commonly enable the executive to rely on poorly defined reasons to limit access. Examples of these provisions include Italy, where the executive can deny the Parliamentary Committee for the Security of the Republic access to information if granting such information might "jeopardise the security of the Republic."[65] British law includes yet greater scope for executive discretion, permitting the directors of the I&SS to deny parliament's Intelligence and Security Committee access to information because (among other reasons) "the Secretary of State [responsible minister] has determined that it should not be disclosed."[66]

Legal provisions granting the executive a broad margin of discretion are particularly problematic in view of the fact that the executive is an integral part of the intelligence process – the subject of oversight by parliamentary and other oversight bodies. There is clear potential for conflicts of interest if the subject of oversight is also the 'gate-keeper' for access to information by overseers. One can easily imagine that such provisions could be used to prevent overseers accessing information showing wrongdoing or with the potential to embarrass members of the executive branch.

4.2 INFORMATION RELATING TO OPERATIONS, SOURCES AND METHODS

It is relatively common for the law to deny oversight bodies access to information pertaining to sources and methods, and the operations of I&SS more generally (see Table 2, for an overview of some such restrictions in Europe).[67] Information pertaining

[65] Italy, Law 14/2007, Article 31(8).

[66] UK, Intelligence Services Act 1994, Schedule 3, Para 3(b)(ii).

[67] Australia, Intelligence Services Act 2001, Schedule 1 (part 1); UK, Intelligence Services Act 1994, Schedule 3, paras. 3–4.

to sources and methods relates to some of the most sensitive work of I&SS. With regard to sources, this is because they are concerned about their identities being exposed, with possible risks to the safety of the person concerned and to intelligence officers. Services' methods are highly sensitive because their exposure may serve to aid hostile I&SS or groups, undermine their effectiveness, and ultimately, compromise national security and public safety.

Restrictions on access to this type of information are sometimes formulated in general terms, as is the case in Australia, where the Parliamentary Joint Committee on Intelligence and Security: "must not require a person or body to disclose to the Committee operationally sensitive information […]."[68] Restrictions on access to information relating to ongoing operations can be particularly problematic given that some operations may last for many years and it can be very difficult to determine when an operation has been completed. This may place overseers' access to information at the mercy of I&SS assessments about the status of an operation and could potentially mean that certain activities remain impervious to oversight.[69] Furthermore, the distinction between 'policy' (information about which may be available to overseers) and 'operations', is not always evident.[70] Thus, overseers may once again be placed at the mercy of agency and/or executive discretion.

In view of this, laws in many states explicitly bar overseers from accessing information relating to the sources and/or methods.[71] Such legal provisions are, of course, premised on assumption that overseers cannot be fully trusted with the most sensitive information. It is our view, however, that this assumption is often unfounded. Indeed, there are few examples of overseers leaking sensitive information, particularly when

[68] Australia, Intelligence Services Act 2001, Schedule 1 (part 1); see also: France, Ordonnance n°58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, Article 6 nonies, Créé par Loi n°2007-1443 du 9 octobre 2007 - art. 1 JORF 10 octobre 2007 – alinéa III

[69] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 124.

[70] See, for example, the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981 [MacDonald Commission] 'Second Report' which discusses the 'policy of operations'.

[71] See, for example: Hungary, Act No. CXXV of 1995, Section 16(1) and Article 31(8); Italy, Law 14/2007, Article 31(8); Spain, Ley 11/2002, Article 11.2; UK, Intelligence Services Act 1994, Schedule 3, paras. 3–4; and De With and Kathmann, Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

compared to the number of leaks originating from within the executive or I&SS themselves.

4.3 INFORMATION RELATING TO JUDICIAL PROCEEDINGS OR CRIMINAL INVESTIGATIONS

In some states, the law bars oversight bodies from accessing information which relates to ongoing judicial proceedings or criminal investigations.[72] These restrictions are sometimes applied in order to safeguard both the right to a fair trial and the state's ability to investigate and prosecute crime. Such provisions may be designed to prevent oversight bodies from examining matters that are subject to criminal or judicial investigations until these investigations have been completed. However, there are oversight bodies whose mandates may require them to examine incidents or issues in parallel to an ongoing criminal or judicial investigation. This is particularly true of oversight bodies that oversee agencies with coercive powers. Evidently, this raises extremely complex issues relating, for example, to access to and the control of (potential) crime scenes and evidence. A full exploration of this issue is, however, beyond the scope of this paper.

4.4 FOREIGN INFORMATION

In recent years, information sharing between I&SS and foreign bodies has been a subject of significant interest to overseers and the media. Information sharing with foreign bodies has become an integral part of agencies' work and there has been an exponential increase in both the breadth (the range of agencies involved) and depth (the amount and level of information shared) of sharing. An inevitable consequence of this is that an increasing amount of information held by I&SS is of foreign provenance.[73] Equally, a significant number of their operations have a nexus with foreign partners.

---

[72] For example, the Swedish Commission on Security and Integrity Protection (SAKINT), discussed in Iain Cameron, Annex to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*); Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 48(2).

