GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF ARMED FORCES

MONITORING SECURITY SERVICES

A GUIDE FOR OMBUDS INSTITUTIONS

Nazli Yildirim Schierkolk

Materials for Georgia

DCAF
a centre for security, development and the rule of law

Monitoring Security Services: A Guide for Ombuds Institutions

Nazli Yildirim Schierkolk

Materials for Georgia

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is an international foundation whose mission is to assist the international community in pursuing good governance and reform of the security sector. The Centre develops and promotes norms and standards, conducts tailored policy research, identifies good practices and recommendations to promote democratic security sector governance, and provides in-country support and practical assistance programmes.

Published by DCAF
2E, Chemin Eugene-Rigot
P.O Box 1360
CH – 1211 Geneva 1
www.dcaf.ch

Author: Nazli Yildirim Schierkolk
Series Editor: Eden Cole
Copy Editor: Richard Steyne
Design: Karina Priajina
Cover photograph: by Jamie McCaffrey on Flickr, CC BY-NC licence

The author and DCAF would like to thank the Public Defender of Georgia, Ucha Nanuashvili, and the staff of the Public Defender's Office for their cooperation on monitoring issues and the opportunity to cooperate on this project. Additionally, the author and DCAF would like to thank Benjamin Buckland, of the Association for the Prevention of Torture (APT), and Graziella Pavone, OSCE ODIHR, for their extended comments on this paper.

While the internet references cited herein were valid as of the date of publication, neither DCAF nor the author can attest to their current validity.

ISBN: 92-9222-445-X

Suggested Citation:

Nazli Yildirim Schierkolk, 'Monitoring Security Services: A Guide for Ombuds Institutions' *Materials for Georgia* (DCAF: 2017)

Monitoring Products for NHRIs Series

National human rights institutions (NHRI)—also known as ombuds institutions—have a crucial role to play in monitoring the security sector and holding the security sector accountable for its practices. NHRIs are also well placed to interact with other stakeholders to help facilitate broader security sector oversight and can ensure the development and maintenance of human rights-observant security policies and practices.

DCAF programming with NHRIs in Ukraine and Georgia focuses on a variety of human rights and security sector governance challenges and the need for guidance materials on monitoring law enforcement and state security services has been noted for some time.

This Series of Monitoring Products is designed to facilitate the work of National Human Rights (Ombuds) Institutions on monitoring the security sector. The series provides guidance on relevant best practices and may also be used for relevant capacity development trainings.

DCAF has also developed a number of products to assist Ombuds institutions on both broad and highly specific oversight and policy challenges, particularly in terms of gender equality and human rights monitoring within the armed forces. For more information please see: http://www.dcaf.ch/ombuds-institutions

Table of Contents

Introduction

Project background

This guide was produced as part of a project initiated by the Geneva Centre for the Democratic Control of Armed Forces (DCAF). The objective of the project is to develop knowledge products on overseeing security services, to be used in training activities for the Office of the Public Defender of Georgia (PDO).

The content of this guide may also serve as a basis for capacity building activities for other ombuds institutions operating in similar contexts.

A note on terminology

Security services

The label 'security services' is defined herein as 'state bodies, including both autonomous agencies and departments/units of other government that have a mandate to collect, analyze and disseminate intelligence within the borders of their state in order to inform decisions by policy makers, police investigators and border/customs agencies about threats to national security and other core national interests.'[1] For the purposes of this guide, the term does not cover agencies collecting and analysing foreign intelligence.

[1] Council of Europe*, Democratic and Effective Oversight of National Security*

Oversight

The term oversight is frequently used in this guide, and it is therefore important that it is clearly defined from the outset. Oversight is a comprehensive term that refers to several processes including: ex-ante scrutiny, on-going monitoring, and ex-post review, as well as evaluation and investigation. Oversight of security services is undertaken by a number of external actors, including the judiciary, parliament, National Human Rights Institutions (NHRI) and ombuds institutions, National Preventive Mechanisms (NPM), audit institutions, specialised oversight bodies, media and NGOs. Oversight should be distinguished from control as the latter implies the power to direct policies and activities. As such, control is typically associated with the executive branch of government.[2]

Ombuds institutions

An ombuds institution is defined as 'an office established by constitution or statute, headed by an independent high-level public official who receives complaints about human rights violations and maladministration against government agencies, officials, employees

---

Services, (2015), p. 18, available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

[2] Hans Born and Geisler Mesevage, 'Introducing Intelligence Oversight' in Born and Wills (ed.) *Overseeing Intelligence Services: A Toolkit,* (DCAF: 2012), p. 6, available from: http://www.dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf

or who acts on his/her own initiative on the basis of information from a wide range of sources'.[3] An ombuds institution has powers to, inter alia, investigate, criticise, and provide recommendations for relevant authorities, as well as to propose new laws or amendments to existing legislation. In some countries, ombuds institutions may have other titles such as 'public defender' or 'protector of citizens'. This guide will use the term 'ombuds institutions', except for examples of national best practices, where the full title of the institution is provided.

Monitoring security services—the need for external oversight

Security services are typically tasked with collecting, analysing and disseminating information related to national security threats. In doing so, they are entrusted with exceptional powers, such as employing covert surveillance methods and collecting, using and exchanging personal data. Such powers, if misused, can violate fundamental human rights; including the right to liberty and security, the right to privacy, as well as the right to freedom of expression.

In democratic societies, security services are subjected to control and oversight by various mechanisms. While the executive develops relevant policies and priorities, and directs and controls the services; the senior management of security services is responsible for ensuring compliance with policies, laws, and regulations. However, as stated by the Venice Commission, executive and internal control is

[3] The Parliamentary Ombudsman of Malta, *Frequently Asked Questions*, (2014), available from: http://www.ombudsman.org.mt/how-can-one-define-the-ombudsman-institution/

never sufficient, since security services have a tendency to 'over-collect' information:

> 'Unless external limits are imposed, and continually re-imposed, then the natural tendency on all agencies is to over-collect information. Internal limits will not suffice because, while the staff of a security agency should set limits on the collection of data, it is not primarily their job to limit themselves and think about the damage which over-collection of intelligence can do to the vital values of democratic societies...'[4]

Over-collecting information is just one example of the ways in which security services can abuse their powers and violate fundamental human rights. Unlawful storage and exchange of personal data with foreign security services, incommunicado detention and extraordinary rendition are among the other serious human rights violations which may be committed by security services when their activities are not strictly regulated, controlled and overseen. It is therefore essential to ensure effective external oversight of security services. While various actors with different mandates exercise such oversight, it is the judiciary who authorises the use of special powers and adjudicates cases relating to the activities of security services. The parliament adopts, reviews and amends the legal framework for the services and their oversight, reviews and approves their budgets,

[4] Venice Commission, *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session,* (2007), para 58, available from: http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

and oversees their activities through parliamentary or specialised expert committees. Ombuds institutions handle individual complaints against services, launch own-motion investigations or those based on complaints, and initiate thematic investigations into the activities of the services. Finally, civil society and media can expose misconduct on the part of services, and contribute to an informed public debate about policies concerning the security services.[5] It should be noted that these are rather generic descriptions of the role of the aforementioned institutions. Their exact mandate and powers differ in each country.

While each external oversight actor has an important role in the accountability system, this guide primarily focuses on the role of ombuds institutions in overseeing domestic security services. Wherever necessary, reference is also made to specialised oversight bodies, as they often embody best practice and in some cases their work is comparable to that of ombuds institutions, particularly with respect to complaints handling and the conducting of thematic and other investigations.

[5] Hans Born and Geisler Mesevage, 'Introducing Intelligence Oversight' in Born and Wills (ed.) *Overseeing Intelligence Services: A Toolkit,* (DCAF: 2012), p. 8.

The structure and content of the guide

This guide consists of three chapters.

Chapter 1—International Standards on Overseeing Security Services presents an overview of the key instruments and court jurisprudences which provide the legal and normative basis for overseeing security services.

Chapter 2—Key Features for Effective Oversight of Security Services addresses the essential elements of an effective oversight system, namely, independence, resources, mandates, powers, reporting and transparency; as well as what these entail for ombuds institutions.

Chapter 3—Key Areas of Intelligence Oversight: Best Practices focuses on the role of ombuds institutions in monitoring security services and provides an overview of international and European best practices in the following areas:

- Overseeing covert information collection;
- Overseeing the use of personal data; and
- Overseeing information sharing.

In each chapter, the substantive content is followed by a section on its relevance for Georgia, and concludes with a section whereby key reference material on the subject matter is listed.

Chapter 1: International and European Standards on Overseeing Security Services

1. International Standards

International Covenant on Civil and Political Rights

Currently, no international legal instrument deals exclusively with the oversight of security services. However, **the International Covenant on Civil and Political Rights (ICCPR)**, amongst other instruments, lays out the fundamental rights and legal standards that security services should respect. One of the main objectives of oversight is to ensure that state institutions and their agents act in accordance with the law and do not unlawfully infringe upon human rights. The rights that are stipulated in the ICCPR and most relevant in this context are the right to life (Art. 6), the right to liberty and security of person (Art. 9), the right to privacy (Art. 17), the right to freedom of expression (Art.19), and the right to an effective remedy (Art. 2).[6]

Ombuds institutions with a mandate to oversee security services facilitate state efforts to provide effective remedy. While most ombuds institutions are not able to provide remedy themselves, the findings of their investigations and subsequent recommendations to

[6] *International Covenant on Civil and Political Rights*, (1976), UNGA RES 2200A(XXI), available from: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

authorities contribute to that purpose. Further, ombuds institutions are typically tasked with reviewing national legislation, proposing legislative amendments where necessary, monitoring security services, and initiating investigations into particular areas of activity. In this regard, overseeing security services' compliance with the standards stipulated in the ICCPR (for instance, those relating to the right to privacy) forms an indispensable part of ombuds institutions' thematic investigations.

Paris Principles

Over the last decades the international community has increasingly emphasised the need for independent oversight mechanisms for the protection and promotion of human rights. In 1993, the United Nations General Assembly adopted the **Principles relating to the Status of National Institutions (The Paris Principles).** The Principles are considered as the leading normative instrument for the mandate, powers, composition and scope of the work of national human rights institutions, which apply to many ombuds institutions.

The Paris Principles are of a general nature; that is to say that they are not customised for the oversight of any particular sector. Nevertheless they provide important guidance for the effective functioning of human rights institutions.

According to **the Paris Principles**, such institutions should:

- Be vested with a broad mandate;
- Be responsible to submit upon request or on the institution's own initiative, opinions, recommendations,

proposals and reports on any matters concerning the protection and promotion of human rights in relation to legislative, administrative, judicial provisions, or any situation in which human rights may have been violated;

- Have the mandate to draw the attention of the Government to situations in any part of the country where human rights are violated and to submit to the Government proposals for initiatives to put an end to such situations and, where necessary, express an opinion on the positions and reactions of the Government;
- Freely consider any questions falling within their competence, hear any person and obtain any information necessary to make an assessment of situations falling within their competence and publicise its opinions and recommendations.[7]

The last two points in particular can be considered as a basis of two central functions of ombuds institutions: conducting own-motion investigations, and accessing all information relevant for handling complaints. The principles underline the powers that are necessary for overseeing intelligence agencies; including access to information, hearing persons and conducting own-motion reviews of policies and practices falling under their mandate.

[7] *The Paris Principles*, Principles 1-3, available from: http://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx

United Nations Human Rights Council—Compilation of Good Practices

In 2009, the United Nations Human Rights Council mandated the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to develop a '**Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies'.** The compilation, which is comprised of thirty-five practices, is distilled from requirements of international law as well as existing and emerging practices from a wide range of States.[8]

Practices 6 and 7 of the compilation refer explicitly to external oversight mechanisms, emphasising their independence and powers, especially those relating to initiating own-motion investigations.

[8] Human Rights Council, *Compilation Of Good Practices On Legal And Institutional Frameworks And Measures That Ensure Respect For Human Rights By Intelligence Agencies While Countering Terrorism, Including On Their Oversight* (hereinafter*, UN Compilation of Good Practices*), A/HRC/14/46 para 14, available from: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

UN Compilation of Good Practices

Practice 6: Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is **independent of both the intelligence services and the executive**. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

Practice 7: Oversight institutions have the **power, resources and expertise to initiate and conduct their own investigations**, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.

It is important to note that Practice 7 also refers to the power to compel intelligence and law enforcement agencies' cooperation for hearing witnesses and obtaining documentation and evidence. This is an essential power required for ombuds institutions to effectively conduct investigations.

Practices 9 and 10 address the issue of complaint-handling and, in doing so, refer to the role and powers of ombuds institutions. The complaint handling function of ombuds institutions is discussed in more detail in Chapter 2.

UN Compilation of Good Practices

Practice 9: Any individual who believes that her or his rights have been infringed by an intelligence service is able to **bring a complaint to a court or oversight institution, such as an ombudsman**, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

Practice 10: The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services are **independent of the intelligence services and the political executive**. Such institutions have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

The UN Compilation of Good Practices includes several other standards relating to specific areas of security service activity. They can be accessed at: https://fas.org/irp/eprint/unhrc.pdf

Following the Compilation of Good Practices, UN bodies and special rapporteurs continued to emphasise the need for independent oversight of security services. In 2014, after the Snowden revelations, the UN Special Rapporteur on human rights and counter terrorism recommended that 'states using mass surveillance technology must establish strong independent oversight bodies that are adequately resourced and mandated to conduct ex ante review of the use of intrusive surveillance techniques against the requirements of legality, necessity and proportionality.'[9]

Besides the standards and practices recommended by the UN, two important civil society-led documents also contribute to the international normative framework on the oversight of security services: the Ottowa Principles and the Tshwane Principles.

Ottawa Principles

The **Ottawa Principles on Anti-Terrorism and Human Rights**, developed by subject matter experts in 2006, stress the need for an independent 'review body' to oversee the activities of security services. Ottawa Principles recommend that such a 'review body' should be empowered to:[10]

- Review and investigate, where and how it sees fit, the activities and policies of the agencies within its purview;

[9] Human Rights Council, *Report Of The Special Rapporteur On The Promotion And Protection Of Human Rights And Fundamental Freedoms While Countering Terrorism,* (23 September 2014), A/69/397, para 47.
[10] *The Ottawa Principles*, Principle 9.3, available from: http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf

- Compel any information, including all levels of secure information, from any person;
- Investigate and resolve complaints, including ensuring effective access, representations and remedies for complainants;
- Make reports of its findings and recommendations public; and
- Take all reasonable steps to protect the confidentiality of information that is subject to national security confidentiality.

Most national ombuds institutions do not have the expansive powers that the Ottawa Principles call for, especially with respect to conducting full and independent investigations of alleged violations committed by security service personnel, or ensuing remedy for complainants. Therefore, some North American and European countries have established separate, specialised oversight bodies focusing exclusively on intelligence oversight, and entrusted them with greater powers than ombuds institutions.

Tshwane Principles

The Global Principles on National Security and the Right to Information (The Tshwane Principles), were developed in consultation with 500 experts from seventy countries, and have been endorsed by PACE and the European Parliament.[11] The Principles

[11] PACE, *Parliamentary Assembly of the Council of Europe Resolution 1954* (2 October 2013); European Parliament 2014, *Report On The US NSA*

place particular emphasis on the access of independent oversight bodies to information, as stipulated in the following articles:

- 33 a) 'Independent oversight bodies should have adequate legal powers in order to be able to access and interpret any relevant information that they deem necessary to fulfil their mandates.
    - At a minimum, these powers should include the right to question current and former members of the executive branch and employees and contractors of public authorities, request and inspect relevant records, and inspect physical locations and facilities.
- 33 (c) […] Independent oversight bodies should have access to the necessary financial, technological, and human resources to enable them to identify, access, and analyze information that is relevant to the effective performance of their functions.'[12]

It is important to note that merely providing independent oversight bodies with access to information may not be sufficient for the realisation of this power. As stated in Tshwane Principle 33 (c), for an effective oversight system, such bodies should be supplied with the

---

Surveillance Programme, Surveillance Bodies In Various Member States And Their Impact On EU Citizens' Fundamental Rights And On Transatlantic Cooperation In Justice And Home Affairs, A7-0139/2014, (21 February 2014).

[12] *The Tshwane Principles*, Principle 33 (a) and (c), available from: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

necessary financial, technological, and human resources to enable them to identify, access, and analyse information.

While neither the UN Compilation of Good Practices, nor the Tshwane or Ottawa Principles are legally binding, they provide guidance and a solid framework for the independent oversight of security services, especially with regards to their mandates, powers and resources.

2. European Standards

At the European level, the **European Convention on Human Rights (ECHR)** is the most comprehensive legally binding instrument stipulating fundamental human rights and relevant state obligations to protect them. In contrast to the ICCPR, the articles of ECHR are interpreted by the European Court of Human Rights, whose rulings are legally binding on the States that are party to the Convention. In this context, the Court's jurisprudence has played a key role in the establishment of standards for the independent oversight of security services.

By way of example, in its judgement for the case ***Kennedy v. UK,*** the Court put forth a list of features that would enable an oversight body to effectively investigate complaints concerning intrusive surveillance. The Investigatory Powers Tribunal (IPT) of the UK is mandated to hear allegations by citizens of wrongful interference with their communications, and to investigate complaints accordingly. As part of the *Kennedy v. UK* case, the Court reviewed the safeguards against abuse within the surveillance system and

ruled that the IPT conducts a diligent review, and stated that there was no violation of the right to privacy. According to the Court, the factors that enabled IPTs diligent review were as follows:

- Being an independent and impartial body;
- Members of the tribunal having to hold or having previously held high-level judicial positions, or be experienced lawyers;
- Access to closed material, and the power to require the Commissioner to provide any assistance it sees fit and to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant;
- The power to quash any interception order, require the destruction of intercept material and order compensation to be paid.[13]

With this judgement, the Court established the power to quash an interception order and request the destruction of intercepted material as key factors for the diligent supervision of security services.

Apart from the aforementioned case, the Court has been pivotal in establishing standards on particular activities of the security services, such as the use of covert surveillance and the retention of personal data. These will be discussed in more detail in Chapter 2 of this guide.

Besides the Court, there are several institutions and actors in Europe that contribute to European soft-law on the oversight of security services. Most notable among these is the Council of Europe.

[13] *Kennedy v. the UK* (26839/05), para 167-169, available from: https://hudoc.echr.coe.int/eng#{"fulltext":["Kennedy v. the UK"]}

Council of Europe—European Commission for Democracy through Law (Venice Commission)

The Venice Commission has played a key role in standard setting for the democratic oversight of security services. Its report, adopted in 2007, provides a comprehensive overview of parliamentary, judicial, and specialised accountability bodies as well as complaint mechanisms.[14]

The Commission emphasises the importance of ombuds institutions, particularly in the context of the State's duty to provide effective remedy. Recognising the limited capacity of ordinary courts to serve as an effective remedy, the Commission points out that many countries mandate their ombuds institutions to investigate complaints against security services and report their findings. While the majority of ombuds institutions do not have the power to adjudicate on a case, their investigations and subsequent recommendations assist the authorities in taking corrective action.[15] However, the commission notes that ombuds institutions should have sufficient resources and expertise in order to effectively investigate complaints and make a meaningful contribution to the accountability system.[16]

In view of technological advancements in the field of intelligence

[14] Venice Commission, *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session,* (2007).
[15] *Venice Commission,* (2007), para 243-245.
[16] Ibid. para 237.

gathering, and the increasing use of strategic and mass surveillance, the Commission adopted a new report in 2015, focused exclusively on the oversight of signals intelligence.[17]

Council of Europe—Commissioner on Human Rights

Based on country visits and observations, the Commissioner on Human Rights makes recommendations pertinent to governance and oversight of security services. In 2015, taking into account the findings and conclusions of a CoE study,[18] the Commissioner set forth a serious of recommendations on democratic and effective oversight of security services. With regards to ombuds institutions, the Commissioner recommended that States should: 'Create or designate an external oversight body to receive and investigate complaints relating to *all aspects of security service activity* [emphasis added].'[19] The Commissioner's recommendation that complaints be received on all aspects of security service activity is notable in that it promotes a wider scope of work for oversight bodies such as ombuds institutions.

This section has outlined the key international and European standards on independent oversight of security services. More specialised instruments and standards on key areas of intelligence oversight such as overseeing the collection, use and sharing of

[17] Venice Commission, *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session,* CDL-AD, (2015), 011, available from: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e

[18] Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015).

[19] Ibid, Recommendation 10, p. 12.

personal data are discussed in Chapter 3 of this guide.

International and European Standards on Overseeing Security Services—Relevance to Georgia

In 2015, Georgia established a new security service—the State Security Service of Georgia—with a mandate to collect, analyse and disseminate intelligence to, inter alia, protect the constitutional order; combat terrorism, transnational organised crime and corruption. In addition to its broad mandate, the Service is tasked with preventing, detecting, suppressing and investigating crimes falling under its mandate, and to that end, is provided with law enforcement powers.[1]

Entrusting a security service with law enforcement tasks and powers such as 'detecting and investigating corruption'[2] constitutes a great risk for human rights violations. In this context, without strong safeguards it would be difficult to ensure that personal data collected for intelligence purposes is not used for domestic crime investigations and *vice versa*.

Currently, Georgia does not have a specialised oversight body with an exclusive mandate over the State Security Service, which makes the role of the Public Defender's Office (PDO) all the more important. The oversight of security services is already challenging for ombuds institutions due to the highly complex and closed nature of the services, and the limited capacity and resources of ombuds institutions. However, in the case of Georgia, the law enforcement powers of the State Security Service pose an

additional challenge to its oversight, as their misuse has serious implications for the right to life, liberty and security, as well as to a fair trial. The UN Compilation of Good Practices list a number of standards concerning the arrest and detention powers of security service:[3]

- If national law provides intelligence services with powers of arrest and detention, it is good practice for this to be explicitly within the context of functions pertaining to specific threats to national security, such as terrorism. In this way the services would be legally prohibited from exercising detention powers in other instances.
- The use of arrest and detention powers should be strictly limited to cases where there is reasonable suspicion that a crime (falling under the mandate of the intelligence services) has been, or is about to be, committed. Therefore, those powers should not be used only for the purpose of intelligence collection.
- Use of arrest and detention powers: the same legal safeguards, as well as judicial and independent oversight practices, should be applied to scrutinise the arrest and detention powers of security services. This requires that the PDO investigate complaints regarding arrests and detention, and be able to launch own-motion investigations and unannounced visits to detention facilities used by the security services.

If the above-mentioned standards are not adhered to, there would be a heightened risk of the development of a parallel law enforcement system, whereby intelligence services exercise

powers of arrest and detention in order to circumvent legal safeguards and oversight that apply to law enforcement agencies.[4]

Therefore, it is important for the PDO to be aware of the latest international legal and normative standards for security services and their independent oversight.

Georgia is party to the International Covenant on Civil and Political Rights, and the European Convention on Human Rights, whose provisions are legally binding. With the ratification of the European Convention on Human Rights, Georgia came under the jurisdiction of the European Court of Human Rights. A good understanding of the legal standards established by the Court's jurisprudence would assist the PDO in its oversight activities, particularly in formulating recommendations and policy proposals based on European standards.

Furthermore, the PDO can benefit from the standards and best practices set-out in other normative instruments and reports such as those of the Venice Commission, CoE Human Rights Commissioner as well as the Ottawa and Tshwane Principles. The standards established by these instruments would be useful reference points if legislation on the PDO or the security services is amended.

Sources:
(1) Articles 5 and 11 of the Law on State Security Services.
(2) Article 5 of the Law.
(3) UN Compilation of Good Practices, Practice 28.

(4) International Commission of Jurists, 'Assessing damage, urging action: Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights', (2009), p. 73–78, available from: http://www.un.org/en/sc/ctc/specialmeetings/2011/docs/icj/icj-2009-ejp-report.pdf

Key reference material:

- Council of Europe, 'Democratic and Effective Oversight of National Security Services', (2015), available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770
- Human Rights Council, 'Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies', A/HRC/14/46, (2010), available from: https://fas.org/irp/eprint/unhrc.pdf
- 'The Ottawa Principles on Anti-Terrorism and Human Rights', (2006), available from: http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf
- 'The Tshwane Principles', (2013), available from: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf
- Venice Commission, 'Update of the 2007 Report on the Democratic Oversight of the Security Services—Report on the Democratic Oversight of Signals Intelligence Agencies', (2015), available from:

http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

- Venice Commission, 'Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session', (2007), available from: http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

Chapter 2: Key Features for Effective Oversight of Security Services

There is no single 'correct' model for effective independent oversight of security services. Often States establish a variety of oversight mechanisms, such as ombuds institutions, data protection authorities, specialised expert oversight bodies, and auditor-generals; each monitoring a certain aspect of the activities of security services. However, regardless of the exact institutional set-up of such institutions, there are certain features that determine the effectiveness of oversight. These include independence, mandate, powers, resources, transparency, reporting and outreach. These features are referred to in several guidance documents, including the UN Compilation of Good Practices,[20] the European Parliament's Study 'Parliamentary Oversight of Security and Intelligence Agencies in the European Union',[21] and the CoE's Commissioner on Human Rights' issue paper 'Democratic and Effective Oversight of National Security Services'.[22]

[20] See: Practices 6-8 and paragraph 14, *UN Compilation of Good Practices*, A/HRC/14/46, available from: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

[21] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, (2011), Chapter 4.3, available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456151

[22] Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015).

This chapter will provide an overview of these key features, focusing on what they entail for ombuds institutions.

1. Independence

Independence is widely argued to be the key ingredient for ombuds institutions' effectiveness. [23] Its constituent parts, namely institutional, operational and financial independence, must be present for an ombuds institution to be effective.

Institutional independence

Institutional independence entails that ombuds institutions do not operate under the hierarchy or authority of the security services they oversee, nor the executive. Rather, ombuds institutions should report, and be accountable to parliament. This is a widely recognised and applied practice. Ombuds institutions in most EU Countries are directly accountable to their respective parliament.[24]

The legal basis of ombuds institutions is an important determinant of institutional independence. Ombuds institutions should be

[23] Benjamin Buckland and Will McDermott, *Ombuds Institutions for the Armed Forces: A Handbook* (DCAF: 2012), p. 39, available from: http://www.dcaf.ch/sites/default/files/publications/documents/OMBUDSHbook_FINAL_ONLINE.pdf

[24] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks,* (Luxembourg: 2015), p. 70, available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

established through legislation, and not by ministerial degrees or executive orders. This ensures that their powers cannot be restricted or disbanded at the whim of the executive. A clear and strong legal basis also helps the institution resist pressure.

Another key dimension of the institutional independence of ombuds institutions is the legal security of tenure. Ombudspersons who oversee security services are likely to deal with cases involving wrongdoing by intelligence agencies and officials leading to serious human rights violations. In order to ensure that ombuds persons work effectively and without fear of being dismissed, they should enjoy legal security of tenure during their term of office.[25] There should be clear procedures for the appointment and removal of the ombudsperson, and a narrowly defined set of criteria stipulating the circumstances under which removal can happen. Best practice suggests that both the appointment and removal process should be undertaken by parliament.[26] By way of example, in Finland the Ombudsman may only be removed from office 'for extremely weighty reasons' by a two-thirds majority of Parliament, following the opinion of the Constitutional Law Committee.[27]

[25] Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2015), p. 112, available from: http://www.dcaf.ch/making-intelligence-accountable

[26] Benjamin Buckland and Will McDermott, *Ombuds Institutions for the Armed Forces: A Handbook,* (DCAF: 2012), p. 44.

[27] *The Constitution of Finland*, 11 June 1999 (731/1999), entry into force 1 March 2000, Section 38.

Operational independence

Operational independence of ombuds institutions relates to their ability to perform functions without interference from other authorities. This entails:[28]

- ***Deciding on priorities and matters to be pursued***: given the limited resources of ombuds institutions and the wide-ranging human rights implications of the work of security services', there is no doubt that ombuds institutions need to prioritise the oversight of certain areas/issues over others. It is therefore important that they have the ability to decide on the areas that they wish to prioritise; and have the freedom to choose the matters they wish to further pursue. For instance, the Norwegian Parliamentary Ombudsman chose 'the right to information' as one of its priority areas for the period 2016-2017, and examined the issue extensively in its annual report.[29]
- ***Freedom to establish own working modalities:*** ombuds institutions should have the freedom to establish their own procedures for handling complaints, conducting investigations, and interviewing persons, as long as such procedures are in line with the mandate and powers conferred to them.

---

[28] For more details on operational independence, See: Benjamin Buckland and Will McDermott, *Ombuds Institutions for the Armed Forces: A Handbook,* (DCAF: 2012), p. 47-50.

[29] *Annual Report of the Norwegian Parliamentary Ombudsman*, (2016), p. 20, available from: http://www.theioi.org/ioi-news/current-news/norwegian-npm-releases-annual-report-2016

- ***Power to launch own-motion investigations and compel law enforcement cooperation:*** one of the most important measures of operational independence is the ability to launch an investigation without receiving a complaint or referral. In order to effectively investigate a complaint, an ombuds institution should be able to access facilities and documents of security services and/or hear involved persons. While national ombuds institutions do not have law enforcement powers, best practice is to be able to legally compel law enforcement cooperation so that ombuds institutions are not dependent on the willingness of security services to cooperate in their investigations.

The powers of ombuds institutions are explained in further detail later in this chapter.

Best Practice: Finnish Parliamentary Ombudsman

According to the Parliamentary Ombudsman Act (197/2002), the Ombudsman has the right to executive assistance free of charge from the authorities as he or she deems necessary. More specifically, the Ombudsman may order that a police inquiry, as referred to in the Police Act (493/1995), or a pre-trial investigation, as referred to in the Pre-trial Investigations Act (449/1987), be carried out in order to clarify a matter under investigation by the Ombudsman.