[73] See, for example: Alasdair Roberts, "ORCON Creep: Information Sharing and the Threat to Government Accountability," *Government Information Quarterly* 21, no.3 (2004), 263.

Information sharing is founded upon what is known as the third party rule. This means that the recipient cannot further disseminate information without the prior permission of the originating agency. This is designed to ensure that this agency retains control of the use of information.[74] Oversight bodies are often viewed as third parties. As a result, they are frequently barred or face major constraints on their access to information of foreign provenance.[75] Overseers could, of course, ask an I&SS to request permission from their foreign counterparts, which would allow them to access information (received from the foreign partner concerned). However, it is widely believed that I&SS are very reluctant to make such requests for fear of harming their reputations as "trusted recipients." While there is no data publicly available on how often such requests are made and/or whether they are successful, it is unlikely that many are made.[76]

Restrictions or absolute bars on overseers' access to the information that agencies receive from foreign entities can have profound implications for oversight.[77] This is particularly true given that some services may rely upon the third party rule to prevent overseers for accessing information about a particular matter.[78] Limitations on access to information of foreign provenance have created significant blind spots for overseers which can severely hinder the ability to oversee certain activities. Such blind spots are only likely to increase in line with the growing amount of information shared across borders and thus held by I&SS.

---

[74] Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified Information and Security Sensitive Information,* Report 98, Canberra, May 2004, 47; Aidan Wills and Hans Born, "International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions" in *Intelligence Cooperation and Accountability,* eds. Hans Born, Ian Leigh and Aidan Wills (London: Routledge, 2011), 283.

[75] For examples of legal provisions in this regard, please see: France, Ordonnance n°58-1100 - art. 1 JORF 10 octobre 2007 – alinéa III; Italy, Law 14/2007, Article 31(8); Spain, Ley 11/2002, Article 11.2; UK, Intelligence Services Act 1994, Schedule 3, paras. 3–4; Germany, Parliamentary Control Panel Act, Section 6. See also: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, "A new review mechanism for the RCMP's national security activities," Ottawa, 2006 (hereafter: the Arar Inquiry), 316.

[76] For an in-depth discussion of this issue see: Wills and Born, "International Intelligence Cooperation and Accountability."

[77] Alasdair Roberts, *Blacked Out: Government Secrecy in An Information Age* (Cambridge: CUP, 2006), 147; Wills and Born, "International Intelligence Cooperation and Accountability," 283-284 and 289-292; Sanchez, in Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[78] Wills and Born, "International Intelligence Cooperation and Accountability," 286-287.

It is noteworthy that some oversight bodies have asserted that their right to access information leaves no room for exceptions.[79] In addition, some argue that they are not third parties and thus, not subject to the rule.[80] Overseers do, nevertheless, exercise caution with regard to information from foreign services because they are mindful of the fact that I&SS are extremely sensitive about their relations with foreign entities.[81]

Regardless of whether national law places overseers in a position to assert a right to access foreign information, the third party rule should not be considered to be an absolute bar to access.[82] In jurisdictions where the executive/services may limit or bar overseers' access to foreign information, denials should be supported by a proper assessment of factors such as: the specific risks associated with sharing information with overseers; efforts made to secure a foreign governments permission to share information with overseers; whether or not some or all of the information has already been revealed in other forums, including by the media; as well as the extent to which the foreign partners were aware of the oversight context when sharing information with the service concerned. There should also be scope for judicial review, evaluating, among other things, the public interest served by information being disclosed to overseers versus the public interest in withholding such information.[83]

---

[79] See, for example, Verhoeven in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[80] See, for example, the comments of Van Laethem and Verhoeven both in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*

[81] See, for example: Wills and Born, "International Intelligence Cooperation and Accountability," 285–286 and 291; Van Laethem in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[82] This was the position taken by the German Constitutional Court in the case relating to the *Bundestag's* access to information in the context of a parliamentary inquiry into various activities of the Federal Intelligence Service BND; see German Federal Constitutional Court Press Office, *Press Release No. 84/2009* of 23 July 2009 (in English) pertaining to order of 17 June 2009 – BvE 3/07 (German only).

[83] See, by way of example, *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs*, 2010 EWCA, CIV 158, Case no. TI/2009/2331, para 29; see also, German Federal Constitutional Court Press Office, *Press Release No. 84/2009* of 23 July 2009 (in English) pertaining to order of 17 June 2009 – BvE 3/07 (German only).