(Source: Parliamentary Ombudsman Act (197/2002), Section 8: https://www.oikeusasiamies.fi/en/parliamentary-ombudsman-act)

The power to compel police involvement is usually granted to specialised oversight bodies (such as the Dutch CTIVD, or Belgian Committee I). In this regard, the Finnish Parliamentary Ombudsman is an exceptional example.

Financial independence

Financial independence means that an ombuds institution obtains and manages its funds independently from any of the institutions it oversees; furthermore, that such funds are sufficient for the institution to fulfil its mandate.[30] Financial independence is best achieved when independent oversight mechanisms propose a budget, which is then approved by the parliament.[31] This is the case for the Belgian Committee I.[32] However, it should be noted that it is a specialised oversight body, and not an ombuds institution. The common practice for ombuds institutions is to receive funding from the state budget, reviewed and adopted by the parliament.

[30] Marten Oosting, 'Protecting the Integrity and Independence of the Ombudsman Institution: the Global Perspective,' in *The International Ombudsman Yearbook*, ed. the International Ombudsman Institute (Alphen aan den Riijn: Kluwer Law International, 2001), p. 19.
[31] *UN Compilation of Good Practices*, para 14.
[32] *Belgium Law on the Control of Police and Intelligence Services and the Centre for Threat Analysis*, Art. 48.

2. Resources

In order to operate effectively, ombuds institutions should be well resourced for a number of reasons. Firstly, intelligence governance is a highly complex area, which requires in-depth knowledge and expertise on mobile and electronic communication; management of personal information, collection and storage of mass data, wiretapping and other covert surveillance methods as well as respective national and international laws and regulations. Effective oversight over the activities and methods of security services require staff who are well informed on such topics. To this end, either ombuds institutions should offer competitive salaries to hire highly skilled persons, or should have the resources to offer rigorous in-house training on intelligence oversight related subjects.

Secondly, ombuds institutions may need specific expertise on a certain area in the frame of their investigations. In such cases, ombuds institutions should have the power to hire external experts for a specific period of time.[33]

Best Practices: Swedish Parliamentary Ombudsmen and Slovenian Human Rights Ombudsman

Swedish Parliamentary Ombudsmen

The Chief Parliamentary Ombudsman is allowed to appoint experts and referees to the extent needed and insofar as funds are

[33] Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2012), p. 39, available from: http://www.dcaf.ch/guidebook-understanding-intelligence-oversight

available

(Source: The Act with Instructions for the Parliamentary Ombudsmen, Art. 13: https://www.jo.se/en/About-JO/Legal-basis/Instructions/)

It is best practice to clearly stipulate such a power in law, instead of ombuds institutions having to request the hiring of experts on an ad-hoc basis when such a need arises.

Slovenian Human Rights Ombudsman

The Slovenian Ombudsman does not have the power to hire independent experts as in the case of Sweden, but may appoint employees of state bodies as experts to the service of his office, for a fixed period of time.

(Source: The Slovenian Human Rights Ombudsman Act, Art. 53: http://www.varuh-rs.si/legal-framework/constitution-laws/human-rights-ombudsman-act/?L=6)

Lastly, ombuds institutions handle highly sensitive information when overseeing the work of security services. Therefore such institutions need physical and technical resources such as secure meeting rooms to shield premises from remote communication devices, highly secure IT systems, and encrypted communications channels in order

to ensure confidential information remains secure, and to minimise the risks of leaks.[34]

Without sufficient financial, human and technical resources, ombuds institutions cannot be expected to adequately oversee security services.

3. Mandate

A clear mandate based on publicly available laws is essential for the effectiveness of independent oversight mechanisms. The mandate of most ombuds institutions covers all public administration agencies, including law enforcement and security services. In some cases, security services are explicitly excluded from the ombuds institutions' mandate. Examples include the UK's Parliamentary Commissioner and the Greek Ombudsman.[35] Thus, best practice is to explicitly state in law that overseeing security services falls under the mandate of the ombuds institution.

Another important factor in this regard is to define in law the specific functions that fall under the ombuds institutions' mandate. In overseeing security services, ombuds institutions are usually mandated to handle complaints. It is imperative that the scope of

[34] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (2011), p. 143-144, available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456151

[35] United Kingdom, *Parliamentary Commissioner Act 1967*, 22 March 1967, Section 5; Greece, Law No: 3094/2003, Art. 3.2.

mandate of the ombuds institutions is defined as broadly as possible to allow 'all and any member of the public to bring a complaint on the full breadth of intelligence service activities'.[36] Legislation should not limit the complainants to citizens, or affected persons only.

Best Practice: Dutch National Ombudsman

The Dutch Intelligence and Security Services act expressly states that 'Each person is entitled to file a complaint with the National Ombudsman on the actions or the alleged actions of the relevant Ministers, the heads of the services, the co-ordinator and the persons working for the services and for the co-ordinator'.
(Art. 83 (1):
http://www.dcaf.ch/sites/default/files/publications/documents/Netherlands_EN.pdf)

However, in addition to investigating complaints, best practice is to provide ombuds institutions with a mandate to launch own-motion and thematic investigations. This is a widely adopted practice in Europe, with examples including the Danish Parliamentary Ombudsman, Slovenian Human Rights Ombudsman and Serbian Protector of Citizens.[37]

[36] Craig Forcese, 'Handling Complaints about Intelligence Services' in Born and Wills (eds.) *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012), p. 196.
[37] 'Serbian Law on the Protector of Citizens art 24', *Slovenian Human Rights Ombudsman Act*, Art. 26; Danish Ombudsman Act. Chapter 5.

Best Practice: Serbian Protector of Citizens

In 2010, the Serbian Protector of Citizens launched an own-motion investigation of the BIA (Serbian Security Information Agency) concerning, inter alia, the surveillance of electronic communications and collection of metadata on telephone traffic. To this end, the Protector of Citizens carried out two inspections of BIA facilities, selected files for detailed review, and conducted meetings and interviews with BIA director and employees. It identified a number of irregularities with regards to obtaining interception warrants and the use of electronic surveillance methods. Consequently, the Protector of citizens made recommendations to BIA and other relevant authorities.

The full report can be accessed at:
http://www.ombudsman.org.rs/attachments/088_Report%20on%20the%20Preventive%20Control%20Visit.pdf

Recently, the Danish Parliamentary Ombudsman, on his own initiative, became involved in a case concerning access to information, which came to his attention due to media coverage. While the Ombudsman did not officially launch an investigation, it can still be considered as an own motion act.

Operational example: Danish Parliamentary Ombudsman

In 2013, the Danish Security and Intelligence Service (PET) postponed its reply to a citizen who had requested access to

information on nineteen separate occasions, providing no concrete reason for the delay. After each request, PET informed the citizen that it expected to be able to process the request within the next thirty days.

After reading about the case in a daily newspaper, the Ombudsman asked the Security and Intelligence Service and the Ministry for Justice for comments on the course of events. Upon the authorities' replies, the Ombudsman stated that the Service's handling of the citizen's request for access to files violated the Access to Public Administration Files Act.

A month and a half after the Ombudsman had asked the authorities for their comments; PET decided that the citizen could not be granted access to the files.

(Source: The Danish Parliamentary Ombudsman, 'Annual Report 2013', (2014), Case No. 12/04974, p. 50, available from: http://beretning2013.ombudsmanden.dk/english/ar2013/)

Lastly, the mandate of ombuds institutions should not limit the scope of investigations into procedural aspects. As regards privacy violations caused by surveillance, the European Union Agency for Fundamental Rights stated that most ombuds institutions predominantly investigate administrative failures, rather than the

actual merits of surveillance,[38] which hampers their ability to exercise effective oversight. States that are reforming their accountability mechanisms, or who are in the process of establishing ombuds institutions, may consider this aspect, and entrust those institutions with the mandate and necessary resources to investigate the merits of the case, in addition to procedural and administrative wrongdoings.

4. Powers

Ombuds institutions should have sufficient legal powers to be able to effectively investigate complaints relating to security services. The most notable power in this regard is access to information. Ombuds institutions should be given access to all information they deem necessary to carry out their functions, including classified and otherwise confidential information not in the public domain.[39] It is important that 'information' should not be limited to documents. The Tshwane Principles state that 'Information to which oversight bodies should have access includes, but is not limited to:

[38] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks,* (Luxembourg: 2015), p. 76, available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[39] Aidan Wills and Benjamin Buckland, *Access to Information by Intelligence and Security Service Oversight Bodies*, (DCAF/OSF: 2012), p. 2. available from: http://www.dcaf.ch/sites/default/files/publications/documents/Access_information_oversight_bodies_draft.02.12.pdf

(i) all records, technologies, and systems in the possession of security sector authorities, regardless of form or medium and whether or not they were created by that authority;
(ii) physical locations, objects, and facilities; and
(iii) information held by persons whom overseers deem to be relevant for their oversight functions.'[40]

There are different methods for accessing information, including interviewing persons, reviewing classified documents and information, and inspecting the premises of security services. While a comprehensive legal analysis of such methods is beyond the scope of this guide, this section will provide a brief overview of the aforementioned powers for investigating complaints.

Access to classified information

A certain degree of secrecy inevitably accompanies the work of the security services. The government classifies information and regulates access to such information through laws. While classified information is understandably shielded from the general public, it is essential for independent oversight mechanisms to effectively investigate complaints.

A widely endorsed practice is to provide the ombuds institution with full and unhindered access to all information, regardless of its level of

[40] *The Tshwane Principles*, Principle 32, 'Unrestricted Access to Information Necessary for Fulfilment of Mandate', available from: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

classification. However, in order to obtain such access, they are typically required to have security clearance. An exception to this rule is the Serbian Protector of Citizens, who does not need to be vetted.[41]

The power to access classified information comes with the duty to ensure that the information accessed by ombuds institutions is not unlawfully disclosed and used solely for the purposes of oversight. This duty is often enshrined in the laws regulating the activities of ombuds institutions. Ideally, the law should require independent oversight bodies to implement *all necessary measures* to protect the information they accessed.[42] Best practice suggests that the protective measures should be equivalent to those used by security services.

When ombuds institutions decide to disclose information obtained in the frame of their investigations, they should pay the utmost attention to the 'do-no-harm' principle towards the victims and affected persons. In this respect, the Tshwane Principles state that:

> 'The names and other personal data of victims, their relatives and witnesses may be withheld from disclosure to the general public to the extent necessary to prevent further harm to them, if the persons concerned or, in the case of deceased persons, their family members, expressly and voluntarily request withholding, or withholding is otherwise manifestly

[41] Aidan Wills and Benjamin Buckland, *Access to Information by Intelligence and Security Service Oversight Bodies*, (DCAF/OSF: 2012), p. 42.
[42] *Tshwane Principles*, Principle 35.

consistent with the person's own wishes or the particular needs of vulnerable groups. These caveats, however, should not preclude publication of aggregate or otherwise anonymous data.'[43]

Despite the laws entrusting ombuds institutions with the power to access classified information, in practice there may be obstructions. Most often the executive attempts to obstruct ombuds institutions' access to classified information by claiming that the disclose of highly sensitive information to such external bodies risks information being leaked or lost, which could have catastrophic consequences for national security. In such cases, it is worth pointing out that there are no examples of ombuds institutions leaking classified information. On the contrary, leaks considered to be 'damaging' to national security have almost always come from within the executive.

One safeguard against such obstructions is to impose some form of legislative sanction for non-compliance with access to information requests.

Best Practices: Public Defender of Georgia; and Swedish Parliamentary Ombudsman

The Law on the **Public Defender of Georgia** sets a ten day period in which authorities are obligated to provide the required material, documents and other information (Art. 23), with failure to do so punishable by law (Art. 25, see:

[43] *The Tshwane Principles*, Principle 10 (B)3.

http://www.ombudsman.ge/uploads/other/2/2058.pdf)

The **Swedish Parliamentary Ombudsman** is entitled to issue a penalty of up to SEK 10'000 for non-compliance with their request for information:

'When the Ombudsmen, in accordance with the stipulations of the Instrument of Government, request information and statements in cases other than those in which it has been decided to institute a preliminary inquiry, they may do so on penalty of fine not exceeding SEK 10,000. The Ombudsmen may impose such a penalty, if incurred.' (The Act with Instructions for the Parliamentary Ombudsmen, para 21, https://www.jo.se/en/About-JO/Legal-basis/Instructions/)

Interview and subpoena persons

An investigation cannot be based solely on written material. In order to establish sound findings and develop relevant recommendations, ombuds institutions should be entrusted with the power to interview any person deemed to possess any information relevant to the fulfilment of ombuds institution's mandate. This is a widely applied practice among ombuds institutions in Europe.[44] When required,

[44] See, for example, *Finnish Parliamentary Ombudsman Act*, Section. 9, available from: https://www.oikeusasiamies.fi/en/parliamentary-ombudsman-act; *Slovenian Human Rights Ombudsman*, Art. 36, available from: http://www.varuh-rs.si/legal-framework/constitution-laws/human-rights-ombudsman-act/?L=6

such powers should be used with the full cooperation of law enforcement agencies.[45] A further step is to establish a power to subpoena persons to give evidence in court on any matter of importance to an investigation, which is the case for the Danish Ombudsman.[46] However, it should be noted that the power to subpoena should be best viewed as 'an option of last resort, only to be used in the event that an agency or the executive fails to cooperate with an investigation.'[47]

Access to facilities

Access to the premises of security services forms an essential component of investigations. Such visits enhance an ombuds institution's understanding of a security service and serve as an opportunity to conduct interviews with staff and access physical and electronic records.[48]

A clear stipulation in the law permitting unhindered access to **all** facilities is considered as best practice. Restricting the exercise of this power for national security or other purposes should be avoided. An example of this suboptimal practice is the Ombudsmen Act of New Zealand, which allows the Attorney General to deny access to

[45] *The Tshwane Principles*, Principle 33(a).
[46] *Danish Ombudsman Act*, Art. 19 (3), available from: https://en.ombudsmanden.dk/loven/
[47] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (2011), p. 137.
[48] Aidan Wills and Benjamin Buckland, *Access to Information by Intelligence and Security Service Oversight Bodies*, (DCAF/OSF: 2012), p. 16.

Ombudsmen 'if he is satisfied that the exercise of the power conferred by this section might prejudice the security, defense, or international relations of New Zealand, including New Zealand's relations with the government of any other country or with any international organization.'[49] This power is open to abuse as the 'security, defense, or international relations' is not clearly defined in the law, and thus can be broadly interpreted in order to restrict access to facilities.

Ombuds institutions should be given the power to make unannounced visits to facilities used by security services, and independently decide which files and records they wish to review.

Access to information is a relatively complex legal issue. A comprehensive analysis of legal standards pertaining to access to information is beyond the scope of this guide. Further information on international standards, as well as challenges encountered by independent oversight institutions, can be found at: http://www.dcaf.ch/Publications/Access-to-Information-by-Intelligence-and-Security-Service-Oversight-Bodies.

5. Reporting and Recommendations

When an investigation is completed, ombuds institutions are required to draft a report including, inter alia, findings of the

[49] *New Zealand Ombudsmen Act* (1975), Art. 27 (3), available from: http://www.legislation.govt.nz/act/public/1975/0009/latest/DLM4395429.html

investigation and recommendations (primarily for the security services), as well as other actors involved in their governance and oversight.

Oversight bodies often produce two versions of their reports, one version for the executive and the security services that may contain classified information, and a second for the public.[50] It is recommended that ombuds institutions consult with the executive and intelligence services before releasing public reports. This would allow security services to share any concerns on sensitive information before the report is published,[51] and serves as a confidence building measure between ombuds institutions and the services. It is however imperative that the final decision regarding what should be published rests with the ombuds institution.[52]

Apart from reports on investigations, ombuds institutions also publish thematic and annual reports to the authorities they report to, which in most cases is the parliament.

Reporting is a useful tool to inform the general public about the oversight activities of the ombuds institutions, and what they recommend to enhance the protection of fundamental human rights. While the recommendations of ombuds institutions are not legally binding, they are nevertheless an important instrument to pressure the executive, legislature and security services to take corrective

[50] Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2012) p. 40.
[51] Ibid.
[52] *The Tshwane Principles*, Principle 34 (b).

action. Without effective recommendations, oversight activities of the ombuds institutions can only identify problems rather than solutions. In this respect, the Association for the Prevention of Torture (APT) has developed a 'double-smart recommendations model' that builds upon assessing the effectiveness of recommendations against ten criteria:

'**Specific**: each recommendation should address only one specific issue

Measurable: the evaluation of the implementation should be as easy as possible

Achievable: each recommendation should be realistic and feasible

Results-oriented: the actions suggested should lead to a concrete result

Time-bound: it should mention a realistic timeframe

AND

Solution-suggestive: wherever possible, recommendations should propose credible solutions

Mindful of prioritization, sequencing and risks: it might be useful to address more urgent recommendations first and reserve others for subsequent reports

Argued: recommendations should be based on high-quality, objective evidence and analysis and refer to standards

Real-cause responsive: recommendations should address the cause of the problem, rather than the symptoms

Targeted: recommendations should be directed to specific institutions/actors rather than 'the authorities.'[53]

6. Transparency, Accessibility, and Public Outreach

Ombuds institutions should be transparent in their own work in order to ensure public confidence. To this end, annual reports as well as the budget and expenses of the institution should be accessible to the public.

Best Practice: Public Defender's Office, Georgia

The PDO not only publishes its annual reports online, but also organises a yearly conference, whereby the Annual Activity Report is presented to representatives of Parliament, governmental agencies, international organisations and non-governmental organisations. This multi-stakeholder platform allows for dialogue on the activities and achievements of the PDO, as well as on challenges encountered.

(Source: Public Defenders Office (PDO), 'Activity Report 2016', (2017), available from:

[53] Association for the Prevention of Torture (APT), *Making Effective Recommendations,* Briefing No: 1, Detention Monitoring Briefings, (2008), available from: https://www.apt.ch/content/files_res/Briefing1_en.pdf

http://www.ombudsman.ge/en/news/public-defenders-activity-report-2016.page)

Without awareness among the public, the work of ombuds institutions would have little effect. The public should be aware of how the ombuds institution functions and how it can be accessed. Persons belonging to minority communities, asylum seekers, foreign nationals and migrants may be disproportionally targeted by security services in their information collection activities. Some among these groups may not be aware of their rights or lack the resources to seek remedy. It is therefore important that ombuds institutions pay particular regard to the principle of non-discrimination in their accessibility policies and practices. In this context, the following constitute best practices:

- Publishing necessary information in an uncomplicated manner and in several languages, particularly those spoken by minority communities;
- Providing different means of access to the ombuds institution (e.g., online, per phone, per mail or physical access to their offices) to take into account the special needs of persons at risk of vulnerability, including, detainees, children, and persons with disabilities;
- Establishing flexible visiting hours and a play space for children accompanying complainants;
- Guaranteeing the availability of female and male interviewers, in case a complainant would like to be interviewed by someone of the same sex; and
- Ensuring that offices in rural areas, as well as in cities, are

easily reachable on foot or by public transportation.[54]

Best Practices: German Institute for Human Rights; Scottish Public Service Ombudsman

The German Institute for Human Rights, Germany's independent national human rights institution, has a separate section on its website where it provides text and information in simplified German, addressing those who are not fluent in the language.

(Source: http://www.institut-fuer-menschenrechte.de/leichtesprache/)

The Scottish Public Service Ombudsman accepts enquiries and complaints in all languages, and provides telephone interpretation support as well. The office of the Ombudsman also provides reasonable accommodation for persons with disabilities, including a Braille and loop induction system.

(Source: http://www.spso.org.uk/accessibility)

Taking into consideration the transformation in communication means, ombuds institutions should actively use a variety of media to promote their work and to raise awareness on the importance of

[54] Megan Bastick, *Integrating Gender into Oversight of the Security Sector by Ombuds Institutions & National Human Rights Institutions* (Geneva: DCAF, OSCE, OSCE/ODIHR, 2014), p. 27.

overseeing security services, as well as implications for human rights in the absence thereof.

Presented below are several best practices from Serbia, Netherlands, Ireland, Canada and Hong Kong where Ombuds Institutions utilised a variety of media and public information tools to raise awareness on the right to privacy, the right to know (access to information) the surveillance activities of security services, as well as what ombuds institutions are doing to protect fundamental human rights and how they can assist complainants in seeking effective remedy.

Best Practice: Serbian Protector of Citizens

The Protector of Citizens gave an interview to a popular daily newspaper concerning citizens' complaints against the work of security services, during which he explained technical issues such as illegal eavesdropping and its implications in a simple manner, and provided information on how citizens may submit complaints. He also explained how his office investigates complaints as well as the possible outcomes of an investigation.

Such an interview with a popular daily newspaper enhances the visibility of the ombudsman, and enables wider outreach. The full transcript of the interview can be accessed at: http://www.ombudsman.org.rs/index.php?option=com_content&view=article&id=33:saša-janković-protector-of-citizens-speaks-for-danas-daily-about-the-citizens-complaints-against-the-work-of-security-agencies-&catid=16&Itemid=19

Best Practice: Office of the Ombudsman, Hong-Kong, China

In an attempt to inform the public on the Law on Access to Information, privacy rights and the Ombudsman's jurisdiction on these matters, the Office of the Ombudsman collaborated with the public broadcaster of Hong-Kong to produce and broadcast a televised mini-series called 'The Ombudsman 5-minuter'.

'The Ombudsman 5-minuter' comprises of five short episodes, each of which, in sequence of broadcast date, covers one of the following subjects: the Ombudsman's jurisdiction, direct investigation, secrecy and privacy, the Code and mediation. Commencing on 24 April 2016, the mini-series was broadcast on five consecutive Sundays on RTHK Channel 31 at 6.55pm and on TVB Jade Channel at 3.50pm.

(Source: http://www.theioi.org/ioi-news/current-news/ombudsman-hong-kong-promotes-code-on-access-to-information-and-launches-tv-programme)

Best Practice: Dutch National Ombudsman; the Office of the Ombudsman in Ireland

The Dutch National Ombudsman actively uses social media, including WhatsApp and YouTube. The Ombudsman produced a video entitled 'A Day in the Life of a National Ombudsman' which shows an average working day of the Ombudsman, including

meetings with her staff, briefings by the investigation team, media interviews and so forth. Use of such audio-visual tools and diverse media platforms would be useful when reaching out to new audiences, especially youth. The video can be accessed at: https://www.youtube.com/watch?v=v8iEsw1BZmM&feature=youtu.be

The Office of the Ombudsman in Ireland produced short videos explaining who the Ombudsman is, what the functions of the office are, how they can assist complainants and affected persons, and how they can be contacted. The video was also produced in Gaelic and sign language, and has been viewed by thousands on YouTube. https://www.youtube.com/watch?v=Ae7SEZdyCy8

For similar best practices and further guidance, see the Social Media Guide for Ombuds Institutions for the Armed Forces, published by DCAF: http://www.dcaf.ch/Publications/Social-Media-Guide-for-Ombuds-Institutions-for-the-Armed-Forces

Best Practices: Office of the Ombudsman in Manitoba, Canada

Since 2005, the Manitoba Ombudsman celebrates the national Right to Know Week from 22 to 28 September and international Right to Know Day on September 28.The purpose of Right to Know is to raise awareness of an individual's democratic right of access to government-held information and to promote the benefits of open, accessible, and transparent governance.[1]

In doing so, the Ombudsman invites citizens to visit staffed display tables at public libraries to obtain more information, tips and practical advice on making an access request under *The Freedom of Information and Protection of Privacy Act, and displays videos produced by his office giving practical tips for* submitting an access request under Manitoba's Freedom of Information and Protection of Privacy Act (FIPPA). The video can be accessed at: https://www.youtube.com/watch?v=9zq_O4tcpQE
(Source: http://www.theioi.org/ioi-news/current-news/ombudsman-celebrates-right-to-know-week)

Key Features for Effective Oversight—Relevance to Georgia

This chapter has focused on the key features for effective oversight of security services, namely independence, resources, mandate and powers, reporting and public outreach. The State Security Service of Georgia has been recently established; therefore it is difficult to assess challenges encountered by the PDO in overseeing the Security Service, as well as the PDO's needs and priorities in this regard. However, relevant standards and best practices provided in this chapter are intended to serve as a useful reference for the PDO for comparison and self-assessment.

Independence: This section analysed independence on three levels: institutional, operational and financial. The law on the Public Defender of Georgia has clear stipulations establishing institutional independence. The PDO is hierarchically independent

from the executive and the security services it oversees; and is accountable to the parliament.

The appointment of the public defender is done through the parliament upon a cross-party nomination process (Art. 6). The Public Defender enjoys personal immunity and may not be prosecuted for opinions and views expressed in the exercise of his/her duties (Art. 5). The criteria for termination are listed in the law, and the decision requires a parliamentary majority. All of these stipulations embody best practice with respect to institutional independence.

As regards operational independence, the PDO is able to determine its structure, organisation; areas of activity, rules of operation and other issues (Art. 26). Furthermore, the PDO is able to independently decide on which matters to further pursue and launch own-motion investigations (Arts. 14 and 17). However, it lacks the power to compel law enforcement cooperation in its investigations, which is a significant restraint on its operational independence (also see section on Mandate and Powers). If the PDO's powers are revised in the future, the Finnish Ombudsman's power to compel law enforcement in their investigations can serve as a reference.

The funding of the PDO is provided through the State budget, which is adopted by the Parliament. According to the 2016 activity report of the PDO, grants received from foreign donors amounted to nearly half of its budget. While foreign grants are crucial for the PDO's capacity development and project implementation in the short term, it is important not to rely on external funding and

ensure a sustainable budget for the institution in the long term.

Mandate and powers: The PDO has a wide mandate, of which oversight of the State Security Service (SSS) is part of. Although the SSS has been established recently, the PDO has begun to exercise oversight by reviewing the relevant legal framework and respective amendments to the legislation on surveillance, and by putting forth relevant recommendations.

In May 2017, the PDO filed a constitutional suit with the Constitutional Court of Georgia with regards to the constitutionality of the legislation adopted by the Parliament of Georgia on the regulation of secret investigative actions.

However, in terms of powers the PDO faces certain challenges. Even though the law provides the Public Defender with the power to access any information regardless of its level of classification, in practice executive authorities sometimes disregard this obligation, and do not provide the PDO with the necessary information. This was the case in January 2017 when the Ministry of Justice did not respond to the Public Defender's request for information on MoJ officials. If such a practice is replicated by the SSS in the future, it may pose a serious risk to the effectiveness of PDO oversight.

(Source: Public Defender Office of Georgia, 'Information Bulletin on Public Defender of Georgia,' No. 2, (February 2017), p. 4, available from: http://www.ombudsman.ge/uploads/other/4/4312.pdf)

Furthermore, as previously mentioned, the PDO does not have the power to compel law enforcement cooperation in their investigations. According to the PDO, the investigating authorities, especially the office of the Prosecutor, are uncooperative and unresponsive to the requests and recommendations of the PDO. The lack of law-enforcement type investigatory powers, combined with the uncooperative attitude of prosecutorial authorities poses another challenge to the PDO in overseeing the SSS.

(Source: Public Defender Office of Georgia, 'The Report of the Public Defender of Georgia: On the Situation of Protection of Human Rights and Freedoms in Georgia', Short Version, (2015), p. 66, available from: http://www.ombudsman.ge/uploads/other/3/3652.pdf)

Reporting and Recommendations: As is the case with other ombuds institutions and national human rights institutions, recommendations of the PDO are not legally binding. However, a decisive follow-up on the recommendations is an effective way to exert pressure over the executive. In 2017, the PDO, in cooperation with the parliament, launched a practice whereby representatives of the executive are invited to attend relevant parliamentary committee meetings. In the presence of PDO representatives and committee members, Ministry officials are asked to report on progress with respect to implementing the recommendations of the PDO. This constitutes an excellent example of cooperation with the parliament in following up on recommendations. If this practice continues, and particularly if it is applied to the SSS in the future, it would enhance the oversight

capacity of the PDO.

Transparency, Accessibility, Public Outreach: The PDO is very active in terms of raising awareness on certain issues through public conferences and debates, and campaigns. As regards the right to privacy, the PDO is participating in the 'This affects you' campaign, which aims to raise awareness on privacy related issues. Furthermore, the website of the PDO has a self-timer, which indicates the time since the PDO has called upon investigating authorities to identify those who recorded and leaked video footage showing the private life of a politician.

(Source: http://www.ombudsman.ge/en/news/public-defender-launches-campaign-against-release-of-video-footage-showing-private-life.page)

With respect to oversight of the State Security Service of Georgia, there remains potential to reach out to and engage with a larger public audience. Considering that the SSS has been recently established, the public may not be fully aware of its powers, nor how their abuse may infringe upon their privacy.

In this regard, the PDO can use both mass and social media more effectively and hold awareness raising activities to explain the powers of the SSS, as well as how the PDO oversees it. To this end, the PDO can benefit from the innovative practices employed by the Manitoba Ombudsman in Canada, Serbian Protector of Citizens and the Office of the Ombudsman in Hong Kong.