4.5 JURISDICTION

The jurisdictional reach of oversight bodies can also constrain their access to information. Oversight bodies normally have either service-based or thematic mandates. In other words, they may have a mandate to oversee a specific I&SS (for example, Canada's Security Intelligence Review Committee [SIRC] vis-à-vis the Canadian Security Intelligence Service [CSIS] or the British Intelligence and Security Committee [ISC's] jurisdiction vis-à-vis the UK's three main I&SS), or a mandate to oversee, for example, all intelligence activities performed by government bodies. Service-based mandates usually imply that an overseer can only have detailed knowledge of and (potentially) full access to information from a particular I&SS. This can be problematic when they examine issues which are of a cross-cutting nature involving several agencies or departments. Examples of this may include cooperation between I&SS and law enforcement or the role of I&SS in immigration activities.[84] In such situations overseers may be "blinkered" and unable to properly examine the issue concerned. In view of this, thematic mandates are preferable because they are accompanied by broader access to information.[85]

Beyond the domestic context, oversight bodies are invariably limited by the fact that their authority to access information only extends to agencies and officials of their own state.[86] This can be an obstacle to oversight of various aspects of international cooperation between agencies. International intelligence cooperation, such as information sharing and joint-operations, leaves its mark in two or more states. However, oversight bodies only have legal authority to examine the role played by their own state's agencies. By way of example, they may be in a position to access information sent to a foreign entity but may have no access to information on requests made by the foreign entity, or indeed, the end use of information sent pursuant to such requests. Additionally, oversight bodies cannot compel foreign officials to provide them with information, and have generally been unsuccessful when asking for voluntary cooperation. This was, for example, the case with the Arar Inquiry in Canada and the German *Bundestag's* inquiry into to various activities of the German Federal Intelligence

[84] EOS Utvalget, *Annual Report 2008*, 41-45.

[85] CTIVD, *Annual Report 2008-2009*, 7.

[86] Wills and Born, "International Intelligence Cooperation and Accountability."

Service. As a result of these limitations, oversight bodies often have an incomplete view of activities involving their own state's agencies.[87]

4.6 PRACTICAL LIMITATIONS

Practical limitations may also have a significant impact on the ability of oversight bodies to access information and, in consequence, impair their ability to conduct oversight.

First, is the problem that overseers may not always know what they are looking for, or indeed what information even exists. Such gaps may relate to entire programmes or to specific details thereof. A similar obstacle, also relating to understanding, is the problem that arises when employees of I&SS do not understand the role of overseers. This can lead them to obstruct or hinder the work of oversight bodies (see section 2 for more details).

The second practical limitation on access to information is the sheer volume of information produced by I&SS, as well as the sometimes technical nature of this information. This may make it very difficult for oversight bodies to be able to identify what, if any, information is most relevant to their work. These related issues may require significant and specialised resources on the part of oversight bodies if they are to be overcome.

Third, limitations may be imposed by the way that information is recorded and stored by agencies. This may be a particular problem when oversight bodies are looking into older cases where records may have been lost or where record keeping standards may have changed. This was, for example, the case in the Norwegian EOS Utvalget Committee's investigation into the methods used by the Norwegian Police Surveillance Service in the 1980s Treholt case.[88] I&SS may have strong incentives to utilise informal and oral communications and transactions. An intelligence officer may be unlikely, for

[87] Andrea Wright, "Fit for Purpose? Accountability Challenges and Paradoxes of Domestic Inquiries," in *Intelligence Cooperation and Accountability,* eds. Hans Born, Ian Leigh and Aidan Wills (London: Routledge, 2011), 177–179.

[88] EOS Utvalget Committee, *Investigation into the Methods Used by the Norwegian Police Surveillance Service.* Special Report to the Storting (Norwegian Parliament), 2011, 23 and 25.

instance, to demand a receipt when paying a source or informant. Equally, there are circumstances in which they may not wish to establish a paper trail relating to certain activities, particularly overseas. Such practices may be motivated by a desire to cover up malpractice but can also be the result of legitimate security concerns. Nevertheless, proper record-keeping should be required and national law should be strict on the need for agencies to refrain from deleting information without proper supervision. In the case of *Charkaoui v. Canada*, for example, the Supreme Court of Canada ruled that the Canadian Security and Intelligence Service (CSIS) had a duty to retain operational notes and that their destruction has serious implications from the point of view of both human rights and accountability.[89] It is axiomatic that overseers cannot access information which was never recorded or was destroyed (for example, information from face-to-face discussions, telephone calls or notes taken by a field officer).

Finally, overseers face major challenges in accessing information which is located remotely (for example, in overseas liaison offices or stations). Even in cases where they have the power to inspect remote sites, oversight bodies may lack the time and resources that such inspections require. I&SS may also be extremely reluctant to permit overseers to visit overseas sites, given that such visits may draw attention to the presence of undercover operatives.

4.7 SELF-IMPOSED LIMITATIONS

Notwithstanding their possession of the requisite legal powers and resources to access information, oversight bodies may nevertheless abstain from doing so. There are a number of reasons why this may occur. First, many overseers are acutely aware of the need to maintain good relations and mutual trust with I&SS, in part because this can help to facilitate the flow of information. This may lead them to abstain from examining activities and thus seeking access to information on matters which they know to be particularly sensitive. Relations with foreign I&SS, sources and methods are examples of matters which may fall into this category.

[89] *Charkaoui v. Canada* (Citizenship and Immigration), [2008] 2 S.C.R. 326, 2008 SCC 38, para. 64.