Key reference material:

- Aidan Wills and Benjamin Buckland, 'Access to Information by Intelligence and Security Service Oversight Bodies', (DCAF/OSF: 2012), available from: http://www.dcaf.ch/sites/default/files/publications/documents/Access_information_oversight_bodies_draft.02.12.pdf
- Aidan Wills, 'Guidebook: Understanding Intelligence Oversight', (DCAF: 2012), available from: http://www.dcaf.ch/guidebook-understanding-intelligence-oversight
- Aidan Wills and Mathias Vermeulen, 'Parliamentary Oversight of Security and Intelligence Agencies in the European Union', (2011), available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456151
- Council of Europe, 'Democratic and Effective Oversight of National Security Services', (2015), available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770
- European Union Agency for Fundamental Rights, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks', (Luxembourg: 2015), available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf
- Hans Born and Ian Leigh, 'Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of

Intelligence Agencies', (DCAF: 2015), available from: http://www.dcaf.ch/making-intelligence-accountable

- Megan Bastick, 'Integrating Gender into Oversight of the Security Sector by Ombuds Institutions & National Human Rights Institutions', (Geneva: DCAF, OSCE, OSCE/ODIHR, 2014).
- William McDermott and Efrat Gilad, 'Social Media Guide for Ombuds Institutions for the Armed Forces', (2016), available from: http://www.dcaf.ch/sites/default/files/publications/documents/Social-Media-Guide-Ombuds-Institutions.pdf

Ombuds institution legislation referred to in the chapter:

- Danish Ombudsman Act, available from: https://en.ombudsmanden.dk/loven/
- Finnish Parliamentary Ombudsman Act, available from: https://www.oikeusasiamies.fi/en/parliamentary-ombudsman-act
- New Zealand Ombudsmen Act, available from: http://www.legislation.govt.nz/act/public/1975/0009/latest/DLM4395429.html
- Slovenian Human Rights Ombudsman, available from: http://www.varuh-rs.si/legal-framework/constitution-laws/human-rights-ombudsman-act/?L=6
- Serbian Law on the Protector of Citizens, available from: http://www.ombudsman.rs/index.php/o-nama/normativni-okvir-za-rad/643-2009-10-27-16-01-21

- The Netherlands Intelligence and Security Services Act, available from: http://www.dcaf.ch/sites/default/files/publications/documents/Netherlands_EN.pdf

Chapter 3: Key Areas of Intelligence Oversight—Best Practices

In essence, security services have three key roles: to collect information, including personal data; use this data to produce intelligence, and share that intelligence with national and international security agencies and the executive. This chapter provides standards and examples of best practices in overseeing those key processes.

1. Overseeing Information Collection

Information collection—definition and types

The methods and scale of information collection are controversial aspects of the work of security services. In terms of scale, services collect information through targeted or mass surveillance. Targeted surveillance is used against a person or group of persons suspected of engaging in or planning to conduct actions which threaten national security. Usually proof indicating responsibility or probable suspicion is necessary for the judicial authorisation of targeted surveillance. On the other hand, mass surveillance is not necessarily predicated on a suspicion against a particular person or persons; rather it is proactive, aiming to identifying potential threats.[55]

[55] Venice Commission, *Update of the 2007 Report on the Democratic Oversight of the Security Services – Report on the Democratic Oversight of Signals Intelligence Agencies*, (2015), paras 38-46.

Security services collect information through open sources or by employing covert methods. Open sources include information that is publicly available such as that found in the media, on social networking sites and blogs, as well as official data including government reports, demographics, and legislative hearings. Covert methods of surveillance, however, obtain information without the knowledge and consent of the person who is surveilled. This can be done by:[56]

- Monitoring and intercepting verbal, electronic and paper-based communications;
- Secretly recording or photographing individuals and their property; and
- Undertaking undercover operations and infiltrating groups.

International and European standards on the oversight of covert surveillance

Covert surveillance measures are highly intrusive. Therefore an abuse of such measures would likely lead to serious human rights violations, in particular the right to privacy. The right to privacy is enshrined in Article 17 of the International Covenant on Civil and Political Rights, which prohibits arbitrary and unlawful interference into someone's privacy.

In the past decade, there has been a growing interest in the independent oversight of information collection, in particular covert surveillance measures. Practice 22 of the UN Compilation of Good

[56] Aidan Wills, *Understanding Intelligence Oversight*, (DCAF: 2012), p. 17.

Practices refers to the role of independent agencies overseeing information collection by the security services.

UN Compilation of Good Practices

Practice 22. Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence-collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.

Following the Snowden revelations, which sparked a public debate on mass surveillance and erosion of privacy rights, the UN General Assembly adopted a resolution on the Right to Privacy in the Digital Age.[57] The resolution expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. In this regard, the General Assembly called upon all States 'to establish or maintain existing **independent, effective domestic oversight mechanisms** capable of ensuring transparency, as appropriate, and accountability for State surveillance of

[57] UN General Assembly, A/Res/ 68/167, preamble, para 4(d).

communications, their interception and the collection of personal data'.[58]

At the European level, Article 8 of the European Convention of Human Rights (ECHR) protects the right to privacy. It stipulates that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence; and
2. There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law and is necessary in a democratic society in the interests of national security**, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Court of Human Rights interprets the application of ECHR articles. The court has found in several cases that the collection and use of personal data by security services constitutes an 'interference', and should only be permissible under the strict criteria set forth in Article 8.2: 'in accordance with the law', 'necessary', and 'in the interests of national security'.[59] The first criteria requires that states regulate intelligence collection through law which is accessible to members of the public and which clearly stipulates the circumstances in which such covert measures can be used.[60]

[58] Ibid.
[59] For a more detailed discussion, see: Ian Leigh, 'Overseeing the Use of Personal Data', in Born and Wills *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012), p. 105-122.
[60] Ibid, p. 109.

Therefore in most democratic countries, information collection is regulated by law, which defines, inter alia:

- The methods of covert surveillance;
- The necessary conditions whereby covert methods are permissible (level of threshold of suspicion, and restrictions); and
- What information services are and are not permitted to collect.[61]

In this regard, the role of national courts to authorise surveillance requests and/or adjudicate on cases is crucial; since they assess the lawfulness, propriety and necessity of covert surveillance measures.

Besides the aforementioned criteria, the European Court of Human Rights has established important standards on the oversight of covert surveillance through its landmark judgements.

In the case of ***Popescu v. Romania***, the Court ruled that the lack of independent mechanisms to oversee surveillance authorisations constitutes a violation of the right to privacy, since the Romanian legislative framework did not allow for any authority to review ex-post facto the implementation of interception measures authorised by public prosecutors.

This important ruling reinforced the standard on ex-post independent oversight of surveillance authorisations, which can be carried out by either a judicial or specialised oversight body. The court further

[61] Aidan Wills, *Understanding Intelligence Oversight*, (DCAF: 2012), p. 18.

stated that the content of the intercepted material (voice recordings etc.), as well as authorisation for the communications interception, should be open to independent expert assessment in cases where there are doubts as to whether a recording was genuine or reliable.[62]

The role of external bodies in overseeing surveillance measures is not limited to the process of authorisation. The Court, in ***Klass and others v. Germany*** has established that the external oversight of surveillance measures may take place before measures are implemented, during their implementation or following their termination.[63] The ruling is a judicial recognition of the broad scope for external and independent oversight of surveillance process.

Control and oversight mechanisms over covert surveillance—the role of ombuds institutions

The first step in ensuring accountability is to subject the use of covert measures to judicial authorisation so that courts may review the legality, necessity and proportionality of the measures requested by the services. This is a form of ex-ante oversight, and applied in the majority of Council of Europe States. In some countries this form of accountability is not exercised by the judiciary, but rather by quasi-judicial specialised bodies. For instance, the German government is required by law to inform the G10 Commission, an expert oversight body, on upcoming operations that will employ intrusive methods of

[62] *Popescu vs Romania,* (71525/01), available from: https://hudoc.echr.coe.int/eng#{"itemid":["002-2763"]}
[63] *Klass and Others v. Germany,* (para 54).

surveillance. The Commission decides whether the use of intrusive collection methods is permissible and necessary.[64]

A second step is to monitor the surveillance measures employed by the services. Many countries use a combination of mechanisms during this phase, including internal and executive control of the services (through regular inspections); and in some instances, specialised parliamentary or expert bodies (through regular reporting by the services and the ministries).

Ombuds institutions can also play a role in monitoring surveillance measures through conducting monitoring visits or inspections of the security services in the frame of own-motion investigations. In particular, ombuds institutions can review the internal procedures of the services concerning surveillance authorisations and their implementation. This can be done by:

- Reviewing the internal processes for requesting surveillance measures and applying for judicial authorisations;
- Analysing documentation and justifications for a judicial authorisation request, as well as any further correspondence with the judge in question;
- Checking internal guidelines and directions of the senior management once the surveillance is authorised;
- Looking at what records are kept and how are they kept;
- Reviewing whether the surveillance was carried out in accordance with the judicial authorisation (especially with

[64] Lauren Hutton, 'Overseeing Information Collection', Tool 5, p. 99, in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012).

regards to the timeframe, and the protection of the rights of third persons); and

- Looking at the justifications and processes for any renewal of a surveillance authorisation.

While scrutinising these procedural aspects may seem tedious, they can reveal serious wrongdoing and human rights violations. However, given the broad mandate and limited resources of ombuds institutions, own-motion investigations on covert surveillance measures are not common practice among national ombuds institutions. The Serbian Protector of Citizens represents a rare exception in this regard. As mentioned in the previous chapter, the Serbian Protector of Citizens launched an own-motion investigation of the BIA (Serbian Security Information Agency) concerning, inter alia, the surveillance of electronic communications and collection of metadata on telephone traffic. To this end, the Protector of Citizens carried out two inspection visits to BIA facilities in 2010, selected files for detailed review, and conducted meetings and interviews with the director of BIA and its employees.[65]

Taking into account the complexity of covert surveillance, states increasingly opt for establishing expert oversight bodies with exclusive mandates to oversee the activities of security services. They

[65] For more information on the own-motion investigation, see: Serbian Protector of Citizens*, Report: On A Preventive Control Visit By The Protector Of Citizens To The Security-Information Agency With Recommendations And Opinions*, (2014), available from: http://www.ombudsman.org.rs/attachments/088_Report%20on%20the%20Preventive%20Control%20Visit.pdf

are typically well-resourced and entrusted with greater powers. For instance, the Belgian Standing Intelligence Agencies Review Committee monitors intrusive surveillance operations, and has the power to order their termination and the destruction of collected information.[66] The Committee's investigators can exercise police powers to secure the cooperation of security services.[67] The Dutch Control Committee (CTIVD) has its own facilities in the premises of the national intelligence agency, and the CTIVD is permitted to log directly into the files of the agency.[68]

The last step in the accountability cycle is ex-post facto review, i.e. overseeing the surveillance measures after they have taken place. Here, along with other mechanisms, ombuds institutions also have a role; in particular in that they are mandated to handle complaints. However, oversight of covert intelligence collection is inherently more challenging for ombuds institutions because of two primary reasons. First, due to the use of covert methods, the subject of the surveillance may not be aware of the surveillance, and thus not able to file a complaint. Therefore ombuds institutions usually receive few complaints, and have a limited impact in this regard.

---

[66] Lauren Hutton, 'Overseeing Information Collection', Tool 5, p. 99, in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012). Also see: http://comiteri.be/index.php/en/standing-committee-i/eight-assignments

[67] Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p. 49. Also see: Belgium, *Act governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment*, (1991), Art. 45-49.

[68] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (2011), p. 137.

Second, even when ombuds institutions receive complaints, they often lack the powers, resources and expertise to effectively investigate whether the methods were used lawfully and proportionally in accordance with the authorisation. This is why expert oversight bodies are usually also given the task of ex-post review, including the handling of complaints. Expert oversight bodies with complaint handling functions include, inter alia, the G10 Commission in Germany, the Standing Intelligence Agencies Review Committee (Committee I) in Belgium, the Dutch Control Committee (CTIVD), and the Commission on Security and Integrity Protection in Sweden.[69]

While expert oversight bodies often embody best practices, this does not mean that general-purpose ombuds institutions cannot effectively oversee the use of covert intelligence methods. The work of the Finnish Parliamentary Ombudsman is a good example of overseeing not only the practices of services, but also authorisation processes.

Overseeing the process of judicial authorisation has been a controversial issue. In order to protect the judicial independence and the separation of powers, authorisation-issuing processes are not usually subject to *ex post* scrutiny by an oversight body.[70] However

[69] For a more detailed overview of the role of expert oversight bodies, see: Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (2011), p. 90-93.

[70] Iain Cameron, 'Parliamentary and specialised oversight of security and intelligence agencies in Sweden', p. 285, in Aidan Wills and Mathias

quasi-judicial bodes, such as the Administrative Commission in Belgium, which authorises certain surveillance measures, can be held accountable for the authorisation decisions it makes.[71]

In 2015, the Council of Europe Commissioner for Human Rights recommended that states 'Consider how surveillance authorization processes can be kept under ex post facto review by an independent body that is empowered to examine decisions taken by the authorizing body.'[72]

Best Practice: Parliamentary Ombudsman of Finland

In 1995, the Parliamentary Ombudsman of Finland was entrusted with the special task of overseeing covert intelligence gathering. The mandate covers all institutions collecting intelligence including the police, customs, defence forces and the border guard. The Finnish Security Intelligence Service (SUPO) is part of the police organisation, under the authority of the Ministry of Interior.

The scope of oversight exercised by the ombudsman is not clearly defined in law, which provides the ombudsman with considerable discretion. Given its limited resources in terms of expertise and

---

Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (2011).

[71] The expert oversight body in Belgium, Committee I, has the power to overrule the authorisation decisions of the Administrative Commission. For more information, see Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p. 56.

[72] Ibid. p. 12.

personnel, the office of the Ombudsman does not conduct 'direct' oversight of intelligence gathering activities, but rather, in their own words, conducts an 'oversight of oversight' by scrutinising judicial authorisations, and the effectiveness of internal control mechanisms in the aforementioned agencies. Nevertheless, the Ombudsman's oversight has made a considerable impact on safeguarding fundamental human rights. Selected best practices are presented below:

1—Establishing informal channels of communication with judges: requests for telecommunication interceptions are authorised by district court judges. The ombudsman has actively reached out to judges, informed them on different types of communication surveillance and their implications for privacy rights. The careful and constructive tone of the dialogue ensured that the Ombudsman's intentions were not seen as interfering with the independence of the judiciary, but rather to raise awareness on the part of district judges concerning complex surveillance measures and their potential implications for human rights. This has led to a sustained dialogue, based on mutual trust. The Ombudsman reported that on several instances the district judges contacted the office of ombudsman to discuss questions of legal interpretation on a surveillance case.[1] While this does not constitute a direct form of oversight over the security services, providing support to judges ensures that surveillance requests are reviewed more thoroughly.

2—Reviewing court rulings on informing subjects of surveillance: according to the Finnish Coercive Measures Act, persons who are

surveilled by covert methods shall be informed within a year after such measures are applied. Only in exceptional cases may judges rule that the person shall not be informed. The Ombudsman conducted an own-motion investigation into cases in which courts allowed for the exception. The investigation found that in many cases the police requested to apply for exceptions and thus not to inform the person(s) ex-post facto; and courts often ruled in favour of these requests, without thorough examinations of the justifications as to why they were made. After the Ombudsman's investigation, the courts applied a more thorough review; leading to a marked decrease in the number of cases where the exception has been applied.[2]

3—Reviewing authorisation processes for covert surveillance: based on monitoring activities, the Ombudsman observed that in some cases courts approve authorisation requests without proper justification provided by the authorities. It was found that in five per cent of cases, the only grounds presented in support of an application was the police officer's notification that he had reason to suspect that a particular person was engaged in criminal activity, without mentioning on which facts the suspicion was based.[3] Furthermore, the Ombudsman found that in several cases the verbal statements of judges to explain why an authorisation was given were not properly recorded, hampering the ability of the ombudsman to review the reasons for granting the authorisation. However, the Ombudsman noted that in recent years this practice has improved.

4—Inspections of the facilities of security services: the

Ombudsman conducts regular inspections of selected facilities of the police and security services, and reviews requests for using intrusive measures and decisions concerning technical surveillance. In addition to its own inspections, the Ombudsman actively cooperates with the National Police Board, another body inspecting the operations of the security service (SUPO). The Ombudsman reviews the inspection reports of the Board, and regularly meets with them to discuss legal gaps in the system and problematic practices.[4]

Apart from the aforementioned activities, the Ombudsman investigates individual complaints against security services concerning the unlawful violation of privacy and abuse of surveillance powers. However, the Ombudsman notes that the number of complaints is rather low, at no more than ten a year.

Annual Reports of the Ombudsman have a specific section dedicated to the oversight of covert surveillance. English versions of the reports can be found at: http://www.oikeusasiamies.fi/Resource.phx/eoa/english/publications/annual.htx

Sources:
(1) Juha Haapamäki, 'Special report of the Finnish Ombudsman' on *Oversight of Covert Police Intelligence Gathering,* Parliamentary Ombudsman of Finland, (n.d), p. 213, available from: https://www.oikeusasiamies.fi/documents/20184/38532/Haapamaki%2C+Oversight+of+covert++police+intelligence+gathering.pdf
(2) Ibid. p. 214.

(3) Ibid. p. 215.
(4) Parliamentary Ombudsman of Finland, 'Summary of the Annual Report 2015', (2016), p. 134-148, available from: https://www.oikeusasiamies.fi/documents/20184/39006/summary2015

Apart from the Parliamentary Ombudsman of Finland, the Serbian Protector of Citizens (Ombudsman) has been effective in overseeing covert surveillance measures. The Ombudsman has successfully challenged key legislation before the constitutional court, which has led to the amendment of laws on surveillance.

Best Practice: Serbian Protector of Citizens (Ombudsman)

In 2012 the Ombudsman reviewed legislation regulating the operations of Military Security and Intelligence Agencies, and found that the laws were not in compliance with the Constitution with regard to the protection of privacy rights. Some provisions contradicted the constitutional guarantee that any derogation from the privacy of correspondence and other means of communication must be approved by a court. The Ombudsman took the case to the Constitutional Court, which ruled in favor of the Ombudsman, stating that 'the Director of the Military Security Agency may order secret electronic surveillance of communication only if he has an approval of a first-instance court or a higher court at the territory under the jurisdiction of the Court of Appeals where the measure is instituted for secret electronic surveillance of communication and gaining an insight into listing of telephone

calls'. Subsequently, the Ombudsman submitted to the National Assembly a proposal to amend the law in order to bring it in line with the Constitution. In February 2013, the National Assembly accepted the proposal of the Ombudsman, and amended the law in accordance with the ruling of the Constitutional Court.

For more information on this case, see:
https://globalfreedomofexpression.columbia.edu/cases/serb-law-on-military-security-agency-and-military-intelligence-agency-articles-13-1-16-2-2012/
The case is also explained further in: Protector of Citizens, '2013 Annual Report', (2014), p. 209, available from:
http://www.ombudsman.org.rs/attachments/052_2013%20Annual%20Report%20of%20the%20Protector%20of%20Citizens.pdf

Independent oversight of collection information is a complex area. This section primarily dealt with the oversight of covert and targeted surveillance. However, this is not the only method used for information collection. Security services use a variety of other methods and sources, including human intelligence, untargeted bulk surveillance, computer network exploitation and searches of pre-existing databanks, all of which also have serious implications for fundamental human rights.[73]

[73] Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p. 54.

For a more detailed overview of the oversight of strategic and mass surveillance measures, see: Venice Commission, 'Update of the 2007 Report on the Democratic Oversight of the Security Services—Report on the Democratic Oversight of Signals Intelligence Agencies', (2015), available from: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

2. Overseeing the Use of Personal Data

The previous section addressed the oversight of covert information collection. Through covert measures, security services can obtain highly sensitive personal data. The services store, categorise and use the data; and are expected to delete it when it is no longer needed. It is imperative that oversight bodies monitor and where necessary investigate the way in which security services manage personal data since it has important implications for human rights, in particular the right to privacy and the right to freedom of expression.

Implications of the use of personal data on human rights

Personal data is defined as any information relating to an identifiable individual.[74] This includes, inter alia, social security numbers, medical records, membership to religious, civil and political organisations, travel history, financial transactions and personal communication

[74] Art. 2(a), *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

with friends and family.[75] The data collected on phone and electronic communications are categorised into two groups: the actual content of the communications and 'metadata' i.e. data about the communications which can reveal information as important as the content itself. The metadata includes:

- 'The location that it originated from, e.g. home address of the telephone, subscription information, and nearest cell tower;
- The device that sent or made the communication, e.g. telephone identifier, IMEI of the mobile phone, and unique data from the computer that sent a message;
- The times at which the message(s) were made and sent;
- The recipient of the communication, their location and device, and the time they received the message;
- Information related to the sender and recipients of a communication, e.g. email address, address book entry information, email providers, ISPs and IP address;
- The length of continuous interaction or the size of a message; and
- The precise location of the phone when switched on.'[76]

Traditionally, there have been weaker systems of oversight over the collection and use of 'metadata' on the basis that it does not contain the content of the communications, and that the collection is done through automated, computerised systems, which constitutes less of

[75] Aidan Wills, *Understanding Intelligence Oversight*, (DCAF: 2012), p. 21.
[76] Privacy International, *Explainers: What is Metadata*, available from: https://www.privacyinternational.org/node/53

an interference with privacy than wiretapping. However, current technology makes it possible to analyse and combine metadata to create a comprehensive profile of a person including where they are at all times, with whom they talk and for how long, patterns of behaviour, viewpoints, interactions and associations.[77]

Security services are allowed to collect and use personal data for various reasons including security clearance, discovering certain patterns of behaviour and analysing them in order to prevent threats. However, abuses in these processes such as collecting and retaining unnecessary and irrelevant information, using the information for unlawful purposes, maintaining incorrect information and unlawful disclosure can seriously infringe upon the right to privacy and may risk individuals' employment prospects, jeopardise personal and professional relationships and personal safety.[78] Moreover, widespread abuse in the use of personal data and the lack of accountability may have a negative effect on the exercise of other fundamental rights such as the right to freedom of expression,

[77] Ibid. Recently, there has been growing recognition of the need for more oversight of metadata collection and transfer. In this regard, the Court of Justice of the European Union has invalidated the EU Data Retention Directive on the grounds that it 'interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data'. See: Court of Justice of the European Union, *The Court of Justice declares the Data Retention Directive to be invalid*, Judgment in Joined Cases C-293/12 and C-594/12, Press Release No 54/14, (Luxembourg: 8 April 2014), available from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

[78] Aidan Wills, *Understanding Intelligence Oversight*, (DCAF: 2012), p. 22.

association, assembly and the right to participate in political and public affairs.[79]

International and European standards on personal data protection

International and European human rights law provides a clear framework for the protection of the right to privacy. In the past few decades, beyond the legal framework established by the ICCPR, the international community took further steps to develop standards for the processing of personal data.

In 1990, the UN General Assembly adopted the **United Nations Guidelines concerning Computerized Personal Data Files**. The Guidelines provide for the principle of lawfulness and fairness of the collection and processing of personal data, accuracy, purpose-specification, interested-person access, non-discrimination and security of the data files.[80] As mentioned in the previous section, in 2010 the UN Special Rapporteur compiled good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies.[81] Practices 23 to 26 address the management and the use of personal data as well as its oversight. The following best practices focus on oversight aspects, and are thus relevant to Ombuds institutions.

[79] Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p. 6.
[80] See: http://www.un.org/documents/ga/res/45/a45r095.htm
[81] *UN Compilation of Good Practices*, A/HRC/14/46.

UN Compilation of Good Practices

Practice 25. An **independent institution exists to oversee the use of personal data** by intelligence services. This institution has **access to all files** held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

Practice 26. Individuals have the possibility to **request access to their personal data** held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an **independent data-protection or oversight institution**. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence service.

Following the UN Compilation of Good Practices, in 2013 the UN General Assembly adopted a Resolution on 'The Right to Privacy in the Digital Age' and in 2015, the UN Human Rights Council appointed a Special Rapporteur on Privacy.[82] These developments are

[82] *General Assembly Resolution 68/167* 'The right to privacy in the digital age', (18 December 2013), available from: http://undocs.org/A/RES/68/167 Also see: *Report of the Office of the United Nations High Commissioner for Human Rights*, 'The right to privacy in the digital age', A/HRC/27/37, (30 June 2014), available from:

testament to the growing importance of personal data protection and promotion of the right to privacy.

At the regional level, the Council of Europe has taken concrete measures to regulate the use of personal data. In 1985, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data entered into force, which protects the individual against abuses which may accompany the collection and processing of personal data.[83]

The convention brought important obligations for security services regarding the quality and security of data.[84] Furthermore, the convention stipulates that the 'data subject'—the person whose data has been collected and used—has the right to:

- **Establish the existence of personal data**: 'Any person shall be enabled […] to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.
- **Access data:** […] to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; and to obtain, as the case may be,

---

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[83] See: http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[84] See: Art. 5 & 7.

rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving.

- **Right to a remedy:** […] to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with [emphasis added].'[85]

External oversight mechanisms, including ombuds institutions, have a key role in protecting and promoting these rights. Indeed in 2001, an additional protocol to the Convention was adopted which stipulates that states shall designate one or more supervisory authorities responsible for ensuring compliance with the principles stated in the Convention. The protocol states that such supervisory authorities shall:

- Exercise their functions in complete independence;
- Hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence; and
- Have powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities.[86]

While the powers described above are in line with the mandate of ombuds institutions; following the requirements of the EU Data Protection Directive, COE states, who are also members of the EU,

[85] Art. 8.
[86] See: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7834785, Art. 1.

have conferred one national supervisory authority with a wide remit for monitoring the application of and ensuring respect for data protection legislation within their territories (in many countries, prior to the establishment of Data Protection Authorities, the duty to monitor data protection was entrusted to Ombuds institutions).[87]

Case law of the European Court of Human Rights reinforced the standards set out in the aforementioned CoE Convention and additional Protocol. In ***Rotaru v Romania***, the ECtHR expressly recognised that Article 8 of the ECHR should be interpreted in such a way as to encompass guarantees concerning data protection enshrined in the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.[88]

The Court's landmark rulings contributed to standard setting in specific areas of overseeing data protection. For instance, in its judgment on the ***Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria***, the Court established that there was no independent review of the destruction of personal data by intelligence services. Consequently it ruled that Article 8 of the convention (the right to privacy) was violated.[89]

---

[87] European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities*: Strengthening the fundamental rights architecture in the EU II, (2010), p. 19, available from: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[88] *Rotaru v. Romania* (28341/95) para 43, available from: http://hudoc.echr.coe.int/eng?i=001-58586

[89] Association for European Integration and Human Rights*, Ekimdzhiev v. Bulgaria*, paras 84, 92, available from:

For a more detailed overview of the Court's case law, see: 'Factsheet on Personal Data Protection,' available from: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

Overseeing the use of personal data—the role of ombuds institutions

States set up a variety of mechanisms to hold services accountable for the use of personal data. Parliaments enact specific legislation on data protection and have designated that parliamentary committees monitor the implementation of the law;[90] and the security services are expected to carry out internal control through regular assessments of the relevance and accuracy of the data they hold.[91] The judiciary adjudicates on cases concerning the violation of the right to privacy.

Independent oversight mechanisms also have an important role in ensuring human rights compliance with respect to the use of personal data. These include:

- Conducting regular inspection visits to the services and random checks of personal data files;
- Checking whether internal directives on file management comply with domestic law;[92]

---

https://hudoc.echr.coe.int/eng#{"fulltext":["Ekimdzhiev v. Bulgaria"]}

[90] See: *UN Compilation of Good Practices*, Practice 23, for the standards to be included in domestic data protection laws.

[91] *UN Compilation of Good Practices*, Practice 24.

[92] Ibid. para 39.

- Conducting own-motion investigations into the handling of a particular data file;
- Handling requests to access personal data held by security services; and
- Handling complaints and reviewing the legality of services' denial to provide access to personal data.

In most European countries, the aforementioned roles are assumed by multiple external oversight mechanisms, including designated data protection authorities (DPA); expert oversight bodies, and ombuds institutions. As mentioned earlier, in most EU member states DPAs took over to a large extent the oversight role, which was held by ombuds institutions earlier. However in some countries such as Slovenia and Hungary, ombuds institutions continue to oversee matters related to data protection. In Germany, the mandate is shared between the DPA and the G-10 commission (an expert oversight body). In Denmark, the Intelligence Oversight Board oversees the use of personal data by security services; while in Portugal it is the exclusive prerogative of the data protection supervisor/commission.[93] Despite their increasingly limited role, ombuds institutions continue to make an important contribution to the accountability system concerning personal data protection.

Below are selected best practices from Hungary, Slovenia, and Serbia.

[93] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* (2011), p. 116.

Best Practice: Hungarian Commissioner for Fundamental Rights

The principal authority overseeing the use of personal data in Hungary is the Commissioner for Data Protection. However, the Commissioner for Fundamental Rights (Ombudsman) continues to oversee the protection of the right to privacy, particularly by monitoring laws and assessing their impact on human rights.

In 2012, the Government amended certain provisions of laws on National Security Services, Protection of Classified Information and the Registration of Biometric Data. The Data Protection Commissioner launched a petition before the Constitutional Court to annul the amendments. However, his term ended and the petition was not followed up. The Ombudsman closely monitored the process, and after observing that the initial petition had not been followed up, resubmitted the petition, once again requesting the Constitutional Court to review the amendments.

(Source: http://www.ajbh.hu/en/web/ajbh-en/-/the-ombudsman-resubmits-petitions-of-the-commissioner-for-data-protection-to-the-constitutional-court)

In this case, the Ombudsman complemented the efforts of the Data Protection Commissioner. Oversight bodies with overlapping mandates are usually not recommended for a variety of reasons (including confusion of roles, risk of duplication, and inefficient use of resources). However, in this case, it worked well.

Best Practice: Slovenian Human Rights Ombudsman

In 2005, Slovenia established the office of the Information Commissioner, which is an independent oversight body focusing exclusively on data protection and issues related to access to information. However, the Slovenian Ombudsman continues to receive and handle complaints concerning data protection, as it falls under the Ombudsman's mandate to monitor the exercise of the right to privacy.

The Ombudsman receives between forty to sixty complaints on data protection each year. Most are forwarded to the Information Commissioner, while some are dealt with by the Ombudsman. In doing so, the Ombudsman consults with the Information Commissioner, and seeks his or her opinion on legal and technical matters. The reports of the Ombudsman indicate a good level of cooperation with the Commissioner in this regard (See: Annual Report, (2014), p. 33).

In 2012, the Ombudsman received a complaint about unlawful disclosure of personal data by a news channel. The Ombudsman's investigation found that the channel accessed the personal data through the archives of the former State Security Service, which did not have any safeguards against disclosure of sensitive personal data. It was also found that the archived personal data was obtained in violation of fundamental human rights. The investigation led to an internal inspection of the archives, which established a deficiency in the law regulating access to information archives.