Second, in parliamentary committees in particular, oversight can be politicised. This means that members of oversight committees from governing parties may seek to use their position to protect their colleagues in government and/or the directors of services who may have links with their party. Accordingly, they may use their majority to prevent the examination of issues that may be embarrassing or show wrongdoing.[90]

[90] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 88-89.

TABLE 2: THE EXTENT OF SELECTED PARLIAMENTARY AND NON-PARLIAMENTARY OVERSIGHT BODIES' ACCESS TO INFORMATION RELATING TO SECURITY AND INTELLIGENCE SERVICES IN EUROPE[91]

STATE	Future operations	Ongoing operations	Completed operations	Ministerial instructions/ directives issued to agencies	Budget and projected expenditure of agencies	Past expenditure	Agreements with foreign governments, agencies, and international organizations	Information received from other domestic agencies	Information received from foreign governments and security agencies	Information received from international organizations (e.g. the UN, EU or NATO)
Belgium - *Standing Intelligence Agencies Review Committee*	Unlimited	Unlimited	Unlimited	Restricted	Unlimited	Unlimited	Unlimited	Restricted	Unlimited	Unlimited
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	Restricted	Restricted	Restricted	Restricted	No	No	No	No	No	No
Estonia - *Security Authorities Surveillance Select Committee*	Unlimited	Restricted	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Restricted	Restricted
Finland - *The Administration Committee*	Restricted	Restricted	Restricted	Unlimited	Restricted	Restricted	Restricted	Restricted	No	Restricted
Germany - *Parliamentary Control Panel (PKGr)*	Restricted	Restricted	Restricted	Restricted	Unlimited	Restricted	Restricted	Restricted	Restricted	Restricted
Germany - *G10 Commission*	Restricted	Restricted	Restricted	Restricted	No	No	Restricted	Restricted	Restricted	Restricted
Greece – *Authority for Communication Security and Privacy (ADAE)*	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted
Hungary - *Committee on National Security*	No	No	Unlimited	Unlimited	Unlimited	Unlimited	No	Unlimited	Unlimited	Unlimited
Italy - *COPASIR*	No	No	Restricted	Unlimited	Unlimited	Restricted	No	(information not provided)	No	No
Latvia - *National Security Committee*	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Lithuania - *Committee on National Security and Defence*	No	Restricted	Restricted	Restricted	Unlimited	Unlimited	Restricted	Restricted	No	Restricted

[91] Adapted from Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 127-128.

The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	Unlimited	Unlimited	Unlimited	Unlimited	Restricted	Restricted	Unlimited	Unlimited	Unlimited	Unlimited
Poland (Sejm) - *Special Services Oversight Committee*	Restricted	Restricted	Restricted	Restricted	Unlimited	Unlimited	Restricted	Restricted	Restricted	Restricted
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	No	Unlimited	Unlimited	N/A	Unlimited	Unlimited	No	Unlimited	No	No
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	Restricted	Restricted	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Slovakia - *Committees for the oversight of the Slovak Information Service, and for the oversight of the National Security Authority of Slovak Republic*	No	No	No	(Information not provided)	Unlimited	Unlimited	No	No	No	No
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	No	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	No	No
Sweden - *The Commission on Security and Integrity Protection*	Restricted	Restricted	Restricted	Unlimited	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted
The UK - *Intelligence and Security Committee (ISC)*	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted

5. PROTECTION OF INFORMATION BY OVERSIGHT BODIES

The nature of I&SS (and other 'security sector organisations', i.e., the police, armed forces, border management agencies) work means that certain information about their activities must be classified (or otherwise restricted) and protected from disclosure to persons without proper authorisation to receive it.

Anyone who has privileged access to information from or pertaining to I&SS has a duty to ensure that they use it for lawful purposes. This obviously includes ensuring that information is not disclosed (without proper authorisation or legal basis) to persons who are not authorised to receive it. This duty is incumbent upon not only employees of I&SS and the executive branch, but also upon members and staffers of oversight bodies. It is worth noting here that the authors are not aware of any examples of oversight bodies being responsible for significant leaks of classified information. Indeed, it is our understanding that, in many jurisdictions, members of I&SS and the executive branch are responsible for far more leaks. In our experience, members and staffers of oversight bodies take their responsibilities to protect information extremely seriously.

Oversight bodies' access to classified information and, ultimately, their capacity to conduct oversight is often dependent upon their ability to demonstrate that they can protect information they have access to.[92] This helps to win the trust of the bodies they oversee and thus, to lubricate the flow of information. If overseers can demonstrate their capacity to protect classified information, this serves to undermine attempts by the executive branch (or I&SS) to invoke concerns about information security to deny overseers access to information. By contrast, failures to protect classified information can result in I&SS or the executive hindering or even blocking the future flow of information to oversight bodies.

[92] The Arar Inquiry, 425-426.