(Source: Human Rights Ombudsman, 'Eighteenth Regular Annual Report of the Human Rights Ombudsman of the Republic of Slovenia for the Year 2012', (2013), p. 26-27, available from: http://www.varuh-rs.si/fileadmin/user_upload/pdf/lp/LP2012_ANG_www.pdf)

Following the ombudsman's investigation, the Government of the Republic of Slovenia prepared the Act on Supplementing and Changing of the Protection of Documents and Archives and Archival Institutions Act.

In this case, the Ombudsman's investigations on personal data protection led to a concrete change in the legal framework.

(Source: http://www.theioi.org/ioi-news/current-news/ombudsman-reviews-disclosure-of-archived-materials)

Best Practice: Serbian Protector of Citizens

The Serbian Protector of Citizens (Ombudsman) regularly communicates and cooperates with the Commissioner for Information of Public Importance and Personal Data Protection (Commissioner) on data protection issues, particularly in the security sector. The Ombudsman and the Commissioner have held a series of consultations on legal gaps and implementation problems concerning the collection, use and sharing of personal data by the military, law enforcement and security services. In doing so, they reached out to civil society and sought their input.

As a result of these consultations, in 2012 the Ombudsman and the Commissioner jointly issued fourteen recommendations, addressing issues related to the collection and the use of personal data, as well as its oversight. Some of the recommendations include:

- 'ensure undeletable recording of accesses to telecommunications, with all data necessary to make subsequent control of legality and regularity of access.
- re-examine results of implementation of the Law on Data Privacy (including adoption of necessary by-laws, declassification of older documents, conducting of investigations, issuance of security certificates...) and make serious amendments to this Law or adopt a new one.
- strengthen the capacity of supervisory institutions to handle sensitive data and keep them.'

The full text can be accessed at: http://docplayer.net/12621900-14-points-identified-by-the-ombudsman-and-the-commissioner-for-information-of-public-importance-and-personal-data-protection.html

Since then, the Ombudsman followed up on these recommendations and put forth concrete proposals for legislative amendments. In this context, the Ombudsman's cooperation with the Data Protection Commissioner, the involvement of civil society, and the Ombudsman's determination in following up on recommendations represent best practice.

3. Overseeing Information Sharing

Taxonomy of information sharing

Information sharing is a core function of security services. Services collect and analyse data to produce intelligence, and disseminate it to relevant State institutions that are tasked with preventing and combatting crimes, such as the police, border guards and customs. Beyond domestic intelligence sharing, security services share information with their counterparts in other countries. Although international intelligence cooperation has existed for decades, the scope and scale of information sharing has significantly increased since 9/11, primarily in response to the increasingly transnationalised nature of terrorism and other serious threats to national security.[94]

Security services share information with their foreign counterparts for a number of **purposes,** including:

- To prevent serious threats to public safety such as transnational terrorism, and thereby to safeguard the right to life;
- To avoid duplications of efforts, and thus save resources; and
- To avoid engaging in high-risk information collection activities.[95]

[94] Hans Born, Ian Leigh and Aidan Wills, *Making International Intelligence Cooperation Accountable*, (DCAF/ EOS: 2015), p. 2, available from: http://www.dcaf.ch/making-international-intelligence-cooperation-accountable

[95] Ibid. p. 18-21.

Information shared internationally between security services can be categorised into three groups: 1) '**strategic information'**, consisting of assessments covering foreign policy developments, the security environment, trends relating to specific issues such as terrorism and WMD proliferation; 2) **'operational information',** referring to the capabilities and working modalities of non-state armed groups and individuals; and 3) '**tactical information',** which includes data on existing operations or investigations, including specific details on the identity, locations and activities of individuals under surveillance.[96]

There are essentially two **forms of information sharing**: reactive and automated. Traditionally, security services mostly shared information reactively, i.e. in response to a specific request from a foreign partner concerning a particular issue, group, or individual. However, the rapid development of technology, which allowed for the collection and storage of mass data, as well as intensified cooperation between close partners, have led to an increase in automated information sharing. Such exchange occurs without a specific request, often by providing secure electronic links or even granting foreign partners direct access to the database of the service.[97] The latter was the case for GCHQ, which was granted access to raw material collected in bulk by NSA and other foreign intelligence agencies.[98]

[96] Ibid. p. 18-19.
[97] Ibid. p. 20-21.
[98] James Ball, 'GCHQ views data without a warrant, government admits', *The Guardian*, (29 October 2015), available from: https://www.theguardian.com/uk-news/2014/oct/29/gchq-nsa-data-surveillance

Implications of information sharing for human rights

Both domestic and international information sharing pose important risks to the protection of human rights.

At the domestic level, States have been encouraging enhanced cooperation between security services and law enforcement agencies to combat terrorism and other serious threats to national security. Accordingly, States have amended their legal framework to foster domestic intelligence sharing. For example, the UK Terrorism Act of 2008 explicitly authorised security services to disclose information to the police for the purpose of furthering criminal proceedings.[99] In order to further facilitate information sharing, many States established 'fusion centres' to aggregate information about security threats provided by multiple domestic and foreign sources.[100] However, sharing information obtained by security services with the police can be problematic. Laws regulating the collection of information by security services usually differ from those of law enforcement agencies; thus the information obtained by security services may be inadmissible in a legal proceeding. Furthermore, if not regulated or strictly controlled, security services may keep personal data for a long period of time, which may no longer be accurate or reliable. Disclosure of such data in a court proceeding would seriously infringe upon the right to privacy.

[99] Kent Roach 'Overseeing Information Sharing' in Born and Wills (ed) O*verseeing Intelligence Services – A Toolkit* (DCAF: 2012), p. 139.
[100] Ibid. p. 132.

On the other hand, security services may not be willing to share information with the police, as it requires disclosing their sources and may disrupt their own intelligence activities. Such hesitation also has implications for human rights, as the lack of cooperation can result in the failure to prevent deadly terror attacks.[101]

Information exchange with foreign security services poses additional risks to human rights, concerning both outgoing and incoming information. When security services send information to their counterparts, they have very little control over how their counterparts use that information. Although there are certain legal and procedural safeguards such as the 'third party rule' and 'caveats' (explained in the following sub-sections), in practice they do not fully ensure that recipient services will use the information lawfully and appropriately. The recipient service may use that information to unlawfully arrest, detain or even torture an individual; or subject the individual to extraordinary rendition or targeted/extrajudicial killing, all of which constitute grave human rights violations. In such cases, the sending service would be considered complicit in the wrongful acts of their partners.[102]

When services receive information from their foreign partners, there is no way to be fully sure that information was obtained lawfully; in

[101] Ibid, p. 131.

[102] Hans Born, Ian Leigh and Aidan Wills, *Making International Intelligence Cooperation Accountable*, (DCAF/ EOS: 2015), p. 38-42. For a more detailed overview of human rights implications and case law, see Chapter 4, 'International Legal Standards and International Intelligence Cooperation', of the same publication.

accordance with obligations under international human rights law. This is particularly the case for information received by services in non-democratic states, which are often not effectively and independently overseen. Information sharing with such services raises the risk of receiving evidence or information gained through the use of torture, and consequently makes security services which cooperate with them vulnerable to allegations of complicity. In an attempt to minimise such a risk and provide guidance to the security services on intelligence sharing in line with international human rights standards; the United Kingdom published a 'Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees' in 2010.'[103] Similarly, in 2011 Canada published the 'Ministerial Direction to Canadian Security Intelligence Service (CSIS): Information sharing with foreign entities'. However, both documents have been criticised by experts and international community, including Amnesty International, [104] with regard to the use of vague terminology and establishing criteria that fall short of international standards. The Association for the Prevention of Torture published the report 'Before the Gift of Poison Fruit–Sharing information with States that torture', which analysed the shortcomings of both documents. The report can be accessed at:
http://www.apt.ch/content/files_res/report-exclusionary-rule-

[103] See: http://intelligencecommissioner.com/content.asp?id=29
[104] Amnesty International, 'Canada must withdraw Ministerial Direction on information sharing with foreign entities tainted by torture', (2012), available from: http://www.amnesty.ca/news/canada-must-withdraw-ministerial-direction-information-sharing-foreign-entities-tainted-torture

workshop-en.pdf

The British Equality and Human Rights Commission challenged the Government in court over the Guidance. The Court ruled that guidance on hooding practices were not in line with the UK's obligations under international law.[105] This constitutes best practice with respect to independent oversight, since the Equality and Human Rights Commission reviewed the Guidance, challenged the Government in court and advocated for compliance with the absolute prohibition of torture.

While both documents have certain ambiguous formulations and flawed parts, the attempts of British and Canadian governments to issue such guidance on information sharing and identifying potential torture-tainted information acknowledges the importance attached to this issue. Developing such detailed guidance should be encouraged on the condition that it should be open to regular parliamentary and independent oversight.[106]

Another caveat of intelligence sharing is that the incoming information is not subjected to laws and regulations on information collection of the receiving country. This may lead to intelligence services purposefully rely on information from foreign partners in

[105] UK High Court, *The Equality and Human Rights Commission, v. The Prime Minister*, Judgement, 3 October 2011, [2011], EWHC 2401 (Admin).
[106] Association for the Prevention of Torture (APT), *Before the Gift of Poison Fruit: Sharing information with States that Torture*, Outcome Report, (2012), p. 42, available from: https://www.apt.ch/content/files_res/report-exclusionary-rule-workshop-en.pdf

order to avoid domestic legal processes for collecting information. In other words, whereas security services would have to obtain a judicial authorisation to carry out targeted surveillance within their jurisdiction, if this same information were obtained by a foreign security service and later shared, it is possible that no such safeguards would be applicable.[107] This was the case for GCHQ. According to domestic laws and regulations, whenever GCHQ obtains intelligence from the US, a warrant signed by a minister is needed. However, the bilateral arrangement between GCHQ and NSA allowed the former to obtain raw intelligence, which can include communications of UK citizens, without a warrant, 'if it was "not technically feasible" to obtain the communications under a warrant'.[108] Such an arrangement is certainly open to abuse and the deliberate circumvention of domestic legal safeguards.

International standards on the oversight of information sharing

The serious human rights implications of domestic and international intelligence sharing make standards on effective oversight all the more necessary. Currently there is no international legal instrument regulating information sharing between security services. However following 9/11, the United Nations Security Council adopted Resolution 1373, which calls upon States to 'cooperate, particularly through bilateral and multilateral arrangements and agreements, to

[107] Council of Europe, *Democratic Oversight of National Security Services*, (2015), p. 24.
[108] James Ball, 'GCHQ views data without a warrant, government admits', *The Guardian*, (29 October 2015).

prevent and suppress terrorist attacks'. More specifically, the Resolution calls for 'intensifying and accelerating the exchange of operational information 'regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups'; and the threat posed by the possession of weapons of mass destruction by terrorist groups'.[109] It is the most concrete reference to information sharing between States. While there is no particular reference to the oversight of information sharing, the Resolution states that the exchange of information should be in accordance with international and domestic law.[110]

Besides the Resolution, the UN Compilation of Good Practices has a specific section on 'Intelligence–sharing and cooperation', and Practice 34 refers explicitly to the role of independent oversight institutions.

UN Compilation of Good Practices

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

[109] UNSC *Res 1373* (2001), 3(a), 3(c), available from: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf
[110] Ibid. 3b.

The UN Special Rapporteur acknowledged that while oversight institutions should have access to *all* information necessary to conduct their mandate, in practice they encounter challenges with overseeing incoming information sent by foreign services, due to the third party rule, which restricts the disclosure of the shared information to oversight bodies.[111]

However, since then the international community has increasingly emphasised a need for independent oversight of incoming information, thereby reinterpreting the third party rule and its application to oversight bodies, and contending that oversight bodies should be considered as within the 'ring of secrecy'.

In 2011, the Parliamentary Assembly of the Council of Europe adopted a resolution which stipulated that 'it is unacceptable that activities affecting several countries should escape scrutiny because the services concerned in each country invoke the need to protect future co-operation with their foreign partners to justify the refusal to inform their respective oversight bodies.'[112]

In 2015, the Council of Europe Commissioner for Human Rights recommended that 'access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of

[111] Ibid. para 49.
[112] Parliamentary Assembly of the Council of Europe, *Resolution 1838* (2011), para 7.

originator control.' [113] More specifically, the Commissioner recommended that States 'mandate oversight bodies to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information….' External oversight of security service cooperation with foreign bodies should include but not be limited to examining:

- Ministerial directives and internal regulations relating to international intelligence Cooperation;
- Human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation;
- Outgoing personal data and any caveats (conditions) attached thereto;
- Security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance; and
- Intelligence cooperation agreements.[114]

Overseeing information sharing—the role of oversight bodies

As with other aspects of intelligence governance, the executive, judiciary, parliament and independent oversight bodies share

[113] Council of Europe Commissioner for Human Rights, D*emocratic and Effective Oversight of National Security Services*, (2015), Recommendation 16.
[114] Ibid. Recommendation 5.

responsibility for overseeing information sharing. Independent oversight institutions are primarily responsible for:

- 'Advising parliament and/or the executive on the legal framework relating to intelligence cooperation and assuring that it is sufficiently covered by law;
- Overseeing the propriety, legality, effectiveness, and efficiency of information sharing; and
- Investigating issues related to information sharing.'[115]

As far as the activities of security services are concerned, information sharing is perhaps the most difficult to oversee. This could be explained by the complexity of international information sharing, as well as the lack of available expertise and resources.[116]

Among the different types of independent oversight institutions, expert bodies with exclusive mandates over security services are better suited to oversee information sharing (particularly international information sharing), compared to national ombuds institutions with a broad, general mandate. This is because expert oversight bodies usually have more powers and resources, which they can focus exclusively on intelligence oversight. There are very few examples of national ombuds institutions conducting effective oversight in this regard. This subsection will explain some of the challenges of overseeing information sharing and provide examples of best practices.

[115] Hans Born, Ian Leigh and Aidan Wills, *Making International Intelligence Cooperation Accountable*, (DCAF/ EOS: 2015), p. 8.
[116] Ibid. p. 132.

Overseeing domestic information sharing

The previous sections referred to the increase of information sharing between security services and domestic law enforcement agencies. While expert oversight bodies are better positioned to oversee security services, a common challenge faced by such bodies is that they usually have an exclusive mandate over a single agency. That is, specialised intelligence oversight bodies do not have jurisdiction over the activities of law enforcement agencies and vice versa. Therefore, in some cases, matters relating to cooperation between the two agencies may fall outside the scope of oversight.

One way to overcome this challenge is to allow and encourage different specialised oversight bodies to cooperate when it comes to overseeing information sharing. In Belgium, the Committee P and the Committee I are the two specialised expert oversight bodies in charge of overseeing the police and security services respectively. The two oversight bodies are permitted to share information concerning cooperation between the police and security services; and they have conducted several joint investigations in this regard.[117] Where such cooperation between oversight mechanisms is lacking, one way to oversee information sharing between agencies is to set up an ad-hoc inquiry commission with the necessary mandate. However it should be noted that such ad-hoc commissions solely exercise ex-post oversight, often in response to a major incident, and

[117] Kent Roach 'Overseeing Information Sharing' in Born and Wills (ed) O*verseeing Intelligence Services – A Toolkit* (DCAF: 2012), p. 141.

can never replace standing mechanisms conducting proactive oversight.