As we have argued throughout this paper, the law should empower oversight bodies to access all information, regardless of its level of classification, which they deem necessary for the fulfilment of their mandate. In view of this, withholding certain information from overseers is not a legitimate strategy for protecting information and, in many states discussed in this paper, it is unlawful. Taking this as the point of departure, the challenge is to devise safeguards which can reduce – to the greatest extent possible – the risk of accidental or deliberate disclosure of classified information by members and staffers of oversight bodies. In many ways the rules and procedures used by oversight bodies mirror those used by I&SS and the executive branch. The principal difference with regards to oversight bodies is that such rules and procedures cannot: (a) infringe upon their independence; (b) undermine the effectiveness of oversight processes, or (c) unnecessarily impinge upon the minimum level of transparency, for example, in reporting on their work, which underpins public confidence in oversight processes.

We must remain mindful of the axiom that no system of rules and procedures can fully prevent the unauthorised disclosure of information by overseers or any other persons with privileged access. There are however, three main ways that states seek to reduce the risk of unauthorised leaks by overseers. Firstly, there are procedures which help ensure that only persons who can be trusted with classified information are appointed or elected to oversight bodies. Secondly, criminal and other penalties are used to deter persons from disclosing information and to sanction those who do. Finally, overseers take various measures to ensure the physical security of information. Each of these methods is discussed in turn.

5.1 ENSURING APPROPRIATE PERSONS ARE GIVEN ACCESS TO CLASSIFIED INFORMATION

5.1.1 VETTING AND SECURITY CLEARANCES

Vetting and the issuing of security clearances are widely viewed as one of the foundations of policies to prevent the unauthorised disclosure of information (See Table 3 for an

overview of clearance requirements in selected I&SS oversight bodies). Vetting processes are essentially risk assessments which evaluate whether or not a given person has anything in their private or professional lives which could make them vulnerable to blackmail or financial incentives to disclose information. Vetting is also intended to detect whether the person has links to foreign states, organised criminal groups, terrorist organisations, or groups committed to sedition or subversion. Such links are usually deemed to render a person unsuitable for access to classified information due to the risk that they may pass it on to these actors. Vetting is usually carried out by an I&SS, or the police. A security clearance is then issued or denied on the basis of this assessment. The clearance may be issued or adjudicated by the same the body that conducted the vetting or by another body.

It is good practice for the oversight body itself to decide whether or not, on the basis of the vetting report (risk assessment), someone should be given a security clearance. This is, for example, the case with the Hungarian parliament's National Security Committee, which takes the final decision on whether an MP should be granted clearance and appointed.[93] Such practices help to safeguard the independence of an oversight body and they prevent the executive or security sector organisations from using vetting and clearance processes to control the membership of oversight bodies. Another practice which can be beneficial in this regard, is that of ensuring that overseers are vetted by a different agency than the one they have a mandate to oversee. For instance, a branch of the police could be tasked with vetting overseers with jurisdiction over I&SS. Although this alternative may not be feasible in the case of oversight bodies which have very broad, security-sector wide mandates, it should be attempted wherever possible. Needless to say, it is undesirable for the overseen body, for example, an I&SS, to gather information (necessary for vetting processes) on a

[93] Hungary, Act No. CXXV of 1995, Section 19. See also Földvary, in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*.

person who is likely to become their overseer, let alone for them to be in a position to effectively veto the appointment of would-be overseers.[94]

The arguments in favour of subjecting would-be members and staffers of oversight bodies to vetting and security clearance processes can be summarised as follows. First, overseers should be subject to the same preconditions as employees of the executive branch, I&SS and other security sector organisations before being allowed access to classified information. Second, vetting is meant to filter out persons who cannot be relied upon to maintain the confidentiality of information. Finally, requiring overseers to have security clearance is often viewed as crucial to winning the trust of I&SS and other 'overseen' entities. [95]

Recent research has illustrated that there is considerable divergence between parliamentary and non-parliamentary oversight bodies regarding whether or not members require security clearance (see Table 3 below).[96] The overwhelming majority of European Union member states do not require members of parliamentary oversight committees to have security *clearance*. This is also the case in the Argentine National Congress, the Australian Parliament and the US Congress. Exceptions to this rule are mainly found in post-authoritarian states of Central and Eastern Europe (for example, Estonia, Hungary, Kosovo, Lithuania, Macedonia and Poland). This can perhaps be explained by the fact that, in many such states, legislation regulating parliamentary oversight was passed at a time when levels of trust in politicians were very low. The fact that some of these states had (and still have) highly polarised political spectrums, with parties from the extreme right and left (sometimes linked to subversive or seditious activity), further explains

[94] See, for example, Frederick M. Kaiser, *Protection of Classified Information by Congress: Practices and Proposals* (Washington DC : CRS, 2010).

[95] Stuart Farson, "Establishing Effective Oversight Institutions," (Working Title), Tool 2, eds., Hans Born and Aidan Wills (forthcoming).

[96] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 137-141.

requirements for security clearance of parliamentarians in these states.[97] It is noteworthy that Croatian law initially required members of the parliamentary Committee on National Security to have security clearance but this requirement was later dropped. It was, apparently, no longer deemed necessary as Croatian democracy matured. This is illustrative of the fact that vetting and clearance requirements may need to be adapted to the context and prevailing inter-institutional relations. Regardless of the approach taken, it is important that parliament decides (ideally through legislation) whether or not members of parliamentary oversight committees should be vetted.

That most states do not require parliamentarians (with access to classified information) to be security cleared can be largely explained by the fact that vetting parliamentarians is considered to be a violation of the principle of the separation of powers.[98] The independence of parliament may be seriously undermined if the executive branch is in a position to adjudicate on whether parliamentarians should receive security clearance and thus, be appointed to an oversight role. Additionally, it may be viewed as unacceptable for an executive branch agency to delve into the private affairs and past activities of democratically elected representatives. Such concerns are heightened in contexts where there is a risk that information derived from vetting processes may be used for political purposes, e.g., to smear political opponents. Finally, it is worth noting that some states, for example, France and the US, consider parliamentarians to be security cleared by virtue of being elected.[99]

In contrast to parliamentary oversight bodies, members of non-parliamentary oversight bodies (or their units responsible for overseeing I&SS) such as supreme audit institutions,

---

[97] See, for example, Florian Qehaja, "Kosovo," (Chapter 3) in *Intelligence Governance in the Western Balkans,* eds., Hans Born, Miroslav Hadžić and Aidan Wills (forthcoming).

[98] See, for example, Verhoeven in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*; Stuart Farson, "Establishing Effective Oversight Institutions," 35; Frederick M. Kaiser, *Protection of Classified Information by Congress: Practices and Proposals* (Washington DC : CRS, 2010), 5.

[99] See Martin and Lepri, Annexes to Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*,

expert intelligence oversight bodies and data protection commissions, are normally required to have security clearance.[100] Exceptions to this general rule are sometimes found with regards to judicial oversight bodies (for example, the UK's Investigatory Powers Tribunal), positions occupied by members of the judiciary (for example, the UK's Intelligence Commissioner) and ombuds institutions (for example, the Protector of Citizens in Serbia). Finally, while practices regarding the vetting and security clearance of members of oversight bodies vary, it is an almost universal requirement for staffers of both parliamentary and non-parliamentary oversight bodies to receive security clearance before being appointed.

It is noteworthy that the fact that security clearances are not required for members of some oversight bodies does not necessarily preclude them from applying for one. We are aware of several cases where senior overseers have voluntarily subjected themselves to vetting processes. They have done so in the belief that obtaining security clearance serves as a confidence building measure vis-à-vis the security sector organisations they oversee, and that this can help promote trust in their office and facilitate access to classified information. Research by the Venice Commission is instructive in this regard: it found that oversight bodies whose members are subject to security clearance receive better access to information.[101]

5.1.2 SELECTION AND ELECTION PROCESSES

Selection and election processes are another means through which to ensure that only persons who can be trusted with classified information are appointed to oversight bodies. Appointments processes vary greatly between jurisdictions and between oversight bodies but it is good practice for a range of actors to be involved in such decisions. This helps to ensure the appointment of persons of appropriate integrity, impartiality and expertise. Members of non-parliamentary oversight bodies are sometimes appointed after inputs

[100] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 140-141.

[101] Venice Commission Report 2007, 49.

from all three branches of the state. This is, for example, the case with the Dutch Review Committee on the Intelligence and Security Services. A panel including senior members of the judiciary makes initial recommendations, parliament must then approve the candidates or propose alternatives and the final approval is given by the executive branch.[102]

More commonly, overseers (both parliamentary and non-parliamentary) are appointed by parliament alone (often by a simple majority). This is, for example, the case in Germany, where members (parliamentarians) of the Parliamentary Control Panel (an I&SS oversight body) can only be appointed if they receive the support of a Chancellor's Majority of all members of the *Bundestag* (including those not present in the chamber). There is, nevertheless, agreement between the parties that they should be represented in proportion to their overall number of seats in the chamber, meaning that no party is currently excluded. Similarly, in Spain, members of the Secret Funds Committee of the Spanish *Cortes* (a committee which, despite its name, performs several I&SS oversight functions) are selected from each party but they must receive the backing of 60 percent of all members. This is partly designed as a measure to prevent a political party allied to a violent extremist group from accessing classified information.[103] While the majority of parliament is unlikely to be privy to information that might be uncovered through a vetting process, it is also unlikely to appoint someone who is known to be unreliable or untrustworthy. Finally, when the executive appoints members of oversight bodies, it can be reasonably assumed they will not select anyone who is seen to be a security risk with regards to the handling of information.[104]

---

[102] See Verhoeven in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[103] Sanchez Ferro in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[104] See Leigh in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*.