Best Practice: Canada, Air India Inquiry Commission

In 2006, Canada set up a long-due inquiry commission to investigate the failures that led to the catastrophic 1985 Air India bombing, and to identify gaps in Canada's security and intelligence system. The Commission focused at length on the coordination and information sharing (and lack thereof) among the police and security services. It found that the Canadian Security Intelligence Service, and the national police force, the RCMP, were more interested in protecting turf than sharing information about the terrorist threat.[1] In this case, a lack of proper information sharing resulted the failure to prevent a massive terror attack, in which 329 people died.

In response to the Commission's conclusions, the Canadian Government pledged to introduce legislation to clarify the authorities for information sharing for the purposes of national security; and to enable a review of national security activities involving multiple departments and agencies.[2]

Sources:
(1) Sandro Contenta, 'Air India Bombing: Canada's Saga Continues', *Public Radio International* (PRI), Global Post, (January 12, 2011), available from: http://www.pri.org/stories/2011-01-13/air-india-bombing-canadas-saga-continues
(2) Government of Canada, 'The Government of Canada Response

to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182', (2010), available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rspns-cmmssn/index-en.aspx

In the absence of specialised oversight bodies or ad-hoc inquiry commissions to oversee domestic information sharing, national ombuds institutions can play a key role. They can use their mandate to launch national public inquiries[118] or review existing legislation and policies to identify gaps and suggest improvements. While such oversight of information sharing by ombuds institutions is unfortunately rare, the Serbian Protector of Citizens represents best practice, particularly in identifying gaps in legislation and proposing amendments.

Best Practice: Protector of Citizens (Ombudsman), Serbia

In 2013, the Ombudsman submitted to the parliament a proposal for a legal amendment on regulating domestic information sharing between the Military Intelligence Agency (MIA) and the National Police. The amendment concerned the Law on the Military Security Agency and the Military Intelligence Agency, and stipulated that 'the MSA and the MIA, if they obtain information of which other security services or the police are in charge, are to forward those

[118] See: Asia Pacific Forum, *Manual on Conducting a National Inquiry into Systemic Patterns of Human Rights Violations*, (2012), available from: http://www.asiapacificforum.net/media/resource_file/Conducting_National_Inquiries_Manual.pdf

pieces of information to other security services if they are of relevance for national safety or to the police if they relate to criminal offences for which special presentation of evidence is required under the Criminal Code.'[1]

The proposal of the Ombudsman was adopted by the Parliament. Owing to the Ombudsman's efforts, domestic intelligence sharing between security services and law enforcement agencies are now based on a publicly available law, which emphasises the principles of proportionality and necessity. The need for a legal basis for intelligence sharing has also been acknowledged in the UN Compilation of Good Practices.[2]

Source:
(1) Protector of Citizens, '2013 Annual Report', (2014), p. 209, available from: http://www.ombudsman.org.rs/attachments/052_2013%20Annual%20Report%20of%20the%20Protector%20of%20Citizens.pdf
(2) Human Rights Council, 'Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies', A/HRC/14/46, (2010), para 45, available from: https://fas.org/irp/eprint/unhrc.pdf

Overseeing international information sharing

Overseeing international information sharing is even more challenging for oversight bodies, as it involves at least one foreign security service, multiple jurisdictions, highly complex technologies

and means of information sharing, and competing priorities of oversight bodies. Once again, expert oversight bodies have the advantage of an exclusive mandate, wider powers and more resources compared to national ombuds institutions.

There are certain **facilitating factors** which allow oversight bodies to more effectively scrutinise international information sharing, such as:

A) Explicit mandates

As stated by the UN Special Rapporteur, it is good practice for oversight institutions to be explicitly mandated to oversee agreements and arrangements upon which international information sharing is based.[119] In this way, security services cannot resist or argue that agreements with foreign partners fall outside of the scope of overseers. Unfortunately most oversight bodies do not have such an explicit mandate. In this regard, Canada is an exception as legislation stipulates that one of the functions of the Security Intelligence Review Committee (SIRC) is to review arrangements and cooperation with foreign states.[120]

B) Duty to report to oversight bodies

An important challenge for oversight bodies is that they are often not aware of information sharing with foreign security services due to the

[119] A/HRC/14/46. Para 49.

[120] Canadian Security Intelligence Act, Art. 17 (2). Also see: Hans Born, Ian Leigh and Aidan Wills, *Making International Intelligence Cooperation Accountable*, (DCAF/ EOS: 2015), p. 132.

highly sensitive nature of the information, as well as the covert methods of information collection. As a result, such bodies rarely receive any complaints from individuals. In this regard, best practice is to oblige the security services to report information sharing to an independent oversight institution, as is the case in Germany. According to the law in Germany, the security services have to report intelligence sharing to the G10 Commission.[121] Without such an obligation to report, the only tools oversight bodies would have would be periodic and/or own-motion investigations.

C) Keeping written records of shared information

In the absence of comprehensive written records, it is clear that oversight bodies cannot effectively oversee the process behind and the actual content of the information shared. Indeed the Arar Commission, a Canadian ad-hoc inquiry commission to investigate information sharing between the services of Canada and the US, whose landmark recommendations contributed to standard-setting on overseeing information sharing; stated that the service who provided the information should keep a record of the:

- Description of information shared;
- Basis for the decision to share information; and
- Those responsible for the decision making.[122]

[121] *UN Compilation of Good Practices*, A/HRC/14/46 para 49, footnote 171, (G10 Act, Section 7a).
[122] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations,* (2006), p. 348.

D) Access to information—reinterpretation of the 'third party rule'

As mentioned in the previous subsections, a significant impediment to external oversight is the 'third party rule', which prescribes that information shared with foreign security services cannot be shared with third parties without the permission of the service that provided the information.[123] While this rule can serve as a safeguard to protect information, when used against oversight bodies, it poses a significant challenge to accountability. Therefore it is recommended that States interpret this rule so that it does not apply to oversight bodies. Indeed several oversight bodies such as the Canadian SIRC, Dutch CTIVD, and Norwegian EOS Committee have adopted the approach that legal provisions entrusting them with the power to access all relevant information held by services override any restrictions based on the third party rule.[124]

There are very few oversight bodies that benefit from the facilitating factors listed above, and which are able to effectively oversee international information sharing. While such information sharing continues to be an under-scrutinised area, this section will outline some of the rare best practices by expert oversight bodies in Norway and the Netherlands.

[123] Hans Born, Ian Leigh and Aidan Wills, *Making International Intelligence Cooperation Accountable*, (DCAF/ EOS: 2015), p. 3.
[124] Ibid. p. 153.

Due to the nature of international information sharing, it is evident that oversight bodies receive none or very few complaints from members of public. In addition, if they are not notified by security services, the only available tools for oversight bodies are periodic reviews and thematic investigations.

1: Periodic reviews

A key method to exercise proactive oversight is to conduct periodic reviews to identify gaps and shortcomings in legislation and practice concerning information sharing. In this regard, the key aspects to be overseen are, inter alia:

- The legal and operational framework for international information sharing;
- Processes for assessing risks when sharing information with foreign partners;
- The actual content of personal data exchanges; and
- Caveats and safeguards relating to information shared with foreign services.[125]

Oversight bodies can conduct such reviews through a combination of methods including documentation review, inspection of facilities and interviewing members of security services. The Norwegian EOS Committee embodies best practice in this regard.

[125] Ibid. p. 134.

2: Thematic investigations

Another method to oversee information sharing is to launch thematic investigations, either own-initiative or by referral from the parliament. In this context, thematic investigations usually focus on a particular aspect of information sharing; take a snapshot of the state of affairs, identify the main shortcomings and put forward specific policy recommendations. The Dutch expert oversight body, CTIVD, conducted a thematic investigation into the exchange of telecommunications data.

Best Practice: EOS Committee, Norway

Norway's EOS Committee regularly scrutinises the exchange of personal data with foreign services, with a particular focus on outgoing information. In doing so, it carries out periodic inspections of the security services' facilities, and requests a list of new and updated files and all personal data correspondence with foreign services. Based on the list, the Committee selects a sample of cases. Through its direct access to the database of the Norwegian Security Service (PST), the Committee examines the relevant personal data shared with foreign partners to see whether PST acted in accordance with laws and regulations.[1]

Apart from inspections, the Committee submits written questions to the security service concerning exchange of personal data. The questions particularly address the caveats applied by the service to safeguard human rights, such as the principle of proportionality, risk assessment, and record keeping. Questions included:

- What factors are included in the assessment of whether the consequences for individuals are proportionate to the purposes of the disclosure of information to a foreign entity?
- Does the PST make written assessments in connection with requests for disclosure of biometric data?
- Where and how does the PST record an overview of information disclosed by the PST?
- Do any special conditions apply to the disclosure of unverified information?[2]

Sources:
(1) Hans Born, Ian Leigh and Aidan Wills, Making International Intelligence Cooperation Accountable, (DCAF/ EOS: 2015), p. 148, available from: http://www.dcaf.ch/making-international-intelligence-cooperation-accountable
(2) Ibid. p. 138.

Best Practice: CTIVD Investigation of the Dutch Intelligence Services on the Exchange of Data with Foreign Services

In the wake of Edward Snowden's revelations, the Dutch parliament requested CTIVD to carry out a broad investigation of the services' (both civil and military intelligence) collection, storage and sharing of telecommunications data.
The CTIVD assessed in particular:

- Whether the services used telecommunications data in violation of domestic laws when cooperating with foreign

services.

- Whether the services circumvented legal limitations by asking foreign services to collect data.
    - Caveats attached: restrictions on the exchange of data with foreign services.
- Whether the principles of proportionality, necessity and subsidiarity have been respected in the exchange of data with foreign counterparts.[1]

Source:
(1) Hans Born, Ian Leigh and Aidan Wills, Making International Intelligence Cooperation Accountable, (DCAF/EOS: 2015), p. 146.

Overseeing information sharing is one of the most difficult tasks for independent oversight institutions. This section provided only a brief summary of some of the important issues that may be relevant for ombuds institutions. For a comprehensive overview of international intelligence cooperation, including a detailed analysis of international legal frameworks, as well as key standards and recommendations for internal, independent and judicial oversight of international intelligence cooperation, see the DCAF publication on 'Making International Intelligence Cooperation Accountable' at: http://www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable

Key Features for Effective Oversight—Relevance to Georgia

This chapter has dealt with overseeing three essential areas of intelligence activity: information collection, use of personal data and information sharing.

Georgia's newly established State Security Service (SSS) is authorised to collect information (including covert surveillance measures) and to conduct its analytical processing and generalisation. While this is a typical power granted to intelligence agencies around the world, the SSS is further entrusted with powers to investigate certain crimes and arrest and detain suspects, which are traditional law enforcement tasks.[1]

This chapter outlined the serious human rights implications of using information obtained for intelligence purposes in law enforcement operations. In this regard, best practice is to clearly define by law the circumstances in which information can be exchanged between security agencies. For instance, the German Federal Constitutional Court ruled that exchange of personal data between intelligence and law enforcement agencies is not permitted unless an important public interest so requires and which is clearly prescribed by law.[2]

The Law on State Security Service of Georgia does not prescribe the forms of information sharing or the exercise of oversight over such sharing; and it does not refer to the Law on the Protection of Personal Information, which contains provisions on the transfer of personal information to another State. There is a need to expressly

stipulate in the law the standards and legal and procedural safeguards concerning information sharing, as well as the mandate and powers of the oversight bodies in scrutinising the information shared. The last section of the chapter listed certain standards for effective oversight of information sharing, such as explicit mandate, obligation to report to oversight bodies, the need to keep extensive written records and interpretation of the third party rule. Moreover, examples illustrated how information is overseen in practice, the key aspects of information sharing to be reviewed, along with different methods of oversight.

While expert oversight bodies are better suited to oversee information collection, use and sharing, it does not mean ombuds institutions cannot exercise effective oversight. This chapter provided a number of best practices by ombuds institutions from Finland, Serbia and Slovenia, which are intended to be relevant examples for the PDO.

Sources:
(1) Law on the State Security Service, Art. 12, para 1; also see: Mindia Vashakmadze, 'The Legal Framework of Security Sector Governance in Georgia', (DCAF: 2015), p. 3-8.
(2) Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970).

Key reference material:

- Council of Europe, 'Democratic and Effective Oversight of National Security Services', (2015), available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770
- ECtHR, *Factsheet on Personal Data Protection*, available from: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities*: Strengthening the fundamental rights architecture in the EU II, (2010), available from: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf
- Hans Born, Ian Leigh and Aidan Wills, Making International Intelligence Cooperation Accountable, (DCAF/EOS: 2015), available from: http://www.dcaf.ch/making-international-intelligence-cooperation-accountable
- Ian Leigh, 'Overseeing the Use of Personal Data' in Born and Wills *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012).
- Kent Roach 'Overseeing Information Sharing' in Born and Wills (ed) O*verseeing Intelligence Services – A Toolkit* (DCAF: 2012).
- Parliamentary Assembly of the Council of Europe, *Resolution 1838,* (2011).
- United Nations Security Council Resolution 1373, (2001), available from:

https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

Essential sources relating to best practices:

- Government of Canada, 'The Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182', (2010), available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rspns-cmmssn/index-en.aspx
- Protector of Citizens, '2013 Annual Report', (2014), p. 209., available from: http://www.ombudsman.org.rs/attachments/052_2013%20Annual%20Report%20of%20the%20Protector%20of%20Citizens.pdf
- Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 'Report of the Events Relating to Maher Arar: Analysis and Recommendations', (2006).
- Juha Haapamäki, 'Special report of the Finnish Ombudsman' on *Oversight of Covert Police Intelligence Gathering,* Parliamentary Ombudsman of Finland, (n.d), available from: https://www.oikeusasiamies.fi/documents/20184/38532/Haapamaki%2C+Oversight+of+covert++police+intelligence+gathering.pdf

National human rights institutions (NHRI)—also known as ombuds institutions—have a crucial role to play in monitoring the security sector and holding the security sector accountable for its practices. NHRIs are also well placed to interact with other stakeholders to help facilitate broader security sector oversight and can ensure the development and maintenance of human rights-observant security policies and practices.

DCAF programming with NHRIs in Ukraine and Georgia focuses on a variety of human rights and security sector governance challenges and the need for guidance materials on monitoring law enforcement and state security services has been noted for some time.

This Series of Monitoring Products is designed to facilitate the work of National Human Rights (Ombuds) Institutions on monitoring the security sector. The series provides guidance on relevant best practices and may also be used for relevant capacity development trainings.

DCAF has also developed a number of products to assist Ombuds institutions on both broad and highly specific oversight and policy challenges, particularly in terms of gender equality and human rights monitoring within the armed forces. For more information please see: http://www.dcaf.ch/ombuds-institutions

DCAF
a centre for security, development and the rule of law