5.2 SANCTIONS FOR UNAUTHORISED DISCLOSURES

A second tool commonly used to protect classified information handled by oversight bodies is the availability and enforcement of sanctions for persons who make unauthorised disclosures. Criminal and/or administrative sanctions are designed to deter members and staffers of oversight bodies from disclosing classified information without proper authorisation. Such sanctions often apply to these persons in the same way as they apply to executive branch employees and I&SS personnel.[105] While such sanctions do exist, we are not aware of any recent examples of members of oversight bodies being prosecuted for the misuse of classified information. Furthermore, it is worth underlining at the outset that such sanctions should in no way interfere with the ability of those with access to classified information to make protected disclosures under a whistleblower protection regime.[106]

With regards to criminal sanctions for the unauthorised disclosure of classified information, there are major differences between parliamentary and non-parliamentary oversight bodies and between members and staffers of oversight bodies. Staffers of all types of oversight body can ordinarily be prosecuted for unauthorised disclosures of classified information. The status of members is more complex. Members of most non-parliamentary overseers (such as supreme audit institutions, expert I&SS oversight bodies, data protection commissions) may ordinarily be prosecuted for such disclosures. It should nevertheless be noted that prosecutions under official secrecy legislation are often at the discretion of the attorney general (or equivalent office-holder), and prosecuting a member of an independent oversight body, such as an auditor general, would likely raise many complex political considerations, particularly regarding the separation of powers and the independence of oversight bodies. The prosecution of parliamentarians is even more vexed and state practices vary significantly.

---

[105] See Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 142; See by way of example: Australia, Intelligence Services Act 2001, Schedule 1, part 2, (9, 10, 12) and Italy, Law 14/2007, Article 36; Germany, G10 Act, Sections 17–18; UK, Intelligence Service Act 1994, Section 11(2).

[106] See, in this regard, Buckland and Wills, *Blowing in the Wind: Whistleblowing in the Security Sector,* 2012.

In some jurisdictions, for example, the US, members of Congress cannot be prosecuted for disclosures of classified information during parliamentary proceedings because these are covered by the so-called parliamentary privilege. They may however, be prosecuted if disclosures are made outside such proceedings, notably, to the media directly.[107] In other jurisdictions, parliamentarians may also be prosecuted if parliament has explicitly abrogated the parliamentary privilege through primary legislation. Elsewhere, parliamentarians may be prosecuted for unauthorised disclosures of information regardless of the context in which they are made. Prosecutions may, however, be dependent upon parliament waiving an MP's immunity from prosecution; this is the case, for example, in both Germany and Poland.[108]

Prosecuting parliamentarians for the unauthorised disclosure of information is likely to be highly contentious. Notably, concerns may be raised about parliamentarians' right to free speech, as well as the parliamentary privilege which ordinarily provides immunity for anything which is said in the context of parliamentary proceedings. Furthermore, there are indications, from the US Congress, that the threat of sanctions for disclosing classified information can have a chilling effect on parliamentary proceedings and oversight functions in particular. Some members of Congress have apparently abstained from viewing classified information for fear of inadvertently disclosing such information.[109]

Short of criminal proceedings, there are a number of other sanctions which may be applied to overseers who disclose classified information without authorisation. First, parliamentary and non-parliamentary oversight bodies may vote to revoke or suspend the membership of the person concerned, perhaps pending a full investigation.[110] This is likely

---

[107] Kate Martin in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

[108] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 142.

[109] Susan Milligan, "Classified Intelligence Bills Often Are Unread: Secret Process Can Discourage House Debate," *Boston Globe*, 6 August 2006.

[110] This is, for example, the case in Spain under the Spanish *Cortes'* Rules of Procedure (see Sanchez, in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*). See also Fabbrini

to be essential in order for the oversight body to retain credibility vis-à-vis the entities it oversees. Second, the oversight body may suspend or annul the person's security clearance, meaning that they no longer have access to classified information and cannot continue to fulfil their functions.[111] Third, some parliaments, such as the Spanish *Cortes*, can effectively fine parliamentarians by withholding their allowances for breaches of rules of procedure, including the unauthorised disclosure of classified information.[112] Lastly, some parliaments, such as the Lithuanian *Seimas*, may impeach parliamentarians for the unauthorised disclosure of classified information.[113]

With all disciplinary options it is preferable for the parliament or oversight body itself to be take charge of initial investigations into security breaches, as well as to retain the power to decide what course of action to take.[114] This also applies to the question of immunity from prosecution discussed above; parliament alone should have the power to waive such immunity. Granting oversight bodies such autonomy guards against the executive (mis)using (potentially false) allegations and investigations relating to the use of information in order to suspend or remove overseers for other reasons, for example, because they are seen to be critical of the incumbent government.

5.3 PHYSICAL PROTECTION MEASURES

Finally, it is worth briefly touching on the principal mechanisms which overseers use to physically protect classified information. First among these is the use of *in camera* meetings in cases where discussions involve classified information or where employees of I&SS

---

and Giupponi, Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, on the Italian parliament's COSAPIR; and Van Laethem on the Belgian Committee I (in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*).

[111] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 142.

[112] See Susana Sanchez Ferro in Annex A of Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*.

[113] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 142.

[114] See, for example, the role of the US Congressional Ethics Committees in investigating security breaches; Frederick M. Kaiser, *Protection of Classified Information by Congress: Practices and Proposals* (Washington DC: CRS, 2010).

(whose identities must be kept secret) may be required to testify. Such meetings exclude both members of the public, as well as non-members of relevant parliamentary committees. While acknowledging that *in camera* meetings may be the norm, parliamentary oversight bodies, in particular, should endeavour to hold open meetings wherever possible given the importance of transparency and the need for parliamentarians to remain accountable to the public for their work in parliament.

The intelligence committees of the US Congress provide an instructive example. Meetings of these bodies are always open unless classified matters are actually under discussion. Similarly, the UK government proposed in its 2011 Green Paper on Justice and Security that the Intelligence and Security Committee hold "public evidence sessions" wherever possible.[115] Regardless of the approach taken, if meetings are held *in camera* it is essential that public reports on investigations and proceedings are made available wherever possible.[116]

In addition to *in camera* meetings, oversight bodies use a range of standard practices and protocols regarding the protection of information technology and communications infrastructure, as well as physical documents and records. Notably, many parliaments have secure reading rooms for the viewing of classified material and some oversight bodies also have facilities on their own premises for storing and viewing classified information. Such facilities can help to ensure their autonomy as it negates the need for them to rely on facilities provided by the I&SS or the executive branch.

It is standard practice for security procedures and protocols to provide equivalent protection to information as those used within I&SS and the executive branch. Such procedures may be developed in concert with the I&SS.[117] As a confidence-building

---

[115] UK Government, *Justice and Security Green Paper,* CM 8194, 2011, 44.

[116] See Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 143.

[117] See, for example, the requirement in Australian law for the parliamentary oversight committee to consult with the security services in this regard. Australia, Intelligence Services Act 2001, Schedule 1 (part 3, 22).

measure, it may be advisable for oversight bodies to allow I&SS or other independent security experts to inspect their procedures and practices.

TABLE 3: SECURITY CLEARANCE REQUIREMENTS FOR SELECTED INTELLIGENCE OVERSIGHT BODIES WITH ACCESS TO CLASSIFIED INFORMATION[118]		
STATE & NAME OF OVERSIGHT BODY	**Type of Oversight Body**	**Security Clearance Required?**
Austria - *Standing Subcommittee of the Interior Affairs Committee*	Parliamentary	NO
Belgium - *Standing Intelligence Agencies Review Committee*	Non-parliamentary	YES
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	Parliamentary	NO
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*	Parliamentary	NO
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	Parliamentary	NO
Estonia - *Security Authorities Surveillance Select Committee*	Parliamentary	YES
Finland - *The Administration Committee*	Parliamentary	NO
Germany - *Parliamentary Control Panel (PKGr)*	Parliamentary	NO
Germany - *G10 Commission*	Non-parliamentary	YES (For members who are not MPs)
Greece – *Authority for Communication Security and Privacy (ADAE)*	Non-parliamentary	NO
Hungary - *Committee on National Security*	Parliamentary	YES
Italy – *COPASIR*	Parliamentary	NO
Latvia - *National Security Committee*	Parliamentary	YES

[118] Adapted from Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 140-141.

Lithuania - *Committee on National Security and Defence*	Parliamentary	YES
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	Non-parliamentary	YES
Poland (Sejm) - *Special Services Oversight Committee*	Parliamentary	YES
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	Non-parliamentary	NO
Romania – *The Committee for Defence, Public Order and National Security*	Parliamentary	NO
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	Parliamentary	NO
Slovakia - *Committees for the oversight of the Slovak Information Service* **-** *Committee for the oversight of the National Security Authority of Slovak Republic*	Parliamentary	NO
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	Parliamentary	NO
Sweden - *The Commission on Security and Integrity Protection*	Non-parliamentary	YES
The UK - *Intelligence and Security Committee (ISC)*	Non-parliamentary	NO

6. CONCLUSION

Access to information is essential in a democratic society. In particular, the ability of individuals and the media to access information about the workings and activities of government is a crucial tool for those who seek to hold those in power to account. It is understandable then that the OSF-JI Principles on National Security and the Right to Information should focus their attention, primarily, on access to information by individuals, civil society and the media.

We have argued here, however, that, as the principles acknowledge, there are some types of information that can legitimately be withheld from members of the public, including information that is classified or otherwise confidential (for example, for operational reasons or because it is protected by privacy law). As a consequence, there are a number of areas of state activity that are not transparent and open to public scrutiny. The national security domain is one such area. Yet, in a democratic society, it is clearly unacceptable that areas of government activity exist that are shielded from independent scrutiny and review. It is here that oversight bodies – including, among others, parliamentary and non-parliamentary specialised oversight bodies – play a crucial role. Through its elected representatives, the public delegates the task of accessing relevant information and scrutinising government activity to such bodies. It is their role to ensure that, among other things, the I&SS, conduct their operations in accordance with the law.

This paper has used the example of I&SS oversight bodies to demonstrate the importance of independent overseers having access to all information they deem to be necessary, as well as recourse to the powers and resources they require to access and process such information. It is hoped that the discussion above both informs and supports the relevant sections of the OS-JI Principles by offering examples and suggestions of good practice from the national laws and experiences that informed the initial drafting process